



Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good:

Innovative Public-Private Partnerships

June 2010



**Homeland
Security**

Editors:

Douglas A. Smith
Assistant Secretary for the Private Sector

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer



**Homeland
Security**

U.S. Department of
Homeland Security
Washington, DC 20528

June 2010

Private sector outreach plays a fundamental role in forming and fostering partnerships between the private and public sectors. The major goal of these partnerships is to efficiently and effectively provide technologies, products and services to address the mission critical need of securing the Homeland of the United States. The Private Sector Office in the Department of Homeland Security (DHS) is pleased to provide the resources contained in this book to our partners so that they may better understand how to get involved with DHS. There are several opportunities to learn about our requirements process, role of DHS, and how organizations like the Science & Technology Directorate (S&T) use this information to address the needs of the seven operating components (TSA, CBP, USCIS, ICE, USSS, FEMA, and USCG), first responders and eighteen sectors of the critical infrastructure/key resource owners and operators.

This resource also contains information on S&T's Commercialization initiatives that foster mutually beneficial public-private partnerships in order to field products, technologies and/or services to help meet the many needs and challenges of the public and private sectors as well as the first responder community. This book also demonstrates how sharing information on detailed operational requirements and conservative estimates of potential available markets can lead to the cooperative development of needed capabilities.

The Private Sector Office and S&T will continue to work together to best address the needs and requirements articulated by DHS and its stakeholders. With the combined efforts of both offices, the initiatives described in this book will allow DHS and the private sector to rapidly and effectively address key capability gaps and technology needs. It is our hope that through this resource the private sector will be better equipped at approaching and working with DHS to capitalize on the partnership opportunities available in a mutual effort to enhance our national security.

We would like to thank Mark Protacio, Caroline Greenwood and Timothy Del Monico for their valuable efforts in the development of this book. Any questions regarding the information contained within this resource may be directed to the Private Sector Office at private.sector@dhs.gov.

Sincerely,

A handwritten signature in black ink that reads "Douglas A. Smith".

Douglas A. Smith
Assistant Secretary for the Private Sector

A handwritten signature in black ink that reads "Thomas A. Cellucci".

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer

Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good: Innovative Public-Private Partnerships

Editors: Douglas A. Smith U.S. Department of Homeland Security: Private Sector Office, Washington D.C. 20528

Thomas A. Cellucci U.S. Department of Homeland Security: Science and Technology Directorate, Commercialization Office, Washington D.C. 20528

(Please click the titles below to be taken directly to the file)

I. Private Sector Office Resource Catalog

II. Commercialization Office Overview

Requirements Development Initiative
SECURE™ Program
FutureTECH™ Program
Commercialization Process
Private Sector Outreach

III. Briefs

Opportunities for the Private Sector
Commercialization Office: Providing Value through Efficiency and Cost-Effectiveness

IV. Articles

Commercialization: The First Responders' Best Friend
DHS: Leading the way to Help the Private Sector Help Itself
DHS Implements Commercialization Process
Bridging the Communications Gap Between the Public and Private Sectors
Making it Easier to Work with DHS: The Critical Role of Requirements
DHS Global Outreach Efforts: Looking for the Best Technology and Products
Conservative Estimates of Potential Available Markets
Innovative New Partnership Program Creates "Wins" for Taxpayers and the Public and Private Sectors
Commercialization: It's Not Business as Usual for DHS
Innovative Commercialization Process Delivers Cost-Effective and Efficient Product Development at DHS
Speed-of-Execution in Government? You Bet.
DHS Makes Transition from Acquisition to Commercialization
Capstone IPT and beyond...
Commercialization Office: Offering Transformational Change Beyond DHS
Helping Everyday Heroes Get What They Need
Opportunities to do Business with DHS S&T
Focus on Small Business
FutureTECH™: Guidance to Understanding Future DHS S&T Critical Research/Innovation Focus Areas

V. Charts

Market Potential Templates
Product Realization Chart

VI. Additional Resources

Developing Operational Requirements, Version 2 (November 2008)
Commercialization Operational Requirements Document Template
SECURE™ Program Overview and Concept of Operations
FutureTECH™ Program Overview and Concept of Operations

Private Sector Resources Catalog

May 2010



Homeland
Security

Intentionally blank page. Please continue to the next page.

Contents

Letter from Assistant Secretary Douglas A. Smith	4
Department-wide Resources	5
U.S. Citizenship and Immigration Services (USCIS)	7
Citizenship and Immigration Services Ombudsman (CIS Ombudsman)	8
U.S. Coast Guard (USCG)	9
U.S. Customs and Border Protection (CBP)	10
CBP Publications and Guidance.....	10
CBP Alerts and Newsletters	10
CBP Technical Assistance.....	10
CBP Programs and services	11
Cybersecurity and Communications (CS&C)	14
CS&C Training and Education	14
CS&C Publications and Guidance.....	14
CS&C Alerts and Newsletters	15
CS&C Technical Assistance.....	15
CS&C Programs and Services	16
Federal Emergency Management Agency (FEMA)	17
FEMA Training and Education.....	17
FEMA Alerts and Newsletters.....	18
FEMA Publications.....	18
FEMA Programs and Services	18
U.S. Immigration and Customs Enforcement (ICE)	21
Office of Infrastructure Protection (IP)	23
IP Training and Education	23
IP Guidance Documents/Publications	25
IP Programs/Services/Events.....	28
IP Web-Based Resources	31
Science & Technology Directorate (S&T)	33
S&T Programs.....	33
DHS Centers of Excellence	35
Transportation Security Administration (TSA)	37
TSA Training and Education.....	37
TSA Publications and Guidance	39
TSA Alerts and newsletters.....	40
TSA Technical assistance and help.....	40
TSA Programs and Services	41
Appendix A – Key Contacts	43
Appendix B – Index	47

Letter from Assistant Secretary Douglas A. Smith



Homeland Security

May 10, 2010

Dear Private Sector Partner,

To better facilitate your organization's access to the resources you need to help keep our country secure, DHS has developed this catalog. The first to be targeted specifically towards private sector partners and encompass all of DHS, this document collects the training, publications, guidance, alerts, newsletters, programs, and services available to the private sector across the department. It is organized by component and resource type and a comprehensive index is available to facilitate locating resources. Additionally, contact information across the department is available in Appendix A. Recognizing the diversity of the available resources as well as the continually evolving work of the department, this catalog will be updated regularly to publicize new resources and to increase private sector awareness.

In order to face the new threats and evolving hazards of today's security environment, we must develop and maintain critical homeland security capabilities at all layers of our society. We all share the responsibility to build all-hazards preparedness and resiliency into our way of life. As outlined in the Quadrennial Homeland Security Review Report released earlier this year, this *enterprise* approach is composed of multiple partners whose roles and responsibilities are distributed and shared among a broad-based community with a common interest in the public safety and well-being of America and American society.

The private sector is a critical partner in our homeland security efforts and my office is committed to strengthening the Department's relationship with organizations such as yours. As primary advisor to the Secretary on issues related to the private sector, including academia, non-profits, NGOs, and businesses, the Private Sector Office (PSO) coordinates active engagement between DHS and the private sector.

Regardless of where your organization fits into the homeland security enterprise, the Private Sector Office is committed to providing you with the assistance and support you require. You can contact our office at any time with requests, comments, questions, issues or concerns at private.sector@dhs.gov, (202) 282-8484.

Sincerely,

A handwritten signature in blue ink that reads "Douglas A. Smith". The signature is stylized and includes a large initial "D" and a flourish at the end.

Douglas A. Smith
Assistant Secretary for the Private Sector

Department-wide Resources

The Blog @ Homeland Security provides an inside-out view of what we do every day at the U.S. Department of Homeland Security. The Blog lets us talk about how we secure our nation, strengthen our programs, and unite the Department behind our common mission and principles. It also lets us hear from you. Visit <http://www.dhs.gov/journal/theblog/>.

Commercialization Office is responsible for the development and implementation of a commercialization process and for the execution of two innovative public-private partnerships that leverage research and development efforts in the private sector that are aligned to detailed operational requirements from Department stakeholders. The Commercialization Office also spearheads DHS Science and Technology's (S&T) outreach efforts that inform the private sector on "How to do business with DHS." See http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm. Contact: SandT.Commercialization@hq.dhs.gov, 1-(202) 254-6749.

Cooperative Research and Development Agreements (CRADAs) are part of the national Technology Transfer Program, designed to assist Federal laboratories in leveraging taxpayer dollars. As a designated Federal laboratory and a member of the Federal Laboratory Consortium, the Federal Law Enforcement Training Center (FLETC) can provide personnel services, facilities, equipment and other resources to support research and development that is beneficial to both FLETC and the CRADA partner. FLETC uses the CRADA program to establish partnerships for research and development in areas with potential to advance the nation's ability to train law enforcement personnel. The CRADA program can be used to identify and evaluate emerging technologies and training methodologies that can be incorporated into law enforcement and security training. See <http://www.federallabs.org> or contact FLETC-CRADAProgramOffice@dhs.gov, (912) 267-2100.

DHS Center for Faith-Based and Community Initiatives (CFBCI) builds, sustains, and improves effective

partnerships between government sectors and faith-based and community organizations. Located within FEMA, CFBCI is a vital communication link and engagement partner for faith-based and community organizations across the entire Department of Homeland Security. Visit www.dhs.gov/fbci. For more information or to sign up to receive Information Updates, e-mail Infobfci@dhs.gov.

DHS Office of Infrastructure Protection (IP) leads the national effort to mitigate risk to America's critical infrastructure from the full spectrum of 21st Century threats and hazards. IP coordinates with government and critical infrastructure owners and operators across 18 diverse sectors to enhance critical infrastructure resilience, strengthen protective programs, and share vital information. For more information on IP programs and resources visit www.dhs.gov/criticalinfrastructure.

DHS Private Sector Office As primary advisor to the Secretary on issues related to the private sector, including academia, non-profits, NGOs, and businesses, the Private Sector Office coordinates active engagement between DHS and the private sector to build strong partnerships, shape policy, and enhance internal and external dialog. For more information, contact the private sector office at private.sector@dhs.gov, (202) 282-8484.

DHS Private Sector Community Preparedness Updates The DHS Private Sector Office sends a weekly update e-mail collecting homeland security news and resources. To subscribe, see https://service.govdelivery.com/service/subscribe.html?code=USDHS_99. For more information, contact private.sector@dhs.gov, (202) 282-8484.

DisabilityPreparedness.gov is the Disability Resource Center of the Interagency Coordinating Council on Emergency Preparedness and Individuals with Disabilities (ICC). Maintained by the DHS Office for Civil Rights and Civil Liberties (CRCL), this site is the main repository for information related to the activities of the ICC, including bimonthly updates regarding federal programs and services relevant to individuals with disabilities and emergency preparedness. The site also contains

information to assist individuals with disabilities in personal preparedness planning; provides emergency managers, first responders, and other disaster service providers with resources relevant to working with individuals who have disabilities; and offers tips regarding how individuals with disabilities can get involved in preparedness activities within their communities. This resource can be accessed at www.disabilitypreparedness.gov. For more information, contact Disability.preparedness@dhs.gov, (202) 357-8483.

Electronic Crimes Task Force (ECTF) Program brings together not only Federal, State and local law enforcement, but also prosecutors, private industry and academia. The common purpose is the prevention, detection, mitigation and aggressive investigation of attacks on the nation's financial and critical infrastructures. The U.S. Secret Service's ECTF and Electronic Crimes Working Group initiatives prioritize investigative cases that involve electronic crimes. These initiatives provide necessary support and resources to field investigations that meet any one of the following criteria: significant economic or community impact, participation of organized criminal groups involving multiple districts or transnational organizations, or the use of schemes involving new technology. For more information, see <http://www.secretservice.gov/ectf.shtml>

E-Verify and Unfair Labor Practices The DHS Office for Civil Rights and Civil Liberties (CRCL) staff provides training on the responsibilities imposed upon the private sector when using E-Verify. Training includes best practices, examples of unlawful practices against workers, and preparing an HR Department to use E-Verify. The training assists employer understanding of how to use E-Verify in a responsible manner without violating prohibitions against discrimination. For more information, contact CRCL at crcltraining@dhs.gov, (202) 357-8258.

Homeland Security Information Network (HSIN) is a user-driven, web-based, sensitive but unclassified (SBU) information sharing platform that connects a broad range of homeland security mission partners. One portal of the

HSIN enterprise is HSIN-CS, managed by the Office of Infrastructure Protection. DHS has designated HSIN-CS to be its primary information-sharing platform between Critical Infrastructure Key Resource sector stakeholders. HSIN-CS enables DHS and critical infrastructure owners and operators to communicate, coordinate, and share sensitive and sector-relevant information to protect their critical assets, systems, functions and networks, at no charge to sector stakeholders. Vetted critical infrastructure private sector owners and operators are eligible to access HSIN-CS. To request access to HSIN-CS, please e-mail CIKRISAccess@hq.dhs.gov. When requesting access, please indicate the critical infrastructure sector to which your company belongs and include your name, company, official e-mail address, and supervisor's name and phone number. For more information, see www.dhs.gov/hsin or contact hsin.helpdesk@dhs.gov, (866) 430-0162.

Intelligence and Analysis Private Sector Partnership Program The Office of Intelligence and Analysis (I&A) strives to synchronize information sharing of timely, accurate, and actionable intelligence information with the private sector across the spectrum of business and security operations with respect to protecting privacy and civil rights and civil liberties. I&A provides private sector businesses, groups, and trade associations with tailored threat briefings to meet their security information needs. Additionally, the office creates intelligence products that are posted on the Homeland Security Information Network-Critical Sectors (HSIN-CS) portal for use by vetted critical infrastructure owners and operators. For more information, see www.dhs.gov/hsin. To request access to HSIN-CS, e-mail CIKRISAccess@hq.dhs.gov. When requesting access, please indicate the critical infrastructure sector to which your company belongs and include your name, company, official e-mail address, and supervisor's name and phone number. For more information, contact I&APrivateSectorCoordinator@hq.dhs.gov or call (202) 447-3517 or (202) 870-6087.

Lessons Learned and Information Sharing (LLIS.gov), a US Department of Homeland Security (DHS)/Federal Emergency Management Agency program, is the national online network of lessons learned, best practices, and innovative ideas for the emergency response and homeland security communities. This information and

collaboration resource helps emergency response providers and homeland security officials prevent, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. To register for LLIS, please visit www.llis.gov, contact the program via e-mail feedback@llis.dhs.gov, or call (866) 276-7001.

Office of Small and Disadvantaged Business Utilization (OSDBU) serves as the focal point for small business acquisition matters and works closely with all DHS components to implement the program. OSDBU makes available forecasts of contract opportunities, vendor outreach sessions, a list of component small business specialists, DHS prime contractors, and information about the DHS mentor-protégé program. See <http://www.dhs.gov/openforbusiness> or contact OSDBU, (202) 447-5555.

DHS Open Source Enterprise Daily Intelligence Reports provide open source information on several topics of interest. The following are currently available open source reports: **The DHS Daily Digest Report, The DHS Daily Cyber Report, The DHS Daily Infectious Diseases Report, The DHS Daily Human Trafficking and Smuggling Report, The DHS Daily Drug Trafficking and Smuggling Report, and The Daily Illicit Commercial Trafficking and Smuggling Report.** These reports may be accessed on the Homeland Security Information Network (HSIN) or private sector partners may request that they be added to distribution by e-mailing OSINTBranchMailbox@hq.dhs.gov with subject line reading "Request DHS Daily [name] Report".

The National Information Exchange Model (NIEM) Program is a Federal, State, local and Tribal interagency initiative providing a national approach and common vocabulary for information exchange. NIEM has a robust training curriculum that is accessible both in classroom and on-line. The primary audience for the NIEM Training Program is Executives, Project and Program Managers, Architects and Technical Implementers within Federal, State, local, Tribal and Private Entities. Additional information on the training courses and NIEM can be obtained by visiting www.NIEM.gov or e-mailing NIEMPMO@NIEM.gov.

Ready Business The U.S. Department of Homeland Security and the Advertising Council launched the *Ready Business* Campaign in September 2004. This extension of the successful *Ready* Campaign, *Ready Business* helps

owners and managers of small- and medium-sized businesses prepare their employees, operations and assets in the event of an emergency. For free tools and resources, including how to create a business emergency plan, please visit www.ready.gov.

Traveler Redress Inquiry Program (DHS TRIP) provides a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at airports, train stations, or crossing U.S. borders. To initiate an inquiry, please log onto DHS TRIP's interactive Web site www.dhs.gov/trip. For more information, contact the TSA Contact Center, (866) 289-9673.

U.S. Citizenship and Immigration Services (USCIS)

U.S. Citizenship and Immigration Services (USCIS) is the government agency that oversees lawful immigration to the United States. USCIS will secure America's promise as a nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system. www.uscis.gov

USCIS Asylum Program resources include an information guide for prospective asylum applicants available in a number of languages. For more information, visit www.uscis.gov/asylum.

E-Verify is an Internet-based system that allows an employer, using information reported on an employee's Form I-9, to determine the eligibility of that employee to work in the United States. For most employers, the use of E-Verify is voluntary and limited to determining the employment eligibility of new hires only. There is no charge to employers to use E-Verify. Available resources include a demonstration video, fact sheets, weekly webinars, an overview presentation, brochures and posters for employers and employees, and a rights and responsibilities guide. See <http://www.dhs.gov/everify>. Contact E-Verify@dhs.gov, (888) 464-4218 with any questions or comments.

U.S. Civics and Citizenship Online Resource Center for Instructors provides information about USCIS' Resource Center to help instructors prepare students for naturalization and incorporate civics into ESL instruction. See <http://www.uscis.gov/files/natedocuments/M-662.pdf>.

Civics and Citizenship Toolkit - A Collection of Educational Resources for Immigrants contains a variety of educational materials designed to help permanent residents learn more about the U.S. and prepare for the naturalization process. For more information, visit <http://www.citizenshiptoolkit.gov>.

Expanding ESL, Civics, and Citizenship Education in Your Community: A Start-Up Guide provides an overview and recommendations to help organizations design and offer

ESL and civics/citizenship classes for immigrants. See <http://www.uscis.gov/files/natedocuments/M-677.pdf>.

USCIS Genealogy Program is a fee-for-service program providing family historians and other researchers with timely access to historical immigration and naturalization records. The USCIS Genealogy Program offers two services: **Index Search** using biographical information provided by the researcher and a **Record Copy Request** where researchers with valid record citations (USCIS file numbers), gained through a USCIS Genealogy Program index search or through independent research, may request copies of historical immigration and naturalization records. Questions about the USCIS Genealogy Program may be sent to Genealogy.USCIS@dhs.gov. For more information, see <http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=d21f3711ca5ca110VgnVCM1000004718190aRCRD&vgnnextchannel=d21f3711ca5ca110VgnVCM1000004718190aRCRD>.

Guide to Naturalization contains information about the naturalization process, laws and regulations. See <http://www.uscis.gov/files/article/M-476.pdf>.

If You Have the Right to Work, Don't Let Anyone Take it Away Poster is a poster with Department of Justice information regarding discrimination in the workplace. See <http://www.uscis.gov/files/natedocuments/e-verify-swa-right-to-work.pdf>.

USCIS Information for Employers and Employees on the employment authorization verification process and the immigration petition process. See <http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=ff1d83453d4a3210VgnVCM100000b92ca60aRCRD&vgnnextchannel=ff1d83453d4a3210VgnVCM100000b92ca60aRCRD>.

[83453d4a3210VgnVCM100000b92ca60aRCRD](http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnnextoid=83453d4a3210VgnVCM100000b92ca60aRCRD). For more information contact Public.Engagement@dhs.gov.

USCIS Office of Public Engagement (OPE) seeks to focus on open, candid, and constructive collaboration with community stakeholders at all levels. OPE coordinates and directs USCIS-wide dialogue with external stakeholders to advance the Agency's vision of customer inclusiveness by actively engaging stakeholders to ensure information flow and to institutionalize a mechanism whereby their input will be considered in the process of policy formulation, priority calibration, and assessment of organizational performance. The goal of the office is to provide information and invite feedback to inform our work. See the Outreach tab at <http://www.uscis.gov>. For more information contact Public.Engagement@dhs.gov.

USCIS Resources USCIS offers a variety of resources for our customers, the organizations that serve them and the public. USCIS is committed to supporting the resource needs of stakeholders, including Congress, community-based organizations and legal practitioners, and educators and researchers. Resources include customer guides, videos, citizenship toolkits, an immigration law glossary, reports and studies, civics and citizenship education resources, and a historical library. See the "Resources" section at <http://www.uscis.gov>. For more information contact Public.Engagement@dhs.gov.

Welcome to the United States: A Guide for New Immigrants With this landmark publication, the federal government reaches out to new immigrants with essential orientation materials needed to adjust to life in America. It also contains basic history and civics information that introduces new immigrants to U.S. history and the system of government. See <http://www.uscis.gov/files/natedocuments/M-618.pdf>.

Citizenship and Immigration Services Ombudsman (CIS Ombudsman)

The CIS Ombudsman is a separate office within the Department of Homeland Security dedicated to improved national security, efficiency, and customer service in the immigration benefits process. The CIS Ombudsman provides recommendations for resolving individual and employer problems with the United States Citizenship and Immigration Services (USCIS). The CIS Ombudsman assists individuals and employers in resolving problems with USCIS; identifies areas in which individuals and employers have problems in dealing with USCIS; and proposes changes to mitigate identified problems. Please note that the CIS Ombudsman is not part of USCIS. The CIS Ombudsman is dedicated to open and accessible communication with both individuals and employers and not only welcomes, but encourages your comments. Comments, examples, and suggestions may be sent to the Ombudsman at cisombudsman@dhs.gov. www.dhs.gov/cisombudsman

CIS Ombudsman Annual Reports to Congress By June 30 of each calendar year, the Annual Report is delivered to the House and Senate Committees on the Judiciary without any prior comment or amendment from any administrative agency official including: the Secretary, Deputy Secretary, or Director of USCIS. The Ombudsman's annual reports focus on identifying systemic issues that cause delay in granting immigration benefits as well as pervasive and serious problems faced by individuals and employers in their interactions with USCIS. The Annual Report contains cumulative analysis and recommendations and provides details on activities undertaken by the Ombudsman during the reporting period of June 1 through May 31 of the calendar year. See http://www.dhs.gov/about/structure/gc_1183996985695.shtm.

CIS Ombudsman's Community Call-In Teleconference Series provides an opportunity to discuss your interactions with U.S. Citizenship and Immigration Services (USCIS) and share your comments, thoughts, and suggestions as well as any issues of concern. For more information, including questions and answers from previous teleconference and a schedule of upcoming calls, visit http://www.dhs.gov/about/structure/gc_1171038701035.shtm. To participate in these calls, please RSVP to cisombudsman.publicaffairs@dhs.gov specifying which call you would like to join. Participants will receive a return e-mail with the call-in information.

CIS Ombudsman Updates share information on current trends and issues to assist individuals and employers in resolving problems with USCIS. See http://www.dhs.gov/about/structure/gc_1221837986181.shtm.

Previous Recommendations by the CIS Ombudsman are intended to ensure national security and the integrity of

the legal immigration system, increase efficiencies in administering citizenship and immigration services, and improve customer service in the rendering of citizenship and immigration services. Problems reported to the Ombudsman by individuals and employers (during the Ombudsman's travels), discussions with immigration stakeholders, and suggestions of USCIS employees themselves provide the basis for many of the recommendations. To view the recommendations as well as USCIS responses, see http://www.dhs.gov/files/programs/editorial_0769.shtm.

Send Your Recommendations to the CIS Ombudsman

Your recommendations are accepted and encouraged. The Ombudsman is dedicated to identifying systemic problems in the immigration benefits process and preparing recommendations for submission to U.S. Citizenship and Immigration Services (USCIS) for process changes. The Ombudsman believes that process change recommendations from individuals like you represent one of the best sources for identifying systemic problems in the immigration benefits process. Ideally, your recommendations for process changes should not only identify the problem you are experiencing, but should also contain a proposed solution that will not only benefit your individual case, but others who may be experiencing the same problem as well. Send your comments, examples, and suggestions to cisombudsman@dhs.gov or to the following mailing address:

Citizenship and Immigration Services Ombudsman
ATTN: Recommendations
United States Department of Homeland Security
Mail Stop 1225
Washington, D.C. 20528-1225

Submit a Case Problem to the CIS Ombudsman If you are experiencing problems during the adjudication of an immigration benefit with U.S. Citizenship and Immigration Services (USCIS), you can submit a case problem to the CIS Ombudsman using DHS Form 7001 (CIS Ombudsman Case Problem Submission Form). To submit a case problem on behalf of somebody other than yourself, you should ensure that the person the case problem is about (the applicant for a USCIS immigration benefit, or the petitioner who seeks to obtain an immigration benefit for a third party) consents to your inquiry (see Submitting a Case Problem using DHS Form 7001: Section 15 Consent). See http://www.dhs.gov/files/programs/editorial_0497.shtm.

U.S. Coast Guard (USCG)

For over two centuries the U.S. Coast Guard has safeguarded our Nation's maritime interests in the heartland, in the ports, at sea, and around the globe. We protect the maritime economy and the environment, we defend our maritime borders, and we save those in peril. This history has forged our character and purpose as America's Maritime Guardian — *Always Ready* for all hazards and all threats. www.uscg.mil

America's Waterways Watch is a combined effort of the U.S. Coast Guard and its Reserve and Auxiliary components to enlist the active participation of those who live, work or play around America's waterfront areas. For more information, contact aww@uscg.mil visit <http://www.americaswaterwaywatch.us>. To report suspicious activity call 877-24WATCH (877-249-2824).

U.S. Coast Guard Auxiliary is the uniformed volunteer component of the United States Coast Guard. Created by an Act of Congress in 1939, the Auxiliary directly supports the Coast Guard in all missions, except military and law enforcement actions. The Auxiliary conducts safety patrols on local waterways, assist the Coast Guard with homeland security duties, teach boating safety classes, conduct free vessel safety checks for the public, as well as many other activities. The Auxiliary has members in all 50 states, Puerto Rico, the Virgin Islands, American Samoa and Guam. For more information, visit <http://www.cgaux.org/>.

U.S. Coast Guard Maritime Information eXchange ("CGMIX") makes U.S. Coast Guard (USCG) maritime information available on the public internet in the form of searchable databases. Much of the information on the CGMIX web site comes from the USCG's Marine Information for Safety and Law Enforcement (MISLE) information system. See <http://cgmix.uscg.mil/>.

U.S. Coast Guard Navigation Center provides services for safe, secure, and efficient maritime transportation by delivering: enhanced situational awareness through continuous monitoring and managing of vessel movement system, quality positioning, navigation and timing signals, accurate and timely maritime information services, and system requirements and performing operational oversight of premier navigation services. See <http://www.navcen.uscg.gov/>. For more information use

the e-mail Inquiry located at http://www.navcen.uscg.gov/misc/NIS_contact_us.htm or call (703) 313-5900.

HOMEPORT is an internet repository of detailed information of interest to the Port Community. Specific Homeport Topics Include: Containers, Domestic Vessels (US Flag Vessels), Environmental, Facilities, Incident Management and Preparedness, Investigations (Maritime Casualties and Incidents), Marine Safety, Maritime Domain Awareness (MDA) & Information Sharing (IS), Maritime Security, Merchant Mariners, Port State Control, Ports and Waterways, Regulations/Administrative Adjudications, Strategic Initiatives, USCG Sector (Field Unit) Directory, Vessel Standards, Counter Piracy, International Port Security (IPS) Program, Maritime Transportation Security Act (MTSA), Marine Safety Center, Mariner Credential Verification, and Mariner Credential Application Status. See <http://homeport.uscg.mil>.

USCG National Maritime Center (NMC) issues Merchant Mariner Credentials (MMC) to fully qualified US mariners, approves and audits training programs and courses offered by mariner training organizations throughout the United States, and provides information about merchant mariner records. For more information, see <http://www.uscg.mil/nmc> or contact NMC Customer Service Center: (888) IASKNMC (1-888-427-5662).

National Vessel Movement Center (NVMC) provides the maritime industry with a method to submit electronically a Notice of Arrival and a Notice of Departure, which fulfills USCG and the Customs and Border Protection's (CBP) requirements. See <http://www.nvmc.uscg.gov> or contact the NVMC sans@nvmc.uscg.gov, (800) 708-9823 or (304) 264-2502.

Vessel Documentation (for US Flag Vessels) The National Vessel Documentation Center facilitates maritime

commerce and the availability of financing while protecting economic privileges of United States citizens through the enforcement of regulations, and provides a register of vessels available in time of war or emergency to defend and protect the United States of America. See <http://www.uscg.mil/hq/cg5/nvdc/>. For more information call (800) 799-8362 or (304) 271-2400 (7:30 a.m. to 5:00 p.m. Eastern Time).

U.S. Customs and Border Protection (CBP)

CBP is one of the Department of Homeland Security's largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the U.S. It also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws. www.cbp.gov

CBP Publications and Guidance

AIRBUST program provides awareness of suspicious small aircraft and behaviors. The AIRBUST Card is a pocket-sized laminated card displaying the phone number that people can call to report suspicious or low flying aircraft, 1-866-AIRBUST (1-866-247-2878). This number rings directly to the CBP Air and Marine Operations Center (AMOC) Floor and anyone can use the phone number for reporting. On one side of the card are drawings of single- and twin-engine aircraft often used to transport contraband. The opposite side of the card lists helpful information to note when reporting. The AIRBUST poster, CBP Publication 0000-0716, is an 8.5x11 poster with the 1-866-AIRBUST (1-866-247-2878) phone number. It also lists four general items of interest that can tip off a general aviation airport employee or law enforcement official that a particular aircraft or pilot may be involved in illicit activity. For more information, or to order these publications, call 951-656-8000.

CBP Directives Pertaining to Intellectual Property Rights are policy guidance documents that explain CBP's legal authority and policies implementing certain laws and regulations. They are distributed to CBP personnel to clarify implementation procedures and are made available to the public to explain CBP's policies. To access these directives, please visit <http://www.cbp.gov/xp/cgov/trade/legal/directives/>. For additional information, or e-mail CBP IPR Policy and Programs at iprpolicyprograms@dhs.gov.

Entry Level Test Study Guides for CBP Job Applicants CBP provides study guides and test preparation materials for applicants to several core occupations. Applicants for Border Patrol Agent, Customs and Border Protection Officer & Agriculture Specialist, and Intelligence Research Specialist positions will find these resources beneficial during their application process. These resources provide

test taking hints, helpful information on how to prepare for a test, and practice tests. For more information, please visit: http://cbp.gov/xp/cgov/careers/study_guides/.

Intellectual Property Rights (IPR) Seizure Statistics CBP maintains statistics on IPR seizures made by the Department of Homeland Security (CBP and ICE) at: http://www.cbp.gov/xp/cgov/trade/priority_trade/ipr/pubs/seizure/. For any specific questions or concerns, please contact CBP by e-mail at: iprpolicyprograms@dhs.gov or ipr.helpdesk@dhs.gov.

U.S. Border Patrol Checkpoints Brochure provides information for the public about Border Patrol checkpoints available at: http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/border/border_patrol/bp_checkpoints.ctt/bp_checkpoints.pdf.

CBP Alerts and Newsletters

Informed Compliance Publications are available on a specific trade issue, which summarizes practical information for the trade community to better understand their obligations under Customs and related laws. These publications are available at: <http://www.cbp.gov/xp/cgov/trade/legal/>.

U.S. Border Patrol Blotter, Newsletter, and Alerts compiles the latest information on noteworthy occurrences documenting apprehensions of criminals, seizures of illegal drugs, rescue missions, and many other Border Patrol success stories from around the country. These highlights can be found at: http://cbp.gov/xp/cgov/border_security/border_patrol/weekly_blotter/. The border patrol also publishes a newsletter: http://www.cbp.gov/xp/cgov/newsroom/publications/frontline_magazine/ and alerts: <http://www.cbp.gov/xp/cgov/newsroom/advisories/>.

CBP Technical Assistance

1-800 BE ALERT The public is welcome to actively participate in helping to secure our nation's borders by reporting suspicious activity to the U.S. Border Patrol via a toll free telephone reporting system: "BE ALERT". To report suspicious activity: Call (800) BE ALERT or (800) 232-5378. For more information on U.S. Border Patrol Checkpoints: Call (877) 227-5511. International Callers Call +1 (703) 526-4200.

Automated Commercial Environment (ACE) National Help Desk provides customer technical support services 24 hours a day, seven days a week, including information about ACE Secure Data Portal account access, account management, and report generation. The ACE Help Desk is the first point of contact for all ACE users experiencing system difficulties. To reach the ACE Help Desk, please call: (800) 927-8729.

Cargo Systems Messaging Service (CSMS) is an active, live, searchable database of messages that are of interest to Automatic Broker Interface (ABI) filers, Automated Commercial Environment (ACE) event participants, ACE Portal Accounts users, ACE reports users, air carriers, ocean carriers, Periodic Monthly Statement participants, and rail and truck carriers. CSMS is augmented by an e-mail subscription service, which is available at: https://service.govdelivery.com/service/multi_subscribe.html?code=USDHSCBP&custom_id=938&origin=https://apps.cbp.gov/csms.

CBP Client Representatives are the first points of contact for importers, exporters, transportation providers, and brokers wishing to automate any of their Customs processes. Client Representatives are the contact point for all system-related problems and questions from trade partners. For more information about client reps and the services offered to members of the trade, please visit:

http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/client_reps.xml or contact the CBP Client Representative Office at: (571) 468-5000.

CBP INFO Center Self Service Q&A Database is a searchable database with over 600 answers to commonly (and not so commonly) asked questions about CBP programs, requirements, and procedures. If visitors to the site are unable to find an answer to their question, they may also submit an inquiry or complaint for personal assistance. To use the searchable database, please visit https://help.cbp.gov/cgi-bin/customs.cfg/php/enduser/home.php?p_sid=YeyXThOj. Or call the CBP INFO Center at (877) CBP-5511 or (703) 526-4200.

Entry Process into United States CBP welcomes more than 1.1 million international travelers into the United States at land, air, and seaports on an average day. U.S. citizens and international visitors should consult the following publications and factsheets for information to simplify their entry into the United States. For information about international travel, visit <http://www.cbp.gov/xp/cgov/travel/>. For more information, please contact the CBP Information Center at (877) 227-5511.

Importing into the United States CBP will facilitate about \$2 trillion in legitimate trade this year while enforcing U.S. trade laws that protect the economy and the health and safety of the American people. We accomplish this through close partnerships with the trade community, other government agencies, and foreign governments. See <http://www.cbp.gov/linkhandler/cgov/newsroom/publications/trade/iius.ctt/iius.pdf>. For information about CBP Trade programs, visit <http://www.cbp.gov/xp/cgov/trade/>.

CBP Programs and services

Automated Commercial Environment (ACE) is the United States' commercial trade processing system designed to automate border processing, to enhance border security, and to foster our Nation's economic security through lawful international trade and travel. ACE will eventually replace the current import processing system for CBP, the Automated Commercial System (ACS). ACE is part of a

multi-year CBP modernization effort and is being deployed in phases. For more information about ACE, please visit <http://www.cbp.gov/xp/cgov/trade/automated/modernization/>.

Automated Commercial System (ACS) is a data information system used by CBP to track, control, and process commercial goods imported into the United States. Through the use of Electronic Data Interchange (EDI), ACS facilitates merchandise processing for CBP and the private sector. ACS is accessed through the CBP Automated Broker Interface (ABI) and permits qualified participants to electronically file required import data with CBP. ABI is a voluntary program available to brokers, importers, carriers, port authorities, and independent service centers. For more information about ACS, please visit http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/acs/. For additional information specific to ABI, please contact the CBP Client Representative Office at (571) 468-5000.

Automated Export System (AES) is the electronic way to file export declarations and ocean manifest information with CBP. For more information about AES, including technical documentation, software vendors, and other items of interest, please visit <http://www.cbp.gov/xp/cgov/trade/automated/aes/>.

Automated Manifest System (AMS) is a multi-modular cargo inventory control and release notification system. AMS facilitates the movement and delivery of cargo by multiple modes of transportation. Carriers, port authorities, service bureaus, freight forwarders, and container freight stations can participate in AMS. Sea AMS allows participants to transmit manifest data electronically prior to vessel arrival. CBP can then determine in advance whether the merchandise merits examination or immediate release. Air AMS allows carriers to obtain notifications of releases, in-bond authorizations, general order, permit to proceed, and local transfer authorization upon flight departure or arrival from the last foreign port. Rail AMS allows rail carriers to electronically transmit information to CBP. When all bills on a train are assigned, the rail carrier transmits a list of the bills and containers in standing car order. For more information about AMS, please visit

http://www.cbp.gov/xp/cgov/trade/automated/automated_systems/acs/acs_ams.xmlACS.

Carrier Liaison Program (CLP) This program provides standardized training and assistance to international air carriers related to admissibility and fraudulent document detection in order to encourage carrier compliance with U.S. Immigration Laws. For more information about CLP, please visit http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/clp/, e-mail CLP@dhs.gov, or call (202) 344-3440.

Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary government-business initiative to strengthen and improve the overall international supply chain and U.S. border security. C-TPAT recognizes that CBP can provide the highest level of cargo security only through close cooperation with the ultimate owners of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers. Through this initiative, CBP is asking businesses to ensure the integrity of their security practices, communicate, and verify the security guidelines of their business partners within the supply chain. For more information, or to apply online, please visit http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/. For questions or concerns, please contact the CBP Industry Partnership Program at (202) 344-1180, or by fax (202) 344-2626 or e-mail, industry.partnership@dhs.gov.

eAllegations provides concerned members of the public a means to confidentially report suspected trade violations to CBP. For more information, or to initiate an investigation, please visit <https://apps.cbp.gov/eallegations/>, or contact the Commercial Targeting and Enforcement, Office of International Trade at: (800) BE-ALERT.

Electronic System for Travel Authorization (ESTA) is a free, automated system that determines the eligibility of visitors to travel to the U.S. under the Visa Waiver Program. The ESTA application collects the same information collected on Form I-94W. ESTA applications may be submitted at any time prior to travel, though it is recommended travelers apply when they begin preparing travel plans. To apply online, please visit:

<https://esta.cbp.dhs.gov/>. For additional information, please call: (202) 344-3710.

Global Entry is a pilot program managed by CBP, which allows pre-approved, low-risk travelers, expedited clearance upon arrival into the United States. Although this program is intended for “frequent travelers” who make several international trips per year, there is no minimum number of trips an applicant must make in order to qualify. For more information about Global Entry, please visit: http://www.cbp.gov/xp/cgov/travel/trusted_traveler/global_entry/ or apply online at: <https://goes-app.cbp.dhs.gov/>. For additional questions or concerns, please contact CBP by e-mail, cbp.goes.support@dhs.gov, or by phone, (866) 530-4172.

Importer Self-Assessment Program (ISA) is a voluntary approach to trade compliance. The program provides the opportunity for importers to assume responsibility for monitoring their own compliance in exchange for benefits. Public information regarding this program, including frequently asked questions, policy information, best practices, and requirements can be found at http://www.cbp.gov/xp/cgov/trade/trade_programs/importer_self_assessment/.

Importer Self Assessment – Product Safety Pilot (ISA-PS) CBP and the Consumer Product Safety Commission (CPSC) have a strong history of partnership in combating unsafe imports and have worked together on significant product recalls. CBP announces a new partnership with CPSC and importers to prevent unsafe imports from entering the United States. For more information, please visit http://www.cbp.gov/xp/cgov/trade/trade_programs/importer_self_assessment/isa_safety_pilot.xml.

Intellectual Property Rights (IPR) Enforcement: A Priority Trade Issue The trade in counterfeit and pirated goods threatens America’s innovation economy, the competitiveness of our businesses, the livelihoods of U.S. workers, national security, and the health and safety of consumers. The trade in these illegitimate goods is associated with smuggling and other criminal activities, and often funds criminal enterprises. For more information, please visit http://www.cbp.gov/xp/cgov/trade/priority_trade/ipr/.

Intellectual Property Rights (IPR) e-Recordation and IPR Search The first step in obtaining IPR protection by CBP is to record validly registered trademarks and copyrights with CBP through the Intellectual Property Rights e-Recordation (IPRR) online system. CBP’s on-line recordation allows intellectual property owners to electronically record their trademarks and copyrights with CBP, and makes IPR recordation information readily available to CBP personnel, facilitating IPR seizures by CBP. CBP uses recordation information to actively monitor shipments and prevent the importation or exportation of infringing goods. For more information please visit: <http://iprs.cbp.gov/>. For additional information, please e-mail at hqiprbranch@dhs.gov or call (202) 325-0020.

Intellectual Property Rights (IPR) Continuous Sample Bond CBP established a new continuous bond option for Intellectual Property Rights (IPR) sample bonds. Under CBP regulations, CBP may provide samples of certain merchandise suspected of bearing infringing trademarks, trade names, or copyrights of imports seized for such violations, to trademark, trade name, and copyright owners. A sample bond template can be downloaded at: http://www.cbp.gov/xp/cgov/trade/trade_programs/bond_s/ipr_bonds_samples/. For additional information, please contact CBP’s Revenue Division, Office of Finance by e-mail at: cbp.bondquestions@dhs.gov, or by phone at (317) 614-4880 or by fax at (317) 614-4517.

Intellectual Property Rights (IPR) Help Desk can provide information and assistance for a range of IPR related issues including: IPR border enforcement procedures, reporting allegations of IPR infringement, assistance for owners of recorded IPRs to develop product identification training materials, and to assist officers at ports of entry in identifying IPR infringing goods. To reach the CBP IPR Help Desk, please call at (562) 980-3119 ext. 252, or e-mail at ipr.helpdesk@dhs.gov.

Intellectual Property Rights (IPR) and Restricted Merchandise Branch oversees the IPR recordation program and provides IPR infringement determinations and rulings. For legal questions about CBP’s IPR recordation program, please e-mail at: hqiprbranch@dhs.gov, or call (202) 325-0020.

Intellectual Property Rights (IPR) U.S. – EU Joint Brochure and Web Toolkit for Trademark, Copyright Owners To promote strong and effective border enforcement of Intellectual Property Rights, CBP and Customs Officials in the European Union have jointly developed a brochure and Web toolkit to assist intellectual property owners in working with Customs to enforce their rights and to prepare information to help U.S. and E.U. Customs Agencies determine whether goods are counterfeit or pirated. To access the Protecting Intellectual Property Rights at Our Borders brochure, please visit: http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/pubs/cpg_final_090306.ctt/cpg_final_090306.pdf. To access the Toolkit, please visit: http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/cpg_final_090306.ctt/cpg_final_090306.pdf. For additional questions or concerns, please contact the IPR Help Desk by e-mail, ipr.helpdesk@dhs.gov or phone, (562) 980-3119 ext. 252.

CBP Laboratories and Scientific Services coordinates technical and scientific support to all CBP trade and border protection activities. For more information, please visit http://www.cbp.gov/xp/cgov/trade/automated/labs_scientific_svcs/.

National Gang Intelligence Center is a multi-agency effort that integrates the gang intelligence assets of Federal, State, and local law enforcement entities to serve as a centralized intelligence resource for gang information and analytical support. The mission of the NGIC is to support law enforcement agencies through timely and accurate information sharing and strategic/tactical analysis of Federal, State, and Local law enforcement intelligence focusing on the growth, migration, criminal activity, and association of gangs that pose a significant threat to communities throughout the United States. The NGIC concentrates on gangs operating on a national level that demonstrate criminal connectivity between sets and common identifiers and goals. Because many violent gangs do not operate on a national level, the NGIC will also focus on regional-level gangs. The NGIC produces intelligence assessments, intelligence bulletins, joint agency intelligence products, and other non-standard intelligence products for our customers. For more information, please contact the NGIC, (703) 414-8600.

Private Aircraft Travel Entry Programs The *Advance Information on Private Aircraft Arriving and Departing the United States* final rule requires that pilots of private aircraft submit advance notice and manifest data on all persons traveling on board. Required information must be submitted to CBP via an approved electronic data interchange system no later than 60 minutes prior to departure. The CBP.gov web site offers information about current CBP policies, regulations, documentary requirements, and ports of entry. For more information, please visit http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/apis/. For additional questions or concerns, please contact CBP via e-mail at Private.Aircraft.Support@dhs.gov.

Secure Freight Initiative (SFI) and Importer Security Filing and additional carrier requirements (10+2) The Secure Freight Initiative (SFI), through partnerships with foreign governments, terminal operators, and carriers enhances DHS's capability to better assess the security of U.S.-bound maritime containers by scanning them for nuclear and other radioactive materials before they are laden on vessels bound for the United States. For the domestic CBP officers, SFI provides additional data points that are used in conjunction with advanced data, such as 24-hour rule information, 10+2, Customs-Trade Partnership Against Terrorism information, and the Automated Targeting System to assess the risk of each container coming to the United States. For more information, please visit http://www.cbp.gov/xp/cgov/trade/cargo_security/secure_freight_initiative/, or e-mail questions to securefreightinitiative@dhs.gov.

CBP Trade Outreach The Office of Trade Relations supports communications between CBP and the private sector, and provides information for new importers, exporters and small businesses. For more information, please visit http://www.cbp.gov/xp/cgov/trade/trade_outreach/.

Trusted Traveler Programs (TTP) include FAST-Driver, NEXUS, SENTRI, and Global Entry. TTP provide expedited travel for pre-approved, low risk travelers through dedicated lanes and kiosks (NEXUS at Canadian Pre-Clearance ports). Program members received RFID

embedded cards that facilitate border processing by confirming membership, identity, and running law enforcement checks. For more information about a CBP's trusted traveler programs, please visit http://www.cbp.gov/xp/cgov/travel/trusted_traveler/.

Visa Waiver Program (VWP) enables citizens and nationals from 34 countries to travel to and enter the United States for business or visitor purposes for up to 90 days without obtaining a visa. For more information about the Visa Waiver Program, please visit http://www.cbp.gov/xp/cgov/travel/id_visa/business_pleasure/vwp/.

Western Hemisphere Travel Initiative (WHTI) requires all travelers, U.S. citizens and foreign nationals, to present a passport or other acceptable documents that denote identity and citizenship when entering the United States. For more information about WHTI, please visit: <http://www.getyouhome.gov/>, or contact CBP Customer Service at (877)227-5511 or (703) 526-4200, TDD: (866) 880-6582.

Cybersecurity and Communications (CS&C)

The Office of Cybersecurity and Communications (CS&C) is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm

CS&C Training and Education

Control Systems Security Program (CSSP) Instructor-Lead Cybersecurity Training is provided through an introductory course for IT professionals or a 5-day advanced course which includes hands-on instruction in an actual control system environment. For more information, see http://www.us-cert.gov/control_systems/cstraining.html, or contact CSSP@dhs.gov.

Cyber Education and Workforce Development Program (CEWD) As cyber threats and their sophistication increase, the demand for qualified IT security professionals increases as well. In response, the National Cyber Security Division's Cyber Education and Workforce Development program (CEWD) developed the IT Security Essential Body of Knowledge (EBK). The IT Security EBK is an umbrella framework that links competencies and functional perspectives to IT security roles to accurately reflect a national perspective. See <http://www.us-cert.gov/ITSecurityEBK/>.

CS&C Publications and Guidance

Cybersecurity Information Products and Recommended Practices provide current cybersecurity information resources and recommend security practices to help industry understand emerging control systems cyber security issues and mitigate vulnerabilities. This information will help users reduce their exposure and susceptibility to cyber attacks and exploits. For a complete list and access to cybersecurity information products, visit http://www.us-cert.gov/control_systems/csdocuments.html. An interactive site with recommended practices for control system networks can be found at <http://csr.p.inl.gov/>. For more information, contact CSSP@dhs.gov.

Cybersecurity Public Trends and Analysis Report provides awareness of the cyber security trends as observed by The U.S. Computer Emergency Readiness Team (US-CERT). The analysis in this report is based on incident information that has been reported to US-CERT, incidents identified by US-CERT, and public/private sector information identified when correlating and analyzing the data. For more information, see http://www.us-cert.gov/reading_room/index.html#news. Contact US-CERT at info@us-cert.gov, (888) 282-0870

Cyber Security Evaluation Tool (CSET) is a desktop software tool that guides users through a step-by-step process for assessing the cyber security posture of their industrial control system and enterprise information technology networks. CSET is available in DVD format. To learn more, visit http://www.us-cert.gov/control_systems/satool.html. To obtain a DVD copy of CSET, send an e-mail with your mailing address to CSET@dhs.gov.

Emergency Communications Guidance Documents and Methodologies The DHS Office of Emergency Communications develops stakeholder-driven guidance documents and methodologies to support emergency responders across the Nation as they plan for and implement emergency communications initiatives. These resources identify and promote best practices on improving statewide governance, developing standard operating procedures, managing technology, supporting training and exercises, and encouraging usage of interoperable communications, among other topics. Each is available publicly and is updated as needed. Examples include: *Establishing Governance to Achieve Statewide Communications Interoperability* and the *Formal Agreement and Standard Operating Procedure Template Suite*. For more information, contact the Office of Emergency Communications at oc@hq.dhs.gov or visit <http://www.safecomprogram.gov>.

Industrial Control System Cybersecurity Standards and References provide an extensive collection of cybersecurity standards and reference materials as a ready-resource for the industrial control system stakeholder community. The collection provides a one-stop location for accessing papers, reports, references, and standards associated with industrial control system cybersecurity. To view the collection, visit http://www.us-cert.gov/control_systems/cstandards.html. For more information, contact CSSP@dhs.gov.

Information Technology Sector Risk Assessment (ITSRA) The National Cyber Security Division (NCSA), in partnership with public and private sector partners from the IT Sector Coordinating Council (IT SCC) and the IT Government Coordinating Council (IT GCC), released the baseline ITSRA in 2009. The ITSRA provides an all-hazards risk profile that public and private IT Sector partners can use to inform resource allocation for research and development and other protective measures which enhance the security and resiliency of the critical IT Sector functions. By increasing the awareness of risks across the public and private sectors, the Baseline Risk Assessment is the foundation for ongoing national-level collaboration to enhance the security and resiliency of the critical IT Sector functions. See http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf. For more information, contact ncsd_cipcs@hq.dhs.gov.

Information Technology Sector Specific Plan (IT SSP) the National Cyber Security Division (NCSA), in partnership with private sector members of the IT Sector, has developed the IT SSP to outline the IT Sector security partners' joint implementation of the NIPP risk management framework. It describes an approach for identifying, assessing, prioritizing, and protecting critical IT Sector functions, establishing shared IT Sector goals and objectives, and aligning initiatives to meet them. To view the IT SSP, visit

http://www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf. For more information, contact ncsd_cipcs@hq.dhs.gov.

National Emergency Communications Plan (NECP) is a strategic plan that sets goals and identifies key national priorities to enhance governance, planning, technology, training and exercises, and disaster communications capabilities. The NECP establishes specific national priorities to help State and local jurisdictions improve communications interoperability by adopting a series of goals and milestones that measure interoperability achievements over a period of years beginning in 2008, and ending in 2013. In order to successfully implement the NECP, increased collaboration between the public and private sector will be needed. As a result, the plan establishes specific initiatives and milestones to increase such collaboration. For more information, see http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf or contact the Office of Emergency Communications, oc@hq.dhs.gov.

National Interoperability Field Operations Guide (NIFOG) is a technical reference for radio technicians responsible for radios that will be used in disaster response applications, and for emergency communications planners. The NIFOG includes rules and regulations for use of nationwide and other interoperability channels, frequencies and channel names, and other reference material, formatted as a pocket-sized guide for radio technicians to carry with them. The NIFOG can be accessed online at <http://www.npstc.org/psdocs.jsp#nifog>. For more information, contact the Office of Emergency Communications, oc@hq.dhs.gov.

SAFECOM Guidance for Federal Grant Programs The Department of Homeland Security Office of Emergency Communications, in coordination with the Office for Interoperability and Compatibility, develops the annual *SAFECOM Guidance for Federal Grant Programs*. Although SAFECOM is not a grant-making body, the guidance outlines recommended allowable costs and applications requirements for Federal grant programs providing funding for interoperable emergency communications. The guidance is intended to ensure that Federal grant funding for interoperable communications aligns with national goals and objectives and ensures alignment of

State, local, and tribal investment of Federal grant funding to statewide and national goals and objectives. See http://www.safecomprogram.gov/NR/rdonlyres/31A870C0-0C9D-4C29-86F8-147D61AF25CF/0/FY_2010_SAFECOM_Recommended_Guidance_111809_Final.pdf. For more information, contact the Office of Emergency Communications at oc@hq.dhs.gov.

U.S. Computer Emergency Readiness Team (US-CERT) Monthly Activity Summary summarizes general activity as well as updates made to the National Cyber Alert System each month. This includes current activity updates, technical and non-technical alerts, bulletins, and tips, in addition to other newsworthy events or highlights. See http://www.us-cert.gov/reading_room/index.html#news, contact US-CERT at info@us-cert.gov, (888) 282-0870.

U.S. Computer Emergency Readiness Team (US-CERT) Security Publications provide subscribers with free, timely information on cybersecurity vulnerabilities, the potential impact of those vulnerabilities, and action required to mitigate the vulnerability and secure their computer systems. See http://www.us-cert.gov/reading_room, contact US-CERT at info@us-cert.gov, (888) 282-0870.

U.S. Computer Emergency Readiness Team (US-CERT) Vulnerability Notes Database includes technical descriptions of the vulnerability, as well as the impact, solutions and workarounds, and lists of affected vendors. See <http://www.kb.cert.org/vuls>, contact US-CERT at info@us-cert.gov, (888) 282-0870.

CS&C Alerts and Newsletters

Current Cybersecurity Activity is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to the US-CERT. See <http://www.us-cert.gov/current/>, contact US-CERT at info@us-cert.gov, (888) 282-0870.

Critical Infrastructure Information Notices are intended to provide warning to critical infrastructure owners and operators when a particular cyber event or activity has the potential to impact critical infrastructure computing networks. This document is distributed only to those

parties who have a valid “need to know,” a *direct role in securing networks or systems that enable or support U.S. critical infrastructures*. Access is limited to a secure portal (<https://portal.us-cert.gov>) and controlled distribution list. For more information, contact the US-CERT Secure Operations Center at soc@us-cert.gov; (888) 282-0870.

National Cyber Alert System offers a variety of information for users with varied technical expertise including Technical Cybersecurity Alerts and Bulletins or more general-interest pieces such as Cybersecurity Alerts and Tips on a variety of cyber-related topics. See <http://www.uscert.gov/cas/alldocs.html>. Contact US-CERT at info@us-cert.gov, (888) 282-0870.

CS&C Technical Assistance

U. S. Computer Emergency Readiness Team (US-CERT) Operations Center Report cybersecurity incidents (including unexplained network failures), the discovery of malicious code, and vulnerability information at <https://forms.us-cert.gov/report/>. Contact the US-CERT Operations Center at soc@us-cert.gov; (888) 282-0870.

Cyber Resiliency Review (CRR) is an assessment offered by the Cyber Security Evaluation Program to measure and enhance the implementation of key cybersecurity capacities and capabilities of critical infrastructure and key resources (CIKR). The purpose of the CRR is to gather information regarding cybersecurity performance from specific CIKR in order to gain an understanding of the relationships and impacts of CIKR performance in protecting critical infrastructure operations. The CRR serves as a repeatable cyber review, while allowing for an evaluation of enterprise-specific cybersecurity capabilities. The results can be used to evaluate a provider independent of other assessments, used with regional studies to build a common perspective on resiliency, and used to examine systems-of-systems (i.e., large and diverse operating and organizing models). The key goal of the CRR is to ensure that core process-based capabilities exist, are measurable, and are meaningful as predictors for an organization’s ability to manage cyber risk to national critical infrastructure. For more information about the CRR, contact the CSEP program at CSE@dhs.gov.

Cyber Security Advisors (CSAs) act as principal field liaisons in cybersecurity and provide a Federal resource to regions, communities, and businesses. Their primary goal is to assist in the protection of cyber components essential within the Nation's critical infrastructure and key resources (CIKR). Equally important is their role in supporting cybersecurity risk management efforts at the State and local homeland security initiatives. CSAs will work with established programs in State and local areas, such as Protective Security Advisors, FEMA emergency management personnel, and fusion center personnel. For more information, contact the program at CSE@dhs.gov.

Cyber Security Evaluation Program (CSEP) conducts voluntary cybersecurity assessments across all 18 CIKR Sectors, within state governments, and for large urban areas. CSEP affords CIKR sector participants a portfolio of assessment tools, techniques, and analytics, ranging from those that can be self-applied to those that require expert facilitation or mentoring outreach. The CSEP, in alignment with the DHS National Infrastructure Protection Plan (NIPP), works closely with and coordinates efforts with internal and external stakeholders to measure key performances in cybersecurity management. The Cyber Resiliency Review is being deployed across all 18 Critical Infrastructure Sectors (as denoted by DHS), state, local, tribal, and territorial governments. For more information, visit www.dhs.gov/xabout/structure/editorial_0839.shtm or contact the program at CSE@dhs.gov.

Cybersecurity Vulnerability Assessments through the Control Systems Security Program (CSSP) provide on-site support to critical infrastructure asset owners by assisting them to perform a security self-assessment of their enterprise and control system networks against industry accepted standards, policies, and procedures. To request on-site assistance, asset owners may e-mail CSSP@dhs.gov.

Industrial Control Systems Technology Assessments provide a testing environment to conduct baseline security assessments on industrial control systems, network architectures, software, and control system components. These assessments include testing for common vulnerabilities and conducting vulnerability mitigation

analysis to verify the effectiveness of applied security measures. To learn more about ICS testing capabilities and opportunities, e-mail CSSP@dhs.gov.

CS&C Programs and Services

Control Systems Security Program (CSSP) reduces industrial control system risks within and across all critical infrastructure and key resource sectors. CSSP coordinates cybersecurity efforts among Federal, State, local, and Tribal governments, as well as industrial control system owners, operators, and vendors. CSSP provides many products and services that assist the industrial control system stakeholder community to improve their cybersecurity posture and implement risk mitigation strategies. To learn more about the CSSP, visit http://www.us-cert.gov/control_systems/ or e-mail CSSP@dhs.gov.

Critical Infrastructure Protection – Cyber Security (CIP-CS) leads efforts with public and private sector partners to promote an assured and resilient U.S. cyber infrastructure. Major elements of the CIP-CS program include: managing and strengthening cyber critical infrastructure partnerships with public and private entities in order to effectively implement risk management and cybersecurity strategies, teaming with cyber critical infrastructure partners in the successful implementation of cybersecurity strategies, and promoting effective cyber communications processes with partners that result in a collaborative, coordinated approach to cyber awareness. For more information, contact CIP-CS at cip_cs@dhs.gov.

Global Supply Chain Risk Management (GSCRM) Program provides recommendations to standardize and implement risk management processes for acquiring information and communications technologies (ICT) for the federal government, and processes to reduce the threat of attacks to federal ICT through the supply chain. Your organization can help with this initiative by applying sound security procedures and executing due diligence to provide integrity and assurance through the vendor supply chain. For more information, visit http://www.dhs.gov/files/programs/gc_1234200709381.shtm or contact the Global Supply Chain Program at Kurt.Seidling@hq.dhs.gov.

National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics. For more information, visit <http://nvd.nist.gov/> or contact nvd@nist.gov.

SAFECOM Program is a communications program which provides research, development, testing, and evaluation, guidance, tools, and templates on interoperable communications-related issues to local, Tribal, State, and Federal emergency response agencies. The SAFECOM web site provides members of the emergency response community and other constituents with information and resources to help them meet their communications and interoperability needs. The site offers comprehensive information on topics relevant to emergency response communications and features best practices that have evolved from real-world situations. See <http://www.safecomprogram.gov>, contact SAFECOM@dhs.gov.

Software Assurance Program Software Assurance (SWA) is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. Grounded in the National Strategy to Secure Cyberspace, the Department of Homeland Security's Software Assurance Program spearheads the development of practical guidance and tools and promotes research and development of secure software engineering, examining a range of development issues from new methods that avoid basic programming errors to enterprise systems that remain secure when portions of the system software are compromised. Resources including articles, webinars, podcasts, and tools can be found at the SWA Community Resources and Information Clearinghouse located at <https://buildsecurityin.us-cert.gov/swa/>. For more information, contact software.assurance@dhs.gov.

Federal Emergency Management Agency (FEMA)

FEMA's mission is to support our citizens and first responders to ensure that as a Nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards. www.fema.gov

FEMA Training and Education

Are You Ready? An In-depth Guide to Citizen

Preparedness provides a step-by-step approach to disaster preparedness by walking the reader through how to get informed about local emergency plans, how to identify hazards that affect their local area, and how to develop and maintain an emergency communications plan and disaster supplies kits. Other topics include what to do before, during, and after each hazard type, including Natural Hazards, Hazardous Materials Incidents, Household Chemical Emergencies, Nuclear Power Plant, and Terrorism (including Explosion, Biological, Chemical, Nuclear, and Radiological hazards). For more information visit www.fema.gov/areyouready or call (800) 480-2520 to order materials. Questions regarding the Citizen Corps program can be directed to citizencorps@dhs.gov.

Center for Domestic Preparedness (CDP) offers several programs that are designed for people that have emergency response and healthcare responsibilities, or meet the criteria specified in the web site cited below. CDP offers courses in Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) incident response, toxic agent training, healthcare response for mass casualty incidents, Radiological Emergency Preparedness (REP) Program courses, Field Force Operations, and the National Incident Management System (NIMS). CDP offers integrated training that includes the opportunity to train in the only live agent training facility dedicated to the civilian response community. CDP's healthcare courses include exercises in a training hospital dedicated solely to preparedness and response. CDP offers residential training at its Anniston, Alabama facility and off-campus training throughout the United States. CDP has an integrated training approach that is free of charge to state, local and tribal agencies. Individuals from Federal, International agencies and the private sector are encouraged to attend but, however, must pay a tuition fee for the courses in

addition to their own transportation and lodging fees. For more information, see <http://cdp.dhs.gov/index.html> or call (866) 213-9553.

Community Emergency Response Team (CERT) This program helps train people to be better prepared to respond to emergency situations in their communities. It is a resource for the private sector to use to ensure its employees are prepared for all hazards. When emergencies happen, CERT members can give critical support to first responders, provide immediate assistance to survivors, and organize spontaneous volunteers at a disaster site. CERT members can also help with non-emergency projects that help improve the safety of the community. For more information visit www.citizencorps.gov/cert or contact cert@dhs.gov.

FEMA Emergency Management Institute Independent Study Program The Emergency Management Institute (EMI) offers self-paced courses designed for people who have emergency management responsibilities and for the general public. FEMA's Independent Study Program offers courses that support the nine mission areas identified by the National Preparedness Goal: Incident Management, Operational Planning, Disaster Logistics, Emergency Communications, Service to Disaster Victims, Continuity Programs, Public Disaster Communications, Integrated Preparedness and Hazard Mitigation. For more information on EMI's training courses, please visit <http://training.fema.gov/IS/> or contact us (301) 447-1200.

FEMA Emergency Management Institute Programs The Emergency Management Institute (EMI) offers several programs that are designed for people who have emergency management responsibilities or meet the criteria specified at the web site cited below. The training is free of charge, however, individuals from private sector or contractors to State, local or Tribal governments must pay their own transportation and lodging fees. EMI has an integrated training approach and we encourage individuals

from private sector to participate in our courses. EMI's programs include, but are not limited to the Master Trainer Program, Master Exercise Practitioner Program, Professional Development Series, Applied Practices Series and FEMA's Higher Education Program. For more information, see <http://www.training.fema.gov/Programs/> or call (301) 447-1286.

FEMA Learning Resource Center (LRC) provides current information and resources on fire, emergency management and other all-hazards subjects. With its collection of more than 180,000 books, reports, periodicals, and audiovisual materials, the LRC houses the most extensive collection of fire service literature in the United States. Internet users may access the LRC's Online Public Access Catalog to perform literature searches and download over 17,000 documents. The LRC's collection of books and research reports may also be accessed by requesting interlibrary loan through a local library. For more information visit <http://www.lrc.fema.gov> or contact the program via phone (800) 638-1821 or by e-mail netclrc@dhs.gov.

U.S. Fire Administration's National Fire Academy Training Programs enhance the ability of fire and emergency services and allied professionals to deal more effectively with fire and related emergencies. NFA offers courses in the following subject areas: Arson Mitigation, Emergency Medical Services, Executive Development, Fire Prevention: Management, Fire Prevention: Public Education, Fire Prevention: Technical, Hazardous Materials, Incident Management, Management Science, Planning and Information Management and Training Programs. NFA offers residential training at its Emmitsburg, Maryland facility and off-campus training throughout the United States, as well as online self-study courses free of charge. For more information, see <http://www.usfa.dhs.gov/nfa/index.shtml> or call (301) 447-1000.

First Responder Training & Exercise Integration are delivered in the following formats: Resident – Instructor-led classroom training is provided at a training facility; Mobile – Also referred to as non-resident, mobile training can be performed by FEMA funded instructors at any location; Web-Based – Web-based or ‘online’ training is done via the internet and is often self-paced (no instructor); or Indirect – Indirect training includes training courses taught by instructors (non FEMA or training partner staff) that have completed ‘Train the Trainer’ courses. For more information, visit www.firstrespondertraining.gov or contact the program via phone (800) 368-6498 or e-mail askCSID@dhs.gov.

FEMA Alerts and Newsletters

FEMA Private Sector E-alert The FEMA Private Sector Division, Office of External Affairs, publishes periodic e-alerts providing timely information on topics of interest to private sector entities. The FEMA Private Sector Web Portal aggregates FEMA’s online resources for the private sector. Content includes best practices in public-private partnerships, weekly preparedness tips, links to training opportunities, planning and preparedness resources, information on how to do business with FEMA, and more. For more information visit www.fema.gov/privatesector or sign up for the alert at FEMA-Private-Sector-Web@dhs.gov.

Citizen Corps E-mail Alerts provide weekly Community Preparedness news and events from various departments of the federal government and our national Citizen Corps partners and affiliates. For more information, visit www.citizencorps.gov or sign up for the alert at citizencorps@dhs.gov.

FEMA Publications

FEMA Library is a searchable web-based collection of all publicly accessible FEMA information resources, including thousands of CDs, DVDs, audio tapes, disability resources, posters, displays, brochures, guidance, policy papers, program regulations, guidelines, and forms. Users can search the collection by Subject, Audience Category

including categories specific to private sector audiences, Hazard Type and other categories. For more information, visit <http://www.fema.gov/library/> or call (800) 480-2520.

FEMA Programs and Services

Community Preparedness – Citizen Corps is FEMA’s grassroots strategy to bring together government and community leaders to involve citizens in all-hazards emergency preparedness and resilience. Citizen Corps asks each individual to embrace the personal responsibility to be prepared; to get training in first aid and emergency skills; and to volunteer to support local emergency responders, disaster relief, and community safety. There are currently 2,433 Councils which serve over 227 million people or 80% of the total U.S. population. For more information on how you can participate, e-mail citizencorps@dhs.gov or visit www.citizencorps.gov.

Donations and Volunteers Information FEMA offers information on the best way to volunteer and donate during disaster response and recovery. For more information, see www.fema.gov/donations.

DisasterAssistance.gov DisasterAssistance.gov is a secure, user-friendly U.S. government web portal that consolidates disaster assistance information in one place. If you need assistance following a presidentially declared disaster that has been designated for individual assistance, you can now go to www.DisasterAssistance.gov to register online. Local resource information to help keep citizens safe during an emergency is also available. Currently, 17 U.S. government agencies, which sponsor almost 60 forms of assistance, contribute to the portal. For web site technical assistance, contact (800) 745-0243.

The Emergency Lodging Assistance Program provides prompt lodging payments for short term stays in the event of a declared disaster. The program is administered by Corporate Lodging Consultants, a federal government contractor and the largest outsourced lodging services provider in North America. For more information, see <http://ela.corplodging.com/programinfo.php>, contact femahousing@corplodging.com, or call (866) 545-9865.

The Emergency Food and Shelter National Board Program was created in 1983 to supplement the work of local social service organizations within the United States, both private and governmental, to help people in need of emergency assistance. This collaborative effort between the private and public sectors has provided over \$3.4 billion in Federal funds during its 27-year history. For more information, visit <http://www.efsp.unitedway.org/>.

The FEMA Industry Liaison Program is a point-of-entry for vendors seeking information on how to do business with FEMA during disasters and non-disaster periods of activity. The program coordinates vendor presentation meetings between vendors and FEMA program offices, establishes strategic relationships with vendor-supporting industry partners and stakeholders, coordinates Industry Days, conducts market research, responds to informal Congressional requests, and performs vendor analysis reporting. Vendors interested in doing business with FEMA should take the following steps: Register in the Central Contractor Registration (CCR) at www.ccr.gov, contact the FEMA Industry Liaison Program at <http://www.fema.gov/privatesector/industry/index.shtm>, or call the Industry Liaison Support Center at (202) 646-1895.

FEMA Flood Map Assistance Center (FMAC) provides information to the public about National Flood Insurance Program rules, regulations, and procedures. The FMAC is often the first point of contact between FEMA and various flood map users. The FMAC’s goal is to provide the appropriate information to callers to help them understand the technical issues involved in a particular situation. In addition to taking incoming telephone calls, Map Specialists respond to mapping-related e-mail inquiries, and also review and process Letter of Map Amendment (LOMA), Letter of Map Revision Based on Fill (LOMR-F), and Letter of Determination Review (LODR) requests. There are available resources for Engineers/Surveyors, Insurance Professionals and Lenders, Floodplain Managers. For more information, call (877) FEMA-MAP (877-336-2627) or e-mail FEMAMapSpecialist@riskmapcnds.com.

FEMA Regulatory Materials FEMA publishes its regulations, containing FEMA’s procedures and

requirements on the public, in Title 44 of the Code of Federal Regulations (CFR). These regulations are typically open for public comment before they go into effect. The public can access the regulations that are currently in effect electronically, by selecting Title 44 from the drop down menu at <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=%2Findex.tpl>. The public can submit and view comments submitted by other individuals at www.regulations.gov. For more information on Federal agency rulemaking, visit www.reginfo.gov or to contact FEMA regulatory officials e-mail FEMA-RULES@dhs.gov.

FEMA Small Business Program Small business vendors are routed to the FEMA Small Business Analyst for notification, support and processing. Small Business inquiries can be sent to FEMA-SB@dhs.gov.

U.S. Fire Administration (USFA) Fire Prevention and Safety Campaigns delivers fire prevention and safety education programs to reduce the loss of life from fire-related hazards, particularly among the very young and older adults. The campaigns encourage Americans to practice fire safety and to protect themselves and their families from the dangers of fire. In addition, they provide dedicated support to public fire educators and the media to facilitate community outreach to targeted audiences. For more information, visit <http://www.usfa.dhs.gov/campaigns/> or call (301) 447-1000.

U.S. Fire Administration Publications encourage Americans including private sector constituents to practice fire safety and protect themselves and their families from the dangers of fire. Order online at <http://www.usfa.dhs.gov/applications/publications/> or contact the U.S Fire Administration via e-mail, usfa-publications@dhs.gov or phone, (800) 561-3356.

Freight Rail Security Grant Program funds freight railroad carriers and owners and officers of railroad cars to protect critical surface transportation infrastructure from acts of terrorism, major disasters and other emergencies. For more information, visit <http://www.fema.gov/government/grant/> or contact the program by e-mail, askcsid@dhs.gov or phone, (800) 368-6498.

Intercity Bus Security Grant Program provides funding to create a sustainable program for the protection of intercity bus systems and the traveling public from terrorism. The program seeks to assist operators of fixed-route intercity and charter bus services in obtaining the resources required to support security measures such as enhanced planning, facility security upgrades and vehicle and driver protection. For more information, visit <http://www.fema.gov/government/grant/> or contact the program at askcsid@dhs.gov or (800) 368-6498.

Intercity Passenger Rail Grant Program creates a sustainable, risk-based effort to protect critical surface transportation infrastructure and the traveling public from acts of terrorism, major disasters and other emergencies within the Amtrak rail system. For more information visit <http://www.fema.gov/government/grant/> or contact the program at askcsid@dhs.gov or (800) 368-6498.

National Dam Safety Program Led by FEMA, the National Dam Safety Program (NDSP) is a partnership of the States, Federal agencies, and other stakeholders to encourage individual and community responsibility for dam safety. Since the inception of the NDSP in 1979, FEMA has supported a strong, collaborative training program for dam safety professionals and dam owners. With NDSP training funds, FEMA has been able to expand existing training programs, begin new initiatives to keep pace with evolving technology, and enhance the sharing of expertise between the federal and state sectors. For more information, visit <http://www.fema.gov/plan/prevent/damfailure/ndsp.shtm> or <http://www.damsafety.org/>.

National Incident Management System (NIMS) provides a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment. Web site: www.fema.gov/nims. Questions regarding NIMS should be directed to FEMA-NIMS@dhs.gov or (202) 646-3850.

National Response Framework (NRF) is a guide to how the Nation conducts all-hazards response. It is built upon

scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across the Nation, linking all levels of government, nongovernmental organizations, and the private sector. It is intended to capture specific authorities and best practices for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters. For more information, visit <http://www.fema.gov/nrf>.

National Flood Insurance Program focuses on Flood Insurance, Floodplain Management and Flood Hazard Mapping. Nearly 20,000 communities across the U.S. and its territories participate in the NFIP by adopting and enforcing floodplain management ordinances to reduce future flood damage. In exchange, the NFIP makes Federally-backed flood insurance available to homeowners, renters, and business owners in these communities. See www.floodsmart.gov Flood insurance agents interested in the program please visit www.agents.floodsmart.gov or e-mail asktheexpert@riskmapcds.com.

Nonprofit Security Grant Program provides funding support for target-hardening activities to nonprofit organizations that are at high risk of a terrorist attack and are located within one of the specific UASI-eligible urban areas. It is also designed to promote coordination and collaboration in emergency preparedness activities among public and private community representatives, State and local government agencies, and Citizen Corps Councils. For more information, visit <http://www.fema.gov/government/grant/nsgp> or contact the program by e-mail, askcsid@dhs.gov or phone, (800) 368-6498.

Port Security Grant Program is a sustainable, risk-based effort to protect critical port infrastructure from terrorism, particularly attacks using explosives and non-conventional threats that could cause major disruption to commerce. The PSGP provides grant funding to port areas for the protection of critical port infrastructure from terrorism. This program is primarily intended to assist ports in enhancing maritime domain awareness; enhancing risk management capabilities to prevent, detect, respond to and recover from attacks involving improvised explosive devices, Chemical, Biological, Radiological, Nuclear,

Explosive, and other non-conventional weapons; providing training and exercises; and Transportation Worker Identification Credential implementation. For more information, visit <http://www.fema.gov/government/grant/> or contact the program by e-mail, askcsid@dhs.gov or phone, (800) 368-6498.

QuakeSmart is designed to encourage business leaders and owners in areas of the U.S. that are at risk from earthquakes to take actions that will mitigate damage to their businesses, provide greater safety for customers and employees, and speed recovery in the event of an earthquake. The goal of QuakeSmart is to build awareness within the business community of the risk and to educate businesses, particularly small and emerging businesses, on the relatively simple things they can do to reduce or mitigate the impact of earthquakes, and support community preparedness. Business leaders and owners interested in finding out how to reduce or mitigate the impact of earthquakes on their business should visit www.quesmart.org.

Ready Business The U.S. Department of Homeland Security and the Advertising Council launched the *Ready Business* Campaign in September 2004. This extension of the successful *Ready* Campaign, *Ready Business* helps owners and managers of small- and medium-sized businesses prepare their employees, operations and assets in the event of an emergency. For free tools and resources, including how to create a business emergency plan, please visit www.ready.gov.

Radiological Emergency Preparedness Program (REP) Program helps to secure the health and safety of citizens living around commercial nuclear power plants. REP is responsible for reviewing and approving all community radiological emergency plans. The REP program is a leader in areas of policy guidance, planning, training, public education and preparedness for nuclear power plants. For over three decades, local and state responders have relied on REP's leadership to correct preparedness plans, monitor rigorous training regimens and support effective performance in the unlikely event of a radiological emergency. For more information, visit <http://www.fema.gov/hazard/nuclear/index.shtm>.

Technical Assistance (TA) Program seeks to build and sustain capabilities through specific services and analytical capacities through the development, delivery, and management of TA services that support the four homeland security mission areas (i.e. prevention, protection, response, and recovery), in addition to homeland security program management. TA is offered to a wide variety of organizations and grantees through an extensive menu of services responsive to national priorities. To best accommodate the wide variety of TA needs and deliverables, three levels of TA are provided. Level I/II services can be made available to private sector organizations and includes general information, models, templates, and samples. Level III services, available to private sector organizations who may be DHS grantees, provides onsite support via workshops and interaction between TA providers and recipients. For more information, visit http://www.fema.gov/about/divisions/pppa_ta.shtm or contact (800) 368-6498 or e-mail FEMA-TArequest@fema.gov.

Transit Security Grant Program is a sustainable, risk-based effort to protect critical surface transportation infrastructure and the traveling public from acts of terrorism, major disasters, and other emergencies. For more information, visit <http://www.fema.gov/government/grant/> or contact the program by e-mail, askcsid@dhs.gov or phone, (800) 368-6498.

Tornado Safety Initiative assesses building damages and identifies lessons learned after tornadoes occur; funds research on shelter design and construction standards; develops best practices and technical manuals on safe rooms and community shelters; and produces public education materials on tornado preparedness and response. FEMA produces technical manuals for engineers, architects, building officials, and prospective shelter owners on the design and construction of safe rooms and community shelters. For more information, visit <http://www.fema.gov/plan/prevent/saferoom/index>.

Unified Hazard Mitigation Assistance (HMA) Grant Programs present a critical opportunity to reduce the risk to individuals and property from natural hazards while simultaneously reducing reliance on Federal disaster funds. While the statutory origins of the programs differ,

all share the common goal of reducing the risk of loss of life and property due to natural hazards. HMA programs are subject to the availability of appropriation funding or funding based on disaster recovery expenditures, as well as any directive or restriction made with respect to such funds. HMA programs include Hazard Mitigation Grant Program, Pre-Disaster Mitigation program, Flood Mitigation Assistance program, Repetitive Flood Claims (RFC) program and Severe Repetitive Loss program. See www.fema.gov/government/grant/hma/index.shtm.

U.S. Immigration and Customs Enforcement (ICE)

U.S. Immigration and Customs Enforcement (ICE) is the largest investigative agency in the U.S. Department of Homeland Security (DHS). Formed in 2003 as part of the federal government's response to the 9/11 attacks, ICE's mission is to protect the security of the American people and the homeland by vigilantly enforcing the nation's immigration and customs laws. ICE combines innovative investigative techniques, new technological resources and a high level of professionalism to provide a wide range of resources to the public and to our Federal, State and local law enforcement partners. www.ice.gov

Forced Labor Resources The ICE Office of International Affairs investigates allegations of forced labor in violation of the Tariff Act of 1930 (Title 19 USC §1307). To request more information or a copy of A Forced Child Labor Advisory booklet and brochure, please contact: ice.forcedlabor@dhs.gov. When contacting ICE to report instances of forced labor, please provide as much detailed information and supporting documentation as possible, including the following: a full statement of the reasons for the belief that the product was produced by forced labor and that it may be or has been imported to the United States; a detailed description of the product; all pertinent facts known regarding the production of the merchandise abroad. For the location of ICE foreign offices, go to the ICE web site at <http://www.ice.gov>, click *About Us*, click *Office of International Affairs* and select your country. ICE maintains a 24/7 hotline at (866) DHS-2-ICE.

Human Rights Violators and War Crimes Center has a mission to protect the public by targeting war criminals and those who violate human rights, including violators living both domestically and abroad. The assigned staff of ICE investigators and intelligence analysts dedicated to the Center work with governmental and non-governmental agencies. They accept tips and information from those who report suspected war criminals and human rights violators. Individuals seeking to report these abuses of human rights may contact the Center at HRV.ICE@DHS.GOV.

Human Trafficking: "Hidden in Plain Sight" is the ICE human trafficking public outreach campaign that heightens awareness of human trafficking through announcements via billboards and posters on public transportation, bus stops and in businesses. The Hidden in Plain Sight campaign provides critical human trafficking information to the public and gives people a method for reporting suspected human trafficking activity. ICE's Office

of Investigations (OI) designed a one-minute video Public Service Announcement (PSA), which is a broadcast message used for public outreach. ICE uses the PSA during presentations to provide information to the general public and human trafficking-related organizations. The PSA is accessible to the public via the ICE Web site at www.ice.gov and it is also distributed to the public on DVD during training and presentations worldwide. See the flash video at <http://www.ice.gov/flashmovie/human-trafficking/plain-sight.htm>.

Human Trafficking: Indicators Pamphlet is currently produced in English, Spanish, and Portuguese and is distributed during presentations and trainings worldwide. See <http://www.ice.gov/pi/news/factsheets/humantrafficking.htm>.

Human Trafficking: Awareness Resources ICE is the primary agency within the Department of Homeland Security that fights human trafficking. Trafficking in Persons (TIP) is a modern day form of slavery. Human trafficking is defined by Section 103 of the Trafficking Victims Protection Act of 2000 as '(A) sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age; or (B) the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery. ICE is committed to a victim-focused approach to trafficking investigations that places equal importance on protecting the victims and prosecuting the traffickers. Part of this strategy includes an aggressive public outreach campaign to raise awareness of the issue and provide a mechanism for the public to report suspected trafficking activity. ICE also conducts continuous outreach and training to U.S. and foreign law enforcement, non-

governmental and international organizations, in order to provide awareness and the latest investigative techniques and victim assistance practices. The public is encouraged to report all suspicious activity to ICE at (866) DHS-2ICE (1-866-347-2423). Informational material on human trafficking is produced in a variety of languages, and is available to law enforcement, NGOs and includes the following: a public service announcement; human trafficking brochure; human trafficking indicator wallet cards; and human trafficking indicators for law enforcement brochure. See <http://www.ice.gov/pi/investigations/publicsafety/humantrafficking.htm>.

Human Trafficking: Trafficking in Persons (TIP) Card ICE currently distributes human trafficking material, known as the human trafficking in persons (TIP) card. This plastic business card helps distinguish between the crime of human trafficking versus the crime of human smuggling, listing indicators of each as the two crimes are often confused. The TIP card includes the ICE telephone number for individuals to call for guidance or to report suspicious activity. The TIP card is currently produced in 17 different languages. To request the TIP card, contact your local ICE office. The TIP cards are also distributed during presentations and training offered worldwide. For more information visit the ICE Web site at www.ice.gov. For ICE principal field offices across the country, see <http://www.ice.gov/about/investigations/contact.htm>.

ICE LINK Portal The ICE National Incident Response Unit (NIRU) for incident awareness, continuity of operations, exercises, incident response, special event coordination and many other homeland security requirements administers a web-based communications and collaboration platform called the ICE LINK Portal. The ICE LINK Portal is a robust, sensitive but unclassified, information-sharing network used as a force multiplier to enhance coordination with Federal, State, local and Tribal

priorities. ICE LINK Portal users include federal agencies, fusion centers, military components, Interpol and the intelligence community. Additionally, the ICE LINK Portal can be used for Critical Infrastructure and Key Resources (CI/KR) first responder personnel in the private sector in the event of a national crisis or incident. For more information and/or assistance, contact NIRU at niru@dhs.gov.

ICE Mutual Agreement between Government and Employers (IMAGE) Program is a joint government and private sector voluntary initiative that enhances employer compliance and corporate due diligence through training and sharing best practices regarding hiring practices. The goal of IMAGE is for the government to work with employers to develop a more secure and stable workforce and restore the integrity of the U.S. immigration system. More information can be found at ICE's Web site at www.ice.gov/image. Contact: IMAGE@dhs.gov or Section Chief Adam Wilson at (202) 732-3064.

ICE Office of Public Affairs (ICE OPA) is dedicated to building understanding and support for the agency's mission through outreach to DHS employees, the media and the general public. ICE OPA is headquartered at Potomac Center North (PCN), 500 12th St. SW, in Washington, D.C. ICE field public affairs officers are located throughout the country and are responsible for regional media relations in specific geographic areas. For more information, see <http://www.ice.gov> or contact PublicAffairs.IceOfficeOf@dhs.gov, (202) 732-4242.

ICE Privacy Office sustains privacy protections and the transparency of government operations while supporting the ICE mission. The ICE Privacy Office ensures that the Privacy Impact Assessments and System of Records Notices complies with key federal privacy laws and policies. Members of the public can contact the Privacy Office with concerns or complaints regarding their privacy in regard to the mission of ICE. See <http://www.ice.gov/about/privacyoffice/contact.htm>. For more information, contact ICEPrivacy@dhs.gov, (202) 732-3300.

ICE Tip-Line is a 24/7 toll free number enabling the public to report violations of customs and immigration laws, sexual and economic exploitation of children and adults, threats to national security and other activities considered illegal or suspicious in nature. Please assist DHS in maintaining the security and integrity of the nation by reporting illegal activity. More information regarding ICE programs can be found at the ICE Web site <http://www.ice.gov> or <http://www.ice.gov/pi/topics/index.htm> or by calling **(866) DHS-2ICE** (1-866-347-2423) or outside the United States: +1 (877) 347-2423.

ICE Victim Assistance Program (VAP) provides information and assistance to human trafficking victims. The VAP provides information about post-correctional release or removal of criminal aliens from ICE custody. The VAP provides brochures for victims of trafficking and its victim notification program. To request copies of the brochures, please contact the VAP at (866) 872-4973.

The National Intellectual Property Rights (IPR) Coordination Center is the federal government's central point of contact in the fight against IPR violators and the flow of counterfeit goods into the United States since 2000. The new center in Northern Virginia is the high-tech home of a partnership between government, private industry and law enforcement communities. More information can be found at <http://www.ice.gov/pi/iprctr/index.htm>. Report an IPR violation at <http://www.ice.gov/partners/cornerstone/ipr/IPRForm.htm> or contact the IPR Center at (866) IPR-2060 or (866) 477-2060.

Money Laundering and Operation Cornerstone U.S. Immigration and Customs Enforcement (ICE) recognizes that the private sector represents America's first line of defense against money laundering. In Operation Cornerstone, the ICE Office of Investigations reaches out to the U.S. business community, along with State and Federal agencies to combat financial and trade crimes. Operation Cornerstone identifies and eliminates vulnerabilities within the U.S. financial, trade and transportation sectors--vulnerabilities that criminal and terrorist organizations could exploit to finance their illicit operations and avoid being detected by law enforcement.

The ICE Financial Programs/Cornerstone Unit publishes the Cornerstone Report, a quarterly newsletter. This report provides current trends and financial crimes identified by law enforcement and the private sector. To subscribe to the Cornerstone Report or for more information visit: www.ice.gov/cornerstone. Report suspicious activity by calling (866) DHS-2-ICE.

Project Shield America (PSA) is the first line of defense against those who compromise U.S. national security by violating export laws, sanctions and embargoes. Specifically, ICE's Counter-Proliferation Investigations Unit reaches out to applicable high-tech industries to monitor weapons of mass destruction and their components that are potential targets for illegal trafficking. Through PSA, ICE works in partnership with U.S. Customs and Border Protection (CBP) and U.S. companies that manufacture, sell or export strategic technology and munitions. See http://www.ice.gov/doclib/investigations/pdf/cpi_brochure.pdf (pdf 192 KB). For additional information, please contact ICE Headquarters, PSA Program Manager at ICE Headquarters at (202) 732-3765 or (202) 732-3764. Report suspicious activity at the ICE tip line (866) DHS-2-ICE (1-866-347-2423).

Student and Exchange Visitor Program (SEVP) was established in 2003 as the Department of Homeland Security's front line effort to ensure that the student visa system is not exploited by those wishing to do harm to the United States. SEVP's key tool in this effort is the Student and Exchange Visitor Information System (SEVIS), a web-based information management system that allows ICE to monitor the status of non-immigrant student and exchange visitors in the United States. SEVP collects, maintains and provides the information so that only legitimate foreign students or exchange visitors gain entry to the United States. The result is an easily accessible information system that provides timely information to the Department of State, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, and ICE. For more information, visit <http://www.ice.gov/sevis/>. For inquiries by phone, call the SEVP Response Center at (703) 603-3400 or via e-mail at: SEVIS.Source@DHS.gov.

Office of Infrastructure Protection (IP)

From energy systems that power our neighborhoods, to transportation networks that move us around our communities and the country, to facilities that provide our families with safe drinking water, critical infrastructure and key resources (CIKR) impact nearly every aspect of our daily lives. In short, CIKR is an umbrella term referring to the assets of the United States essential to the nation's security, public health and safety, economic vitality, and way of life. CIKR is divided into 18 separate sectors, as diverse as agriculture and food, emergency services, and cyber networks. Because this critical infrastructure provides our country with the enormous benefits and services and opportunities on which we rely, we are very mindful of the risks posed to CIKR by terrorists, pandemic diseases and natural disasters. At the Department of Homeland Security, we know that these threats can have serious effects, such as cutting populations off from clean water, power, transportation, or emergency supplies. Secretary Napolitano is working to raise awareness about the importance of our nation's critical infrastructure and to strengthen our ability to protect it. The Department oversees programs and resources that foster public-private partnerships, enhance protective programs, and build national resiliency to withstand natural disasters and terrorist threats. www.dhs.gov/criticalinfrastructure

IP Training and Education

Active Threat Recognition for Retail Security Officers This 85-minute presentation produced by the Office for Bombing Prevention is split into easy to understand modules and uses specific foreign and domestic case studies to explain lessons learned and to discuss specific considerations for retail and shopping centers. The training discusses signs of criminal and terrorist activity; types of surveillance; and suspicious behavioral indicators. The presentation is available with guest log-in capabilities on the DHS Homeland Security Information Network (HSIN). To access the presentation, please register at: <https://connect.hsin.gov/attrso/event/registration.html> After submitting the short registration information to include setting a password of your choice, you will receive an e-mail confirmation with instructions for logging in to view the material. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Bomb Event Management Web Training is a 60-minute online session produced by the Office for Bombing Prevention that provides an overview of risks and risk mitigation considerations related to improvised explosive devices (IED) threats and planning. This web training is available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know through the Homeland Security Information Network-Critical Sectors (HSIN-CS) (<https://cs.hsin.gov/>) online secure portal. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Bombing Prevention Workshop is a one-day workshop, intended for regional level public and private stakeholders and planners from emergency management, security, and law enforcement, designed to enhance the effectiveness in managing a bombing incident. This workshop reviews the current development of strategies and brings together best practices from regions across multiple localities, disciplines and levels of government. The guided scenario discussion establishes the foundation for the stakeholders within the region to implement a Bombing Prevention Plan. This workshop can accommodate up to 50 participants. To request training contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Chemical Sector Explosive Threat Awareness Training Program The Chemical Sector-Specific Agency (SSA) is offering a series of one day vehicle borne improvised explosive device (VBIED) training sessions to chemical facility security officers. This course is offered in six locations in FY10 (Dallas, Orlando, New Orleans, St. Louis, Seattle, and Buffalo). Contact the Chemical SSA for more information ChemicalSector@dhs.gov.

Counterterrorism Protective Measures Course is a two-day course designed to enhance Commercial Sector awareness on how to devalue, detect, deter, and defend facilities from terrorism, by providing the knowledge and skills necessary in understanding common vulnerabilities and employing effective protective measures. The Protective Measures Course includes lessons learned and industry best practices in mitigating terrorist attacks. It serves as a follow-up to the Soft Target Awareness Course, focusing more on implementation than awareness. This course can accommodate 35 participants. To request

training, contact the DHS Office for Bombing Prevention, OBP@dhs.gov, (703) 235-5723.

Critical Infrastructure and Key Resources (CIKR) Learning Series features one-hour infrastructure protection (IP) Web-based seminars on current topics and issues of interest to CIKR owners and operators and key government partners. Over 5,000 partners/stakeholders have registered for the Learning Series since its inception in August, 2008. The list serve for this series includes more than 27,000 interested individuals. See http://www.dhs.gov/files/programs/gc_1231165582452.shtm. For more information, contact IP_Education@hq.dhs.gov.

Critical Infrastructure and Key Resources (CIKR) Training Module provides an overview of the National Infrastructure Protection Plan (NIPP) and CIKR Annex to the National Response Framework. The module was developed for inclusion in the FEMA Integrated Emergency Management and other incident management related courses. This document is available upon request in PowerPoint format with instructor and participant guides and can be easily integrated into existing training programs. A Spanish version is also available. To request the training module, contact IP_Education@hq.dhs.gov.

DHS/Commercial Facilities Training Resources Guide pamphlet was developed to promote classroom and independent study programs for DHS partners and private sector stakeholders that build functional skills for disaster response effectiveness. Subject matter includes cybersecurity, weapons of mass destruction, and natural disaster planning. Available on request, contact the

Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

DHS Retail Video: "What's in Store - Ordinary People/Extraordinary Events" is a multimedia training video for retail employees of commercial shopping venues alerting them to the signs of suspicious behavior in the workplace that might lead to a catastrophic act. See http://www.dhs.gov/multimedia/dhs_retail_video.wmv. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

DHS Training Video "Check It!: Protecting Public Spaces" is a training video for front line event staff at large public venues. The video demonstrates the proper procedures for conducting bag searches and recognizing suspicious behavior at public gathering spaces like sports venues. The video is available for viewing and download at http://www.dhs.gov/files/programs/gc_1259859901230.shtm#4 or by contacting the Commercial Facilities Sector-Specific Agency at CFSTeam@hq.dhs.gov.

Emergency Services Sector Training Catalog describes public and private resources and programs that are applicable to first responders. Printed catalogs are available by contacting the Emergency Services Sector-Specific Agency ESSTeam@hq.dhs.gov.

Improvised Explosive Device (IED) Awareness / Bomb Threat Management Workshop IED attacks remain the primary tactic for bombers, terrorists, and criminals seeking relatively uncomplicated, inexpensive means for inflicting mass casualties and maximum damage. This four-hour presentation is designed to enhance and strengthen the participant's knowledge, skills, and abilities in relation to the threat of IEDs. The information presented outlines specific practices associated with Bomb Threat Management including IED awareness, explosive incidents, and bombing prevention. This workshop is designed to provide two four-hour sessions, morning and afternoon, with 50 participants for each session. To request training, contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Improvised Explosive Device (IED) Awareness Web Training This 60-minute IED Awareness Web Training,

produced by the Office for Bombing Prevention and similar to the IED Awareness Course, is designed to enhance and strengthen the participant's knowledge, skills, and abilities in relation to the threat of IEDs. Topics addressed during the web training include the use of IEDs as a popular terrorist attack method; types of explosives and explosive effects; construction, components, and categories of IEDs; and IED related safety measures. This web training is available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know through the Homeland Security Information Network-Critical Sectors (HSIN-CS) (<https://cs.hsin.gov/>) online secure portal. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Improvised Explosive Device (IED) Search Procedures Workshop This 8-hour Workshop, consisting of lecture and practical exercises, is designed for security personnel and facility managers of sites hosting any event that requires increased IED security preparedness. The information provided during the Workshop focuses on general safeties used for specialized explosives searches and sweeps, and can be tailored to meet the requirements for supporting any event. The Workshop can accommodate 25 participants. To request training, contact the DHS Office for Bombing Prevention: OBP@dhs.gov, (703) 235-5723.

Independent Study Course IS-821 "Critical Infrastructure and Key Resources (CIKR) Support Annex" provides an introduction to the CIKR Support Annex to the National Response Framework. See <http://training.fema.gov/emiweb/is/is821.asp>, for more information, contact IP_Education@hq.dhs.gov.

Independent Study Course IS-860.a National Infrastructure Protection Plan (NIPP) presents an overview of the NIPP. The NIPP provides the unifying structure for the integration of existing and future CIKR protection and resiliency efforts into a single national program. This course has been updated to align with the NIPP that was released in 2009. Classroom materials are also available for this course. For more information, visit <http://training.fema.gov/emiweb/is/is860a.asp> or contact IP_Education@hq.dhs.gov.

Independent Study Course IS-870: Dams Sector: Crisis Management Overview is web-based training focused on information provided within the Dams Sector Crisis Management handbook. See <http://training.fema.gov/EMIWeb/IS/IS870.asp>. For more information, contact the Dams Sector-Specific Agency, dams@dhs.gov.

Integrated Common Analytical Viewer (iCAV) Web-based Training provides instruction on the use of the iCAV Next Generation geospatial visualization tool, including access and use of DHS geospatial resources and data. Users are guided through system "buttonology" to gain a feel for the types of imagery, infrastructure, and situational awareness data available through iCAV Next Generation, as well as some of the analytical tools that users can leverage to understand infrastructure in a domestic response context. More information on iCAV Next Generation is available at <http://www.dhs.gov/icav>, and the training itself is available at <http://www.jsrts.org/dhs/icav>.

Private Sector Counterterrorism Awareness Workshop is a one-day workshop designed to improve the knowledge of private sector security professionals by providing exposure to key elements of soft target awareness, surveillance detection, and improvised explosive device (IED) recognition. The workshop's training materials enhance and reinforce participants' knowledge, skills, and abilities related to preventing, protecting against, responding to, and recovering from terrorist threats and incidents. The workshop outlines specific counterterrorism awareness and prevention actions that reduce vulnerability and mitigate the risk of domestic terrorist attacks. This workshop can accommodate 100 to 250 participants. To request training contact the DHS Office for Bombing Prevention, OBP@dhs.gov at (703) 235-5723.

Soft Target Awareness Course is designed to enhance individual and organizational awareness of terrorism and help facilitate information sharing at commercial facilities considered soft targets, such as shopping malls and hotels. Commercial infrastructure facility managers, supervisors, operators, and security staff gain a better understanding of their roles in deterring, detecting, and defending their facilities from terrorism. Participants choose from five

focus areas according to their specific affiliation: Stadiums and Arenas; Places of Worship; Education; Malls and Shopping Centers; and Large Buildings, Hotels and Medical Facilities. Each of these focus areas is comprised of a four-hour session of combined informal lecture and capstone guided discussions. Each session can accommodate 35 participants or can be modified for one general session for up to 175 participants. To request training contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff Course is a three-day course that explains how protective measures can be applied to detect and deter potential threats to critical infrastructure and key resources (CIKR), as well as the fundamentals for detecting surveillance activity. The course is designed for commercial infrastructure operators and security staff of nationally significant CIKR facilities. This course can accommodate 25 participants. To request training contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Surveillance Detection Training for Municipal Officials, State and Local Law Enforcement Course is a three-day course that provides the knowledge and skills necessary to establish surveillance detection operations to protect critical infrastructure and key resources (CIKR), during periods of elevated threat. Comprised of five modules of informal lecture and two exercises, it provides participants with an awareness of terrorist tactics and attack history and illustrates the means and methods to detect surveillance through practical surveillance detection exercises. This Surveillance Detection Course is designed for municipal security officials and State and local law enforcement with jurisdictional authority over nationally significant CIKR facilities. This course can accommodate 25 participants. To request training contact the DHS Office for Bombing Prevention, OBP@dhs.gov, (703) 235-5723.

Surveillance Detection Web Training is a 60-minute online session produced by the Office for Bombing Prevention that addresses the threat of hostile surveillance on critical infrastructure. Topics addressed during the web training include basic private sector threat awareness, surveillance and surveillance detection defined, recognition of the

types and patterns of behavior associated with terrorist activity, signs of terrorist activity, and suspicious activity reporting. This web training is available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know through the Homeland Security Information Network-Critical Sectors (HSIN-CS) (<https://cs.hsin.gov/>) online secure portal. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Threat Detection and Reaction by Retail Staff (Point of Sale) This 20-minute presentation is intended for Point-of-Sale staff, but is applicable to all employees of a shopping center, mall, or retail facility. It uses case studies and best practices to explain suspicious behavior and items; how to reduce the vulnerability to an active shooter threat; and the appropriate actions to take if employees notice suspicious activity. To access the 20-minute presentation, visit: <https://connect.hsin.gov/p21849699/>.

Web-Based Chemical Security Awareness Training Program is an interactive tool available free to chemical facilities nationwide to increase security awareness. The training is designed for all facility employees, not just those traditionally involved in security. Upon completion, a certificate is awarded to the student. See <https://www.chemicalsecuritytraining.com/>. Contact the Chemical Sector-Specific Agency at 1-877-CHEMSEC, ChemicalSector@dhs.gov.

IP Guidance Documents/Publications

Active Shooter - How To Respond is a desk reference guide, a reference poster, and a pocket-size reference card to address how employees, managers, training staff, and human resources personnel can mitigate the risk of and appropriately react in the event of an active shooter situation. See http://www.dhs.gov/files/programs/gc_1259859901230.shtm. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Bomb-making Materials Awareness Program (BMAP)/Suspicious Behavior Cards These joint FBI-DHS private sector advisory cards offer simple concise tips and

images helping retailers identify and report suspicious activity and sale of household items that can be used in making home-made explosives (HMEs) and improvised explosive devices (IED). The register cards give front end store employees guidance on precursor materials and what to look for regarding suspicious purchases. See http://www.dhs.gov/files/programs/gc_1259938444548.shtm. To request materials or additional information, contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Chemical Facility Anti-Terrorism Standards (CFATS) Frequently Asked Questions were developed and continue to be regularly updated as a means of assisting facilities in complying with the CFATS regulation. The FAQs are searchable and categorized to further benefit the user and can be found at <http://csat-help.dhs.gov/pls/apex/f?p=100:1:7096251139780888>. For more information, contact the CFATS Help Desk at cfats@dhs.gov, (866) 323-2957.

Chemical Facility Anti-Terrorism Standards (CFATS) Presentations The Infrastructure Security Compliance Division (ISCD) reaches out to people and companies in the chemical industry and those interested in chemical security. Those interested in a live presentation about CFATS by ISCD personnel can find more information about such presentations at DHS' chemical security web site: http://www.dhs.gov/files/programs/gc_1224766914427.shtm. For more information, contact the CFATS Help Desk at cfats@dhs.gov, (866) 323-2957.

Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS) The Infrastructure Security Compliance Division (ISCD) provides outreach to key stakeholders with interest or involvement in chemical facility security. Those interested in a live presentation about CFATS by ISCD personnel can find more information and request a presentation by visiting http://www.dhs.gov/files/programs/gc_1224766914427.shtm. For more information, contact the CFATS Help Desk at cfats@dhs.gov, (866) 323-2957.

Chemical-Terrorism Vulnerability Information (CVI) is the information protection regime authorized by Section 550 of [Public Law 109-295](http://www.gpo.gov/public-law/109-295) to protect from inappropriate public

disclosure of any information developed or submitted pursuant to Section 550. This includes information that is developed and/or submitted to DHS pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS) regulation which implements Section 550. See www.dhs.gov/chemicalsecurity. For more information, contact the CFATS Help Desk at csat@dhs.gov, (866) 323-2957.

Commercial Facilities Sector Pandemic Planning

Documents for use by public assembly sector stakeholders detailing key steps and activities to take when operating during a pandemic influenza situation, a process tracking and status template, and a checklist of recommendations for pandemic response plan development. The products were created in partnership with International Association of Assembly Manager's Academy for Venue Safety and Security. Materials are available on request by contacting the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Dams Sector Resources provide owners/operators with information regarding the Dams Sector. Publications include: **Dams Sector Consequence-Based Top Screen Fact Sheet**, **Dams Sector Councils Fact Sheet**, **Dams Sector Crisis Management Handbook**, **Dams Sector Exercises Series Fact Sheet - 2009**, **Dams Sector Overview Brochure**, **Dams Sector Security Awareness Guide**, **Security Awareness Guide for Levees**, **Security Awareness for Levee Owners Brochure**, **Dams Sector Standard Operating Procedures for Information Sharing**, **Waterside Barriers Guide**, **Suspicious Activity Reporting Fact Sheet**, **Personnel Screening Guide for Owners and Operators**, and **Physical Security Measures for Levees Brochure**. These resources are available on the HSIN-CS Dams Portal, <https://cs.hsin.gov/C2/DS/default.aspx>, the CIKR Resource Center, <http://www.dhs.gov/criticalinfrastructure>, and the Association of State Dam Safety Officials (ASDSO) Web site, <http://www.damsafety.org>. For more information, contact the Dams Sector-Specific Agency at dams@dhs.gov.

Dams Sector Resources (For Official Use Only): The **Dams Sector Security Awareness Handbook** assists owners/operators in identifying security concerns, coordinating proper response, and establishing effective

partnerships with local law enforcement and first responder communities. The **Dams Sector Protective Measures Handbook** assists owners/operators in selecting protective measures addressing the physical, cyber, and human elements and includes recommendations for developing site security plans. The **Dams Sector Research & Development Roadmap: Development of Validated Damage and Vulnerability Assessment Capabilities for Aircraft Impact Scenarios** is a collaborative effort involving multiple agencies focused on investigating vulnerabilities of concrete arch and embankment dams to aircraft impact scenarios. These For Official Use Only (FOUO) documents are available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know. For more information, contact the Dams Sector-Specific Agency at dams@dhs.gov.

DHS Daily Open Source Infrastructure Report is collected each week day as a summary of open-source published information concerning significant critical infrastructure issues. Each Daily Report is divided by the critical infrastructure sectors and key assets defined in the National Infrastructure Protection Plan. The DHS Daily Open Source Infrastructure Report is available on DHS.gov and Homeland Security Information Network-Critical Sectors (HSIN-CS). See http://www.dhs.gov/files/programs/editorial_0542.shtm. For more information, contact NICCRports@dhs.gov or CIKR.ISE@dhs.gov or (202) 312-3421.

DHS Retail Video: "What's in Store - Ordinary People/Extraordinary Events" is a multimedia training video for retail employees of commercial shopping venues alerting them to the signs of suspicious behavior in the workplace that might lead to a catastrophic act. See http://www.dhs.gov/multimedia/dhs_retail_video.wmv. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Education, Outreach, and Awareness Snapshot The National Infrastructure Protection Plan (NIPP) provides the coordinated approach for establishing national priorities, goals, and requirements for critical infrastructure and key resources (CIKR) protection and resilience. The NIPP also establishes a framework that allows people and organizations to develop and maintain key CIKR protection

expertise. This two-page snapshot describes the NIPP's approach to building national awareness and enabling education, training, and exercise programs. See http://www.dhs.gov/xlibrary/assets/nipp_education.pdf. For additional information, contact NIPP@dhs.gov.

Emergency Services Personal Readiness Guide for Responders and Their Families is a tri-fold handout providing a description of the Ready Campaign, the Emergency Services Sector-Specific Agency, a list of website resources and instructions on family preparedness that include suggestions on developing an emergency kit and family emergency plan. The **Emergency Services Sector (ESS) Video** is a three-minute video providing an overview of the ESS Sector. The video is appropriate for conferences and events to grow awareness and participation in sector activities. For more information, or to request materials contact the Emergency Services Sector-Specific Agency at ESSTeam@hq.dhs.gov.

Evacuation Planning Guide for Stadiums was developed to assist stadium owners and operators with preparing an Evacuation Plan and determining when and how to evacuate, conduct shelter-in-place operations, or relocate stadium spectators and participants. The NASCAR Mass Evacuation Planning Guide and Template was modified into an Evacuation Planning Guide for Stadiums by a working group composed of various Federal agencies and members of the Commercial Facilities Sector Coordinating Council. See http://www.dhs.gov/xlibrary/assets/ip_cikr_stadium_evac_guide.pdf. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Guide to Critical Infrastructure and Key Resources (CIKR) Protection at the State, Regional, Local, Tribal, & Territorial Level outlines the attributes, capabilities, needs, and processes that a State or local government entity should include in establishing its own CIKR protection function such that it integrates with the National Infrastructure Protection Plan (NIPP) and accomplishes the desired local benefits. This document is available by contacting the NIPP Program Management Office at NIPP@dhs.gov.

Hotel and Lodging Advisory Poster was created for all staff throughout the U.S. Lodging Industry designed to increase awareness regarding a property's potential to be used for illicit purposes; suspicious behavior and items; and appropriate actions for employees to take if they notice suspicious activity. The poster was designed in tandem with the Commercial Facilities Sector Coordinating Council and the Lodging Subsector. See http://www.dhs.gov/xlibrary/assets/ip_cikr_hotel_advisor_y.pdf. For additional information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Infrastructure Data Taxonomy (IDT) Critical infrastructure and key resources (CIKR) and their elements can be described and categorized in various ways, which can result in inconsistent communication and hinder timely decision-making within the homeland security community. To prevent such problems, the Department of Homeland Security uses an Infrastructure Data Taxonomy to enable transparent and consistent communication about CIKR between government and private sector partners with its structured terminology, the Infrastructure Data Taxonomy allows its users to designate an asset as belonging to a particular group, and then apply additional, associated taxonomy levels to detail the specifics of the asset and describe its functions. By applying a detailed, structured system of categorization to assets that includes sectors, sub-sectors, segments, sub-segments and asset type, the Infrastructure Data Taxonomy minimizes potential confusion and enhances transparency about CIKR. See http://www.dhs.gov/files/publications/gc_122659593457_4.shtm. To request access to download, view, and comment on the Infrastructure Data Taxonomy please visit https://lens.iac.anl.gov/dana-na/auth/url_31/welcome.cgi. Contact: IICD@dhs.gov.

Infrastructure Protection Report Series (IPRS) is a comprehensive series of For Official Use Only (FOUO) reports containing detailed information for all 18 Critical Infrastructure and Key Resources (CIKR) Sectors focusing on infrastructure characteristics and common vulnerabilities, potential indicators of terrorist activity, potential threats, and associated protective measures. The IPRS is available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know through the Homeland Security Information

Network-Critical Sectors (HSIN-CS) (<https://cs.hsin.gov/>) online secure portal. For more information on the IPRS, private sector CIKR owners and operators should contact DHS Office of Infrastructure Protection Vulnerability Assessments Branch at IPassessments@dhs.gov or the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 235-5724.

International Issues for Critical Infrastructure and Key Resources (CIKR) Protection The National Infrastructure Protection Plan (NIPP) brings a new focus to international security cooperation and provides a risk-based framework for collaborative engagement with international partners and for measuring the effectiveness of international CIKR protection activities. This two-page snapshot describes the approach to international issues embodied in the NIPP and the Sector-Specific Plans. See http://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf. For more information, contact NIPP@dhs.gov.

Multi-Jurisdiction Improvised Explosive Device (IED) Security Plan (MJIEDSP) An effective response to bombing threats and actual incidents requires the close coordination of many different public safety and law enforcement organizations and disciplines. MJIEDSP assists multi-jurisdiction areas in developing a detailed IED security plan that integrates the assets and capabilities of multiple jurisdictions and emergency service sectors. To request additional information, contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

National Critical Infrastructure and Key Resources (CIKR) Protection Annual Report Snapshot Homeland Security Presidential Directive 7, which directed the development of the National Infrastructure Protection Plan, also designated 17 Federal Sector-Specific Agencies (SSAs) and required each SSA to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CIKR protection in their respective sectors. This two-page snapshot describes the National CIKR Protection Annual Report that is developed from the Sector Annual Reports. See http://www.dhs.gov/xlibrary/assets/nipp_annrpt.pdf. For more information, contact NIPP@dhs.gov.

National Infrastructure Protection Plan (NIPP) 2009 provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the nation's critical infrastructure and key resources (CIKR) into a single national program. See http://www.dhs.gov/files/programs/editorial_0827.shtm. The **NIPP 2009 Overview Snapshot** provides a brief overview of the NIPP risk management framework and the sector partnership model. See http://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf. The **NIPP Brochure** describes the national approach to achieving the goals articulated in the NIPP, the NIPP risk management framework, the NIPP value proposition, and the sector partnership model. The **NIPP Information Sharing Snapshot** describes the NIPP's approach to achieving active participation by government and private sector partners through robust multi-directional information sharing. It describes the networked approach to information sharing under the NIPP and the establishment of the CIKR Information-Sharing Environment (CIKR ISE). See http://www.dhs.gov/xlibrary/assets/NIPP_InfoSharing.pdf. For more information or to request materials contact the NIPP Program Management Office NIPP@dhs.gov.

NIPP in Action Stories are multi-media pieces highlighting successes in National Infrastructure Protection Plan (NIPP) and Sector Specific Plan (SSP) implementation; these stories can take the form of a printed snapshot, a short video, or a poster board. NIPP in Action stories are developed in concert with sector partners and are designed to promote cross-sector information sharing of best practices with government partners and infrastructure owners and operators. If you would like more information or are interested in developing a NIPP in Action story, contact NIPP@dhs.gov.

Planning for 2009 H1N1 Influenza: A Preparedness Guide for Small Business The Department of Homeland Security, the Center for Disease Control (CDC), and the Small Business Administration have developed this booklet to help small businesses understand what impact a new influenza virus, like 2009 H1N1 flu, might have on their operations, and how important it is to have a written plan for guiding your business through a possible pandemic. See <http://www.flu.gov/professional/business/>

[smallbiz.html](#). For more information, contact IP_Education@hq.dhs.gov.

Protective Measures Guide for U.S. Sports Leagues provides an overview of best practices and protective measures designed to assist sports teams and owners/operators of sporting event venues with planning and managing security at their facility. The Guide provides examples of successful planning, organization, coordination, communication, operations, and training activities that result in a safe sporting event experience. This document is For Official Use Only (FOUO) and is available to vetted critical infrastructure owners and operators on request based on a demonstrated need to know. For more information, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Sector Annual Reports The Sector-Specific Agency Executive Management Office (SSA EMO) Collaborates with State, local, Tribal and territorial government and the private sector to develop, maintain and update Sector Annual Reports for the Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear Sectors. These reports are For Official Use Only (FOUO) and available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know. For more information, contact ssaexecsec@dhs.gov.

Sector-Specific Agency Executive Management Office (SSA EMO) Sector Snapshots, Fact Sheets and Brochures These documents provide a quick look at SSA EMO sectors and generally contain sector overviews; information on sector partnerships; information on key CIKR protection issues and Priority Programs. The products bring awareness to CIKR issues and encourage sector participation in critical infrastructure protection risk management activities. These products include: fact sheets and brochures for the Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services and Nuclear Sectors. Additional materials available on request. See http://www.dhs.gov/files/programs/gc_1189168948944.shtm. For more information, contact NIPP@dhs.gov.

Sector-Specific Pandemic Influenza Guides (Sector-Specific Agency Executive Management Office (SSA EMO) Sectors) SSA EMO worked with Partnership and Outreach Division to develop sector-specific guides for pandemic influenza for the Chemical, Commercial Facilities, Dams, Emergency Services, and Nuclear Sectors. Available on request by contacting SSAexecsec@dhs.gov.

Sector-Specific Plans detail the application of the National Infrastructure Protection Plan (NIPP) risk management framework to the unique characteristics and risk landscape of each sector. The SSPs provide the means by which the NIPP is implemented across all the critical infrastructure and key resources (CIKR) sectors. Each Sector-Specific Agency is responsible for developing and implementing an SSP through a coordinated effort involving their public and private sector CIKR partners. For publicly-available plans, please visit http://www.dhs.gov/files/programs/gc_1179866197607.shtm. For more information, contact NIPP@dhs.gov.

State and Local Implementation Snapshot The National Infrastructure Protection Plan (NIPP) provides the coordinated approach for establishing national priorities, goals, and requirements for critical infrastructure and key resources protection so that Federal funding and resources are applied in the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. This two-page snapshot describes the role of State and local governments in implementing the NIPP. This snapshot is available by contacting the NIPP Program Management Office at NIPP@dhs.gov.

Summary of the NIPP and SSPs provides the executive summary of the 2006 National Infrastructure Protection Plan (NIPP), as well as the executive summaries of each of the 17 supporting Sector-Specific Plans (SSPs). The 18th sector, Critical Manufacturing, is not included in this summary document. This document is available by contacting the NIPP Program Management Office at NIPP@dhs.gov.

Who's Who in Chemical Sector Security (October 2008) The document describes the roles and responsibilities of different DHS components with relation to Chemical

Security. See <http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/ChemicalSectorWhosWho.pdf>. For more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Who's Who in Emergency Services Sector describes the roles and responsibilities of the DHS components with relation to the Emergency Services Sector. Contact the Emergency Services Sector-Specific Agency ESSTeam@hq.dhs.gov.

IP Programs/Services/Events

Bomb-making Materials Awareness Program (BMAP) Developed in cooperation with the Federal Bureau of Investigation, BMAP is designed to assist local law enforcement agencies engage a wide spectrum of private sector establishments within their jurisdictions that manufacture, distribute, or sell products that contain home-made explosives (HMEs) precursor materials. BMAP outreach materials, provided by law enforcement to these local businesses, help employees identify HME precursor chemicals and other critical improvised explosive devices (IED) components of concern, such as electronics, and recognize suspicious purchasing behavior that could indicate bomb-making activity. To request materials or additional information, contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Buffer Zone Protection Program (BZPP) is a DHS administered infrastructure protection grant program targeted to local law enforcement (LLE). The BZPP provides funding to LLE for equipment acquisition and planning activities to address gaps and enhance security capabilities. It is also designed to increase first responder capabilities and preparedness by bringing together private sector security personnel and first responders in a collaborative security planning process that enhances the buffer zone – the area outside a facility that can be used by an adversary to conduct surveillance or launch an attack, around individual assets. Detailed BZPP annual grant guidance is available on the DHS/FEMA grants web site (<http://www.fema.gov/government/grant/bzpp/>).

Cesium Chloride In-Device Delay (Irradiator Hardening)

DHS, as the Nuclear Sector-Specific Agency, coordinates with Department of Energy's National Nuclear Security Administration (NNSA), which is collaborating with the private sector and other Federal agencies to enhance the security of blood and research irradiators that use cesium chloride sources (Cs-137). This effort includes the three major domestic manufacturers and vendors of self-contained irradiators containing Cs-137. The security enhancements consist of adding in-device delay (IDD) kit, which significantly increases the amount of time needed for the unauthorized removal of the radioactive material. The objective is to implement security enhancements that minimize impact to the user community. For more information, contact the Nuclear Sector-Specific Agency at nuclearSSA@hq.dhs.gov.

Chemical Facility Anti-Terrorism Standards (CFATS)

Chemical Facility Security Tip Line Individuals who would like to report a possible security concern involving the CFATS regulation at their facility or at another facility may contact the CFATS Chemical Facility Security Tip Line. They are welcome to report these concerns on the voicemail anonymously, or, if they would like a return call, they may leave their name and contact number. See www.dhs.gov/chemicalsecurity or Contact the CFATS Chemical Facility Security Tip Line at (877) FYI-4-DHS (1-877-394-4347). To report a potential security incident that has already occurred, call the National Infrastructure Coordination Center at (202) 282-9201.

Chemical Security Summit is an annual industry benchmark event, co-sponsored by DHS and the Chemical Sector Coordinating Council. See http://www.dhs.gov/files/programs/gc_1176736485793.shtm. For more information, contact the Chemical Sector-Specific Agency at 1-877-CHEMSEC, ChemicalSector@dhs.gov.

Chemical Security Compliance Assistance Visit (CAV)

Requests Upon request, the Infrastructure Security Compliance Division (ISCD) provides Compliance Assistance Visits (CAV) to Chemical Facility Anti-Terrorism Standards (CFATS)-covered facilities. CAVs are designed to provide in-depth knowledge of and assistance in a facility's efforts to comply with CFATS. Those interested in a CAV can find more information about these visits at DHS'

chemical security web site: www.dhs.gov/chemicalsecurity
To request a CAV, contact cscd.ieb@hq.dhs.gov.

Chemical Sector Monthly Suspicious Activity Calls

Employees of chemical companies, associations, and agencies who have a need to know information concerning potential physical and cyber threats and vulnerabilities to chemical infrastructure are eligible to listen in on the briefings. This monthly unclassified suspicious activity call for the Chemical Sector is scheduled for the first Wednesday of every month at 10:00AM EDT. The call-in information is as follows: DDI number: (800) 501-9384, Conference ID: 4754043. Contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Critical Infrastructure and Key Resource (CIKR) Asset Protection Technical Assistance Program (CAPTAP) assists State and local law enforcement, first responders, emergency management, and other homeland security officials understand the steps necessary to develop and implement a comprehensive CIKR protection program in their respective jurisdiction through the facilitated sharing of best practices and lessons learned. This includes understanding processes, methodologies, and resources necessary to identify, assess, prioritize, and protect CIKR assets, as well as those capabilities necessary to prevent and respond to incidents, should they occur. Through a partnership with the National Guard Bureau (NGB), the U.S. Army Research, Development and Engineering Command (RDECOM), and the DHS Office of Infrastructure Protection (IP) Infrastructure Information Collection Division (IICD), this service also provides Web-based and instructor-led training on Protected Critical Infrastructure Information (PCII) and the use of the *Automated Critical Asset Management System* (ACAMS) and *Integrated Common Analytical Viewer* (iCAV) system. See www.dhs.gov/files/programs/gc_1195679577314.shtm. For additional information, contact ACAMS-info@hq.dhs.gov, or (703) 235-3939.

Dams Sector Exercise Series (DSES) In collaboration with sector partners, including the Emergency Services SSA, the Dams SSA has developed an exercise series to test interoperability, preparedness, and regional resilience. DSES-09: Columbia River Basin was an effort undertaken in collaboration with the Pacific Northwest Economic Region,

U.S. Army Corps of Engineers, and Pacific Northwest region stakeholders to conduct exercise series along the Columbia River Basin to develop an Integrated Regional Strategy to improve disaster resilience and preparedness for the Tri-Cities region of Washington State. See <http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/assets/2009DamsSectorExerciseSeries-ColumbiaRiverBasinFactSheet.pdf>. For more information, contact the Dams Sector-Specific Agency at dams@dhs.gov.

Enhanced Critical Infrastructure Protection (ECIP) Visits

are conducted by Protective Security Advisors (PSAs) in collaboration with Critical Infrastructure and Key Resources (CIKR) owners and operators to assess overall facility security and increase security awareness. ECIP Visits are augmented by the Infrastructure Survey Tool (IST), a web-based tool that provides the ability to collect, process, and analyze ECIP survey data in near real time. Data collected during an ECIP visit is consolidated in the IST and then weighted and valued, which enables the development of ECIP metrics; conduct sector-by-sector and cross-sector vulnerability comparisons; identify security gaps and trends across CIKR sectors and sub-sectors; and establish sector baseline security survey scores. Private sector owners and operators interested in receiving an ECIP Visit should contact the PSA Field Operations Staff PSAFieldOperationsStaff@hq.dhs.gov (703) 235-5724.

National Infrastructure Advisory Council (NIAC) provides the President through the Secretary of Homeland Security advice on the security of the critical infrastructure sectors and their information systems. The Council is composed of a maximum of 30 members, appointed by the President from private industry, academia, and State and local government. For more information, see www.dhs.gov/niac.

National Infrastructure Protection Plan (NIPP) Sector Partnership improves the protection and resilience of the nation's critical infrastructure. The partnership provides a forum for the designated 18 critical sectors to engage with the federal government regularly on national planning, risk mitigation program identification and implementation, and information sharing. Additional information for private sector owners and operators of critical

infrastructure may be found at www.dhs.gov/cipac or by contacting Sector.Partnership@dhs.gov.

Office of Infrastructure Protection (IP) and National Infrastructure Protection Plan (NIPP) booths are available for exhibiting at national and sector-level events to promote awareness of the IP mission and the NIPP to government partners and infrastructure owners and operators. In addition, IP maintains a cadre of trained speakers who are available to speak on critical infrastructure protection and resilience issues at conferences and events. For more information, contact NIPP@dhs.gov.

Protected Critical Infrastructure Information (PCII) Program is an information sharing resource designed to facilitate the flow and exchange of critical infrastructure information (CII) between the private sector, DHS and Federal, State and local government entities. Private sector entities can voluntarily submit their CII to the PCII Program for use in Federal, State and local critical infrastructure protection efforts. Once the PCII Program has validated and marked the CII as PCII, the information will be safeguarded, disseminated and used in accordance with PCII requirements established pursuant to the Critical Infrastructure Information Act of 2002 and the implementing Regulation. PCII is protected from disclosure under Federal, State and local disclosure laws and from use in civil litigation and for regulatory purposes. Information about the PCII Program, including the CII Act of 2002, the implementing Regulation and the PCII Program Procedures Manual can be found on the Program's web site at www.dhs.gov/pcii. For additional information, contact pcii-info@dhs.gov, or (202) 360-3023.

Protective Security Advisor (PSA) Program Established in 2004, the PSA Program provides a locally-based DHS infrastructure security expert as the link between State, local, Tribal, territorial, and private sector organizations and DHS infrastructure protection resources. PSAs assist with ongoing State and local critical infrastructure and key resources (CIKR) security efforts, coordinate vulnerability assessments and training, support incident management, and serve as a vital channel of communication between private sector owners and operators of CIKR assets and DHS. Private sector owners and operators interested in

contacting their PSA should contact the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 235-5724.

Radiological Voluntary Security Enhancements DHS, as the Nuclear Sector-Specific Agency, coordinates with security experts from the Department of Energy's national laboratories, led by National Nuclear Security Administration (NNSA) headquarters staff, to provide security assessments, share observations, and make recommendations for enhancing security at facilities which house high-risk radioactive sources. The security upgrades are aimed at improving deterrence, control, detection, delay, response, and sustainability. Contact the Nuclear Sector-Specific Agency at nuclearSSA@hq.dhs.gov.

Regional Resiliency Assessment Program (RRAP) is a cooperative DHS led interagency assessment of specific critical infrastructure and key resources (CIKR) and regional analysis of the surrounding infrastructure, including key interdependencies. The emphasis for the RRAP is infrastructure "clusters," regions, and systems. The assessment and its final report are protected as Protected Critical Infrastructure Information (PCII). Regions are selected collaboratively by State and DHS Officials. Private sector CIKR owners and operators of infrastructure interested in receiving more information on the RRAP should contact the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 235-5724.

Research and Test Reactors (RTRs) Voluntary Security Enhancement Program As Chair of the Nuclear Government Coordinating Council (GCC) and a participant in the Joint GCC-Sector Coordinating Council (public-private) Research and Test Reactor (RTR) Subcouncil, the Nuclear Sector-Specific Agency coordinates with the Department of Energy's National Nuclear Security Administration on voluntary security enhancements at RTR facilities nationwide. Security enhancements are jointly determined by NNSA and the facility owner-operator and are funded by NNSA. These enhancements improve security beyond what is required by law and are consistent with RTR security regulations. For additional information, contact the Nuclear Sector-Specific Agency nuclearSSA@hq.dhs.gov.

Sector-Specific Agency Executive Management Office/Transportation Security Administration (TSA) Joint Exercise Programs Working with support and funding from TSA, this potentially multi-year program allows Critical Manufacturers with planning support by TSA's Intermodal Security Training and Exercise Program (ISTEP) to develop advanced table-top exercises that determine gaps and mitigate vulnerabilities in their respective transportation supply chains within the U.S. and cross border (particularly across Canadian and Mexican borders). For more information, contact the Critical Manufacturing Sector-Specific Agency cm-ssa@dhs.gov.

Security Outreach and Awareness Program (SOAP) provides critical information to chemical facility managers, control engineers, and IT administrators working in cyber-security management. Participating companies receive a free voluntary review of the security of their system networks and a summary of their cybersecurity policies and processes. For more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Security Seminar Exercise Series with State Chemical Industry Councils This collaborative effort between the DHS Chemical Sector-Specific Agency and various state chemical industry councils fosters communication between facilities and their local emergency response teams by encouraging representatives to share their insight, knowledge, and experiences during a facilitated table-top exercise. The exercises can include a wide-variety of topics and are catered towards the specific interests of the local chemical facilities. For more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Site Assistance Visit (SAV) is a facility vulnerability assessment focused on identifying security gaps and providing options for consideration to enhance protective measures. The SAV uses analyses of critical assets and current security measures, and scenario-based approaches such as assault planning to identify vulnerabilities and develop mitigation strategies. Following the assessment, DHS provides critical infrastructure and key resources (CIKR) owners and operators with an SAV Report,

protected as Protected Critical Infrastructure Information (PCII). The report details the facility information and offers options for consideration to increase the ability to detect and prevent terrorist attacks and reduce infrastructure vulnerabilities. Private sector owners and operators interested in receiving more information on the SAV should contact the DHS Protective Security Advisor (PSA) Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 235-5724.

IP Web-Based Resources

Automated Critical Asset Management System (ACAMS) is a secure, Web-based portal designed to help State and local emergency responders, such as infrastructure protection planners, homeland security officials, law enforcement personnel, and emergency managers, collect and organize critical infrastructure and key resource (CIKR) asset data as part of a comprehensive CIKR protection program. ACAMS is managed by the Office of Infrastructure Protection (IP) and continues to be developed in partnership with State and local communities. ACAMS benefits include it is provided at no cost for State and local use, it has public disclosure protections through the Protected Critical Infrastructure Information (PCII) program, and it is an integrated approach for collecting, protecting and analyzing CIKR asset data. The Federal Emergency Management Agency's National Preparedness Directorate also supports Critical Infrastructure Protection-related ACAMS training. See www.dhs.gov/ACAMS. For more information, contact ACAMS-info@hq.dhs.gov or (703) 235-3939.

Chemical Security Assessment Tool (CSAT) is an online tool developed by the Infrastructure Security Compliance Division (ISCD) to streamline the facility submittal and subsequent DHS analysis and interpretation of critical information used to 1) preliminarily determine facility risk, 2) assess high-risk facility's vulnerability 3) describe security measures at high risk sites and 4) ultimately track compliance with the CFATS program. CSAT is a secure information portal that includes applications for completing the User Registration, Top-Screen, Security Vulnerability Assessment (SVA), and Site Security Plan (SSP). ISCD provides user guides to assist with each of

these applications. See http://www.dhs.gov/files/programs/gc_1169501486197.shtm. Contact the CFATS Help Desk at csat@dhs.gov, (866) 323-2957.

Computer Based Assessment Tool (CBAT) is a cross-platform tool that integrates 360 degree geospherical video, geospatial and aerial imagery of facilities, surrounding areas, routes, and other areas of interest with a wide variety of other facility data, including evacuation plans, vulnerability assessments, standard operating procedures, and schematic/floor plans. By integrating this disparate data, the CBAT provides a comprehensive visual guide of a site that assists facility owners and operators, local law enforcement, and emergency response personnel to prepare for and respond to an incident. This resource is protected at the Protected Critical Infrastructure (PCII) and For Official Use Only (FOUO) level and is available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know. For more information, contact the DHS PSA Field Operations Staff: PSAFieldOperationsStaff@hq.dhs.gov or (703) 235-5724.

Critical Infrastructure and Key Resources (CIKR) Resource Center was designed to build awareness and understanding of each sector's scope and efforts to ensure CIKR protection and resiliency. The Center offers a centralized location page to find sector goals, plans, priorities, online training modules, activities and achievements, useful links, and other sector-based and cross sector resources. See <http://training.fema.gov/emiweb/is/IS860a/CIKR/index.htm>. For more information, contact IP_Education@hq.dhs.gov.

Dams Sector Consequence-Based Top Screen Methodology is an online tool based on the methodology developed to identify the subset of those high-consequence facilities whose failure or disruption could potentially lead to the most severe impacts. The Web-based tool was developed to support the implementation of the methodology across the sector. Available on LENS – <https://lens.iac.anl.gov>, for more information contact the Dams Sector-Specific Agency at dams@dhs.gov.

Dams Sector Suspicious Activity Reporting Tool is an online reporting tool within the Homeland Security

Information Network-Critical Sectors Dams Portal that was established to provide sector stakeholders with the capability to report and retrieve information pertaining to suspicious activities that may potentially be associated with pre-incident surveillance, and those activities related to the exploration or targeting of a specific critical infrastructure facility or system. It is accompanied by a Fact Sheet/Brochure. For additional information, contact the Dams Sector-Specific Agency at dams@dhs.gov.

DHS 20-Minute Retail Security Webinar is a web-based application dealing with security issues for all shopping center, mall, and retail employees. The webinar, produced by the Office of Infrastructure Protection's Protective Security Coordination Division (Office for Bombing Prevention), covers issues such as overall security awareness, suspicious purchases and unattended or suspicious packages. To request, contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

DHS 90-Minute Retail Security Webinar is a web-based application similar to the 20-minute Retail Security Webinar but designed for mall and retail professional security staff. The webinar, produced by the Office of Infrastructure Protection's Protective Security Coordination Division (Office for Bombing Prevention), offers greater detail on the topics covered in the 20-minute webinar, but with a greater scope and detail. Available on request. For additional information, please contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

General Information on Sector-Specific Agency Executive Management Office (SSA EMO) Critical Infrastructure and Key Resources (CIKR) Sectors and Programs provides an overview of the SSA EMO mission in CIKR risk management, and a description of SSA EMO Sectors. See http://www.dhs.gov/xabout/structure/gc_1204058503863.shtm. Contact the Sector-Specific Agency Executive Management Office at SSAexecsec@dhs.gov.

Homeland Security Information Network-Critical Sectors (HSIN-CS) is the primary information-sharing platform between the Critical Infrastructure/Key Resource sector stakeholders. HSIN-CS enables DHS and critical infrastructure owners and operators to communicate,

coordinate, and share sensitive and sector-relevant information to protect their critical assets, systems, functions and networks, at no charge to sector stakeholders. Vetted critical infrastructure private sector owners and operators are eligible to access HSIN-CS. To request access to HSIN-CS, please e-mail CIKRISIAccess@hq.dhs.gov. When requesting access, please indicate the critical infrastructure sector to which your company belongs and include your name, company, official e-mail address, and supervisor's name and phone number.

Integrated Common Analytical Viewer (iCAV) provides a suite of free, Web-based, infrastructure-focused geospatial visualization and analysis tools managed by the DHS Office of Infrastructure Protection. The two primary tools in the iCAV suite are the iCAV Next Generation Web-based visualization and analysis platform and the DHS Earth data service, both of which provide authoritative infrastructure data and various dynamic situational awareness feeds in standard geographic information system (GIS) data formats to authorized Homeland Security Information Network (HSIN) users at the Federal, State, and local levels and within the private sector. iCAV Next Generation is also the GIS platform for the *Automated Critical Asset Management System (ACAMS)*. See www.dhs.gov/icav. For more information, contact iCAV.info@hq.dhs.gov, or (703) 235-4949.

Risk Self-Assessment Tool (RSAT) for Stadiums and Arenas is a secure, Web-based application designed to assist managers of stadiums and arenas with the identification and management of security vulnerabilities to reduce risk to their facilities. The RSAT application uses facility input in combination with threat and consequence estimates to conduct a comprehensive risk assessment and provides users with options for consideration to improve the security posture of their facility. Accompanied by a Fact Sheet/Brochure. See http://www.dhs.gov/files/programs/gc_1259861625248.shtm. For additional information, please contact the Commercial Facilities Sector-Specific Agency at CFSteam@hq.dhs.gov.

Technical Resource for Incident Prevention (TRIPwire) (www.tripwire-dhs.net) is DHS's 24/7 online, collaborative,

information-sharing network for bomb squad, law enforcement, and other first responders to learn about current terrorist improvised explosive device (IED) tactics, techniques, and procedures. The system combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to assist law enforcement anticipate, identify, and prevent IED incidents. To request additional information, contact DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

TRIPwire Community Gateway (TWCG) is a TRIPwire web portal designed specifically for the Nation's CIKR owners, operators, and private security personnel. TWCG provides expert threat analyses, reports, and relevant planning documents to help key private sector partners anticipate, identify, and prevent improvised explosive device (IED) incidents. TWCG shares IED-related information tailored to each of the 18 CIKR Sectors as well as a Community Sector for educational institutions, in accordance with the National Infrastructure Protection Plan (NIPP). TWCG information is currently available to vetted private sector critical infrastructure owners and operators with a demonstrated need to know through the Homeland Security Information Network-Critical Sectors (HSIN-CS) (<https://cs.hsin.gov/>) online secure portal. To request additional information, contact the DHS Office for Bombing Prevention at OBP@dhs.gov, (703) 235-5723.

Voluntary Chemical Assessment Tool (VCAT) is a secure, Web-based application that allows owners and operators to identify their facilities' current risk level using an all-hazards approach and facilitates a cost-benefit analysis by allowing them to select the best combination of physical security countermeasures and mitigation strategies to reduce overall risk. There is also a brochure that describes the features and benefits of VCAT and includes instructions on how to gain access to the tool. Accompanied by Fact Sheet/Brochure. Available on request. For more information, contact the Chemical Sector-Specific Agency at ChemicalSector@dhs.gov.

Science & Technology Directorate (S&T)

The S&T Directorate's mission is to improve homeland security by providing to customers state-of-the-art technology that helps them achieve their missions. S&T customers include the operating components of the Department, State, local, Tribal and territorial emergency responders and officials. www.dhs.gov/scienceandtechnology

S&T Programs

S&T Collaboration in Data and Visual Analytics both internally within the DHS research community as well as externally enables S&T to leverage both its funding and technical expertise by taking advantage of research activities underway in government laboratories, industry laboratories, and in universities across the world. In 2008 S&T's Command, Control, and Interoperability Division (CCI) established a five-year joint program with the National Science Foundation (NSF) on the Foundations of Visual and Data Analytics. In 2009, CCI contributions were matched more than twofold by NSF, and 16 universities have been awarded research grants. Additionally, DHS has signed formal international collaboration agreements between Canada and Germany, and discussions with United Kingdom (UK) and France are underway. These efforts have resulted in the development of joint scientific and technical projects in visualization and data analytics. For more information, contact IVAC@dhs.gov.

Commercial Mobile Alert Service (CMAS) is a component of the Integrated Public Alert and Warning System. It is an alert system that will have the capability to deliver relevant, timely, effective, and targeted alert messages to the public through cell phones, blackberries, pagers, and other mobile devices. This national capability will ensure more people receive Presidential, Imminent Threat, and AMBER alerts. In support of this effort, the first CMAS Forum was recently held. The purpose of the Forum was to convene the alerts and warnings community-including message originators, emergency responder organizations, industry organizations, academia, and organizations representing special needs populations-to address critical issues and determine next steps for the CMAS Research, Development, Test and Evaluation (RDT&E) program. Action teams based around the initiatives that came out of the CMAS Forum were created and are being populated.

<http://www.cmasforum.com/>, contact cmasforum@sra.com.

Commercialization Office is responsible for the development and implementation of a commercialization process and for the execution of two innovative public-private partnerships that leverage research and development efforts in the private sector that are aligned to detailed operational requirements from Department stakeholders. The Commercialization Office also spearheads DHS S&T's outreach efforts that inform the private sector on "How to do business with DHS." See http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm. Contact: SandT_Commercialization@hq.dhs.gov, 1-(202) 254-6749.

Cyber Security Research and Development Center (CSRDC) S&T has the mission to conduct research, development, test and evaluation, and timely transition (RDTE&T) of cyber security capabilities to operational units within DHS, as well as Federal, State, local and critical infrastructure sector operational end-users for homeland security purposes. As part of its cyber security mission, DHS/S&T has established the Cyber Security Research and Development Center (CSRDC). As part of its cyber security mission, DHS/S&T utilizes CSRDC to focus cyber security RDTE&T efforts and to involve the best practices and personnel from academic, private industry and federal and national laboratories. The Cyber Security R&D Center was established by the Department of Homeland Security in 2004 to develop security technology for protection of the U.S. cyber infrastructure. For example, the Linking the Oil and Gas Industry to Improve Cyber Security (LOGIIC) project, which addresses security vulnerability issues related to the oil and gas industry's Process Control Systems (PCS) and Supervisory Control and Data Acquisition systems. The comprehensive monitoring system developed in LOGIIC provides an integrated, multi-component security solution that monitors a PCS for abnormal activity. The Center conducts its work through

partnerships between government and private industry, the venture capital community, and the research community. The Center conducts its work through partnerships between government and private industry, the venture capital community, and the research community. This web site provides information about this and other DHS S&T projects, workshop information and presentations, cybersecurity news, events and outreach information. See <http://www.cyber.st.dhs.gov/>, contact csrdc@dhs.gov.

Defense Technology Experimental Research (DETER) The DETER testbed was jointly funded by S&T and the National Science Foundation (NSF) and has been open to the research community since March 2004. The centerpiece of the experimental environment is a safe (quarantined), but realistic, network testbed based on a mesh of clusters of homogeneous experimental nodes. DETER is a critical national cyber-security experimental infrastructure which enables users to study and evaluate a wide range of computer security technologies including encryption, pattern detection, intrusion tolerant storage protocols, next generation network simulations; as well as, develop and share educational material and tools to train the next generation of cyber-security experts. Existing testing facilities cannot handle experiments on a large enough scale to represent today's operational networks or the portion of the Internet that might be involved in a security attack. Industry has only been able to test and validate new security technologies in small- to medium-scale private research laboratories that do not adequately simulate a real networking environment. Newsletters, published papers, videos and update presentations can be viewed at <http://www.isi.edu/deter/>. Contact testbed-ops@isi.deterlab.net.

Domain Name System Security Extensions (DNSSEC) Deployment Coordinating Initiative To strengthen the domain name system against attacks, S&T has initiated the DoDNSSEC Deployment Initiative. DNSSEC has been

developed to provide cryptographic support for domain name system (DNS) data integrity and authenticity. DHS sponsors a community-based, international effort to transition the current state of DNSSEC to large-scale global deployment, including sponsorship of the DNSSEC Deployment Working Group, a group of experts active in the development or deployment of DNSSEC. It is open for anyone interested in participation. The DNSSEC web site contains articles, published research papers, DNSSEC Tools, Case Studies, Workshop information and presentation materials. See <http://www.dnssec-deployment.org/>.

Emergency Data Exchange Language (EDXL) messaging standards help emergency responders exchange critical data, including alerts, hospital capacity, and availability of response personnel and equipment. Industry can leverage these standards to better ensure compliance and interoperability for their products. See <http://www.oasis-open.org>.

FutureTECH™ program targets critical research/innovation focus areas that detailed the long-term needs of the Department to partner with the private sector, university communities and national labs in the development of technology for future use by Department stakeholders. See http://www.dhs.gov/files/programs/gc_1242058794349.shtm. Contact SandT_Commercialization@hq.dhs.gov, (202) 254-6749.

Long Range Broad Agency Announcement (BAA) is a funding mechanism for original research that addresses DHS capability gaps, which are specified in Part I of its announcement under Research Areas of Strategic Interest. It also funds original research that advances the foundations of technical knowledge in the basic sciences. Successful submissions to the Long Range BAA answer questions such as, “What research problem do you propose to solve? How is your solution different from and superior to currently available solutions or from the efforts of others to achieve a similar solution? What data and analysis do you have to support the contention that funding your R&D project will result in a significant increase in capability for DHS?” All of S&T’s divisions and special programs receive and evaluate submissions, as appropriate, through the Long Range BAA. For submission

instructions, evaluation criteria, and to apply online, visit: <https://baa.st.dhs.gov/>.

National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management (BIdM) encourages greater collaboration and sharing of information on biometric activities among government departments and agencies; commercial entities; state, regional, and international organizations; and the general public. See www.Biometrics.gov, contact info@biometrics.org.

Project 25 Compliance Assessment Program (P25 CAP) was established, in coordination with the National Institute of Standards and Technology (NIST), to provide a process for ensuring that equipment complies with P25 standards, meets performance requirements, and is capable of interoperating across manufacturers. P25 standards are focused on developing radios and other components that can interoperate regardless of manufacturer. P25 CAP allows emergency responders to confidently purchase and use P25-compliant products, and the Program represents a critical step toward allowing responders to communicate with their own equipment. In 2009, the first eight laboratories were officially recognized by DHS as part of the P25 CAP. A DHS-approved laboratory is authorized to produce test reports for P25 equipment. NPPD/CS&C/OEC coordinates the implementation of P-25 compliance standards with S&T to promote communications interoperability, and by encouraging grant recipients to purchase P-25 compliant equipment and technologies with Federal grant funding. See <http://www.safecomprogram.gov/SAFEKOM/currentprojects/project25cap/>, contact P25CAP@dhs.gov.

The Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) will facilitate the accessibility of computer and network operational data for use in cyber defense research and development through large-scale research datasets. PREDICT allows partners to pursue technical solutions to protect the public and private information infrastructure. It also provides researchers and developers with real network data to validate their technology and products before deploying them online. This initiative represents an

important three-way partnership between the federal government, critical information infrastructure providers, and the security development community (both academic and commercial). Within this project, the Los Angeles Network Data Exchange and Repository (LANDER), Network Traffic Data Repository to Develop Secure Information Technology Infrastructure, Routing Topology and Network Reliability Dataset Project, and Virtual Center for Network and Security Data serve as data set collectors and hosts. The PREDICT Data Coordinating Center helps manage and coordinate the research data repository. See <https://www.predict.org>, contact PREDICT-contact@rti.org.

Science & Technology Basic Research Focus Areas represent the technological areas in which S&T seeks to create and/or exploit new scientific breakthroughs and help guide the direction of the S&T research portfolio, within resource constraints, to provide long-term science and technology advances for the benefit of homeland security. The focus areas identified by S&T’s Research Council, with input from our customers and the research community, summarize the fundamental work needed to support the future protection of our Nation. See http://www.dhs.gov/xabout/structure/gc_1242157296000.shtm. Contact the Director of Research, SandT.Research@dhs.gov, (202) 254-6068.

SECURE™ Program leverages the experience and resources of the private sector to develop fully deployable products/services based on Department generated and vetted, detailed operational requirements documents (ORDs) and a conservative estimate of the potential available market of Department stakeholders. See http://www.dhs.gov/files/programs/gc_1211996620526.shtm. Contact sandt_commercialization@hq.dhs.gov, (202) 254-6749.

Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) is a program managed by the Office of SAFETY Act Implementation (OSAI). The program evaluates and qualifies technologies for liability protection in accordance with the *Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002* and the supporting regulations of the Final Rule (6 CFR Part 25) implemented on July 10, 2006. As part of the

Homeland Security Act of 2002 (Public Law 107-296), the SAFETY Act provides risk management and liability protections for sellers of Qualified Anti-Terrorism Technologies. The purpose of the SAFETY Act is to ensure that the threat of liability does not deter potential manufacturers or sellers of effective anti-terrorism technologies from developing, deploying and commercializing these technologies that meet homeland security objectives. See www.SAFETYAct.gov. Contact SAFETYActHelpDesk@dhs.gov, (866) 788-9318.

Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition TCIP highlights DOJ, DHS, and DoD technologies; RDT&E investments; and training tools for the emergency responder community. It provides a forum for emergency responders to discuss best practices and exchange information and offers a unique opportunity for emergency responders; business and industry; academia; and local, Tribal, State, and Federal stakeholders to network, exchange ideas, and address common critical incident technology, preparedness, response and recovery needs, protocols, and solutions. See <http://www.tcipexpo.com>.

DHS Technology Transfer Program serves as the focal point for technology transfer activities at the Department of Homeland Security. Currently, DHS operates from one centralized Office of Research and Technology Applications (ORTA) to manage technology transfers at each of its laboratories and throughout the Department. The Technology Transfer Program promotes the transfer and/or exchange of technology with industry, State and local governments, academia, and other Federal agencies. The technologies developed and evaluated within the DHS can have a tremendous potential for commercial applications throughout the nation and dramatically enhance the competitiveness of individual small businesses as well as expanding areas of exploration and cooperation for all non-federal partners. For more information, visit http://www.dhs.gov/xabout/structure/gc_1264538499667.shtm

Voice over Internet Protocol (VOIP) project researches IP-enabled communication technologies and evaluates promising solutions. This project will enable the

emergency response community to confidently deploy and use IP technologies and integrate video, cellular, and satellite communications. In FY 2009, the project initiated testing and evaluation of IP solutions and completed the first VoIP profile as prioritized by the emergency response community. Ultimately, the project will complete the development of a set of standards based on the needs of emergency responders. DHS and the U.S. Department of Commerce (DOC) gathered key stakeholders from both the public safety and industry communities to form a working group. Led by the DHS Office for Interoperability and Compatibility and DOC's Public Safety Communications Research Program, the Public Safety VoIP Working Group works to define and clarify the expectations for VoIP in the public safety environment. See <http://www.safecomprogram.gov/SAFE/COM/currentprojects/voip/> and <http://www.pscr.gov/projects/broadband/voip/voip.php>, contact VoIP_Working_Group@sra.com.

Video Quality in Public Safety (VQIPS) As video technology has evolved, the array of options for public safety practitioners has grown and the interoperability challenges have become increasingly complex. Thus the need has emerged for public safety to collectively articulate their video quality needs to the manufacturing community. A VQIPS Working Group was formed to focus on the major policy, technology, and practical uses and challenges of public safety video systems. Comprised of emergency responders, academics, Federal partners, and vendors, the Working Group is currently creating an end-user guide to help practitioners articulate their needs to vendors when they look to purchase or upgrade video systems. See <http://www.safecomprogram.gov/SAFE/COM/currentprojects/videoquality/videoquality.htm> and http://www.pscr.gov/projects/video_quality/video_about.php. Contact VQIPS_Working_Group@sra.com.

DHS Centers of Excellence

DHS Center of Excellence: Awareness & Location of Explosives-Related Threats (ALERT) develops new means and methods to protect the nation from explosives-related threats, focusing on detecting leave-behind Improvised Explosive Devices, enhancing aviation cargo security, providing next-generation baggage screening, detecting

liquid explosives, and enhancing suspicious passenger identification. Resources include **Training Opportunities and courses in Explosives**. See <http://www.northeastern.edu/alert/> and <http://energetics.chm.uri.edu>. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: Preparedness and Catastrophic Event Response (PACER) optimizes our nation's preparedness in the event of a high-consequence natural or man-made disaster, as well as develops guidelines to best alleviate the effects of such an event. Resources available include a **Modeling & Simulation Catalog**, a **Model Memorandum of Understanding (MOU) between Hospitals during Declared Emergencies**, and the **Electronic Mass Casualty Assessment and Planning Scenarios Applet (EMCAPS)**. See <http://www.pacercenter.org/>. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Risk and Economic Analysis of Terrorism Events (CREATE) develops advanced tools to evaluate the risks, costs and consequences of terrorism, and guides economically viable investments in countermeasures that will make our Nation safer and more secure. Resources include: an **Executive Program for Counter-Terrorism, Aviation Safety & Security Program** covering the use of models and tools for evaluation of security and anti-terrorism, **Degree Specializations in Homeland Security Analysis**, and the **National Interstate Economic Model (NIEMO)** an operational multi-regional input-output economic impact model. See <http://create.usc.edu/>. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Food Protection and Defense (NCFPD) defends the safety and security of the food system from pre-farm inputs through consumption by establishing best practices, developing new tools and attracting new researchers to prevent, manage and respond to food contamination events. Resources include: **Food and Agriculture Criticality Assessment Tool (FAS-CAT)**; **FoodSHIELD**, a web-based system for communication, coordination, community-building, education, and training among the nation's food and agriculture sectors; **Exercise Design and Facilitation**; **Event and Consequence Models**; **Continuous Tracking and**

Analyzing Consumer Confidence in the U.S. Food Supply Chain; Supply Chain Benchmarking Diagnostic Tool; Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks from 1961-2005; Mass Production of Detection and Neutralizing Antibodies; Biosensors Courses; The Biosecurity Research Institute (BRI); The Frontier Program; Food Protection and Food Safety and Defense Graduate Certificate Programs; The National Agricultural Biosecurity Center (NABC); Optimized Detection of Intentional Contamination using Simulation Modeling; Risk Communication, Message Development/Evaluation and Training; decontamination protocols; and Regulatory, Policy, Technical, and Practical Issues related to Contaminated Food Disposal. For more information, see <http://www.ncfpd.umn.edu/> or contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Foreign Animal and Zoonotic Disease Defense (FAZD) protects against the introduction of high-consequence foreign animal and zoonotic diseases into the United States, with an emphasis on prevention, surveillance, intervention and recovery. Resources include **Courses on Foreign Animal and Zoonotic Diseases, Public and Private sector Awareness Materials, Field Guide to Handling Contaminated Animal and Plant Materials, Mass Livestock Carcass Management workshop, Specialists in Foreign Animal and Zoonotic Diseases, an Avian Influenza Study Curriculum, a Guide to Developing an Animal Issues Emergency Management Plan**, and a compilation of materials pertaining to the **Economic Impact of Foreign Animal Diseases to the United States**. See <http://fazd.tamu.edu/>. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Center for Command, Control, and Interoperability (C2I) creates the scientific basis and enduring technologies needed to analyze massive amounts of information from multiple sources to more reliably detect threats to the security of the nation, its infrastructures and to the health and welfare of its populace. These new technologies will also improve the dissemination of both information and related technologies. Co-led by Purdue University and Rutgers University, available educational opportunities are geared

towards educating the next generation of homeland security professionals with initiatives that span the entire career development pipeline, ranging from K-12 programs through undergraduate and graduate level work, to professional education and training. For more information, see <http://www.purdue.edu/discoverypark/vaccine/> and <http://www.ccicada.org/> or contact universityprograms@dhs.gov.

DHS Center of Excellence: Center for Maritime, Island, & Remote/Extreme Environment Security led by the University of Hawaii in Honolulu for maritime and island security and Stevens Institute of Technology in Hoboken, N.J., for port security, will strengthen maritime domain awareness and safeguard populations and properties unique to U.S. islands, ports, and remote and extreme environments. Programs include the **MARCOOS High Frequency Radar Network** and the **New York /New Jersey Harbor Maritime Awareness System**. See <http://cimes.hawaii.edu/> and <http://www.stevens.edu/csr/>. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Transportation Security Center of Excellence (NTSCOE) develops new technologies, tools and advanced methods to defend, protect and increase the resilience of the nation's multi-modal transportation infrastructure and education and training base lines for transportation security geared towards transit employees and professionals. Educational programs include **H1N1 Training for transit agency managers and employees, Educational opportunities in transportation** at the Mineta Transportation Institute (MTI), **Online Master of Science in Homeland Security Management degree** from the Homeland Security Management Institute of Long Island University. See <http://www.cti.uconn.edu/>, <http://www.tougaloo.edu/>, <http://transportation.tsu.edu/NTSCE/home.htm>, <http://www.policy.rutgers.edu/centers/nti.php>, <http://www.southampton.liu.edu/homeland/index.html>, <http://transweb.sisu.edu/>, and <http://www.mackblackwell.org/>. For more information, contact universityprograms@dhs.gov.

DHS Center of Excellence: National Consortium for the Study of Terrorism and Responses to Terrorism (START)

informs decisions on how to disrupt terrorists and terrorist groups, while strengthening the resilience of U.S. citizens to terrorist attacks. Resources include the **Minorities at Risk Organizational Behavior**, an open-source dataset covering political organizations representing the interests of ethnic groups whose political status and behavior is tracked by the Minorities at Risk project; the **Global Terrorism Database**, an open-source database including information on terrorist events around the world from 1970 through 2007; **Terrorist Organization Profiles**; and **Training Programs related to the Human Causes and Consequences of Terrorism**. See <http://www.start.umd.edu/start/>. For more information, contact universityprograms@dhs.gov.

Transportation Security Administration (TSA)

The Transportation Security Administration protects the Nation's transportation systems to ensure freedom of movement for people and commerce. www.tsa.gov

TSA Training and Education

Airport Watch/AOPA Training TSA partnered with the Aircraft Owners and Pilots Association (AOPA) to develop a nationwide Airport Watch Program that uses the more than 650,000 pilots as eyes and ears for observing and reporting suspicious activity. The Airport Watch Program includes warning signs for airports, informational literature, and a training video to teach pilots and airport employees how to enhance security at their airports. For additional information including a training video, visit <http://www.aopa.org/airportwatch/>.

Alien Flight/Flight School Training The Interim Final Rule, Flight Training for Aliens and Other Designated Individuals and Security Awareness Training for Flight School Employees, requires flight schools to ensure that each of its flight school employees who has direct contact with students (including flight instructors, ground instructors, chief instructors and administrative personnel who have direct contact with students) receive both initial and recurrent security awareness training. Flight schools may either choose to use TSA's security awareness training program or develop their own program. For more information, see http://www.tsa.gov/what_we_do/tsnm/general_aviation/flight_school_security.shtm.

First Observer™ Training TSA provides funding for the First Observer™ program under the Trucking Security Program grant. One component of First Observer is a security awareness training program. The First Observer™ web site has online training modules for Trucking and School Bus with nine other modules planned. You can log on to the web site for training at: <http://www.firstobserver.com/training/home.php>. You can call (888) 217-5902 or E-mail (Firstobserver@hms-world.com) for more information.

Hazmat Motor Carrier Security Action Item Training (SAIT) Program addresses the TSA recommended security actions that were developed by the TSA for the hazmat transportation industry. For more information, see <http://www.tsa.gov/highway>. Or contact TSA Highway and Motor Carrier Division, highwaysecurity@dhs.gov.

Hazmat Motor Carrier Security Self-Assessment Training Program addresses the requirements contained in 49 Code of Federal Regulations (CFR), Part 172.802, which requires motor carriers that transport placarded amounts of hazardous materials to develop a plan that adequately addresses security risks related to the transportation of hazardous materials. Training materials can be found at http://www.tsa.gov/what_we_do/tsnm/highway/self_training.shtm. Contact TSA Highway and Motor Carrier Division with any questions at: highwaysecurity@dhs.gov.

IED Recognition and Detection for Railroad Industry Employees Training (CD) is a self-paced program that leads users through four separate modules which focus on heightening rail employees' awareness of suspicious activity. Topics covered include an overview of the terrorist threat, high risk targets, improvised explosive device recognition, and inspection and response procedures. See http://www.tsa.gov/what_we_do/tsnm/freight_rail/training.shtm, or contact freightrailsecurity@dhs.gov.

Intermodal Security Training and Exercise Program (I-STEP) supports TSA's Transportation Sector Network Management (TSNM) Modal Security Managers with exercises and training. The program is designed to support all transportation security partners with security objectives and training that has clear and consistent performance measures. See http://www.tsa.gov/what_we_do/layers/istep/index.shtm, contact i-step@dhs.gov, (571) 227-5150.

Land Transportation Antiterrorism Training Program (LTATP) is a joint effort by TSA and the Federal Law

Enforcement Training Center (FLETC) to enhance knowledge, skills, and capabilities of law enforcement and security officials to prevent acts of terrorism. The program recognizes that security at most land transportation systems is accomplished by a cooperative effort of private sector and local, State, and federal government personnel. Through a curriculum focused on surface transportation security, this 5-day program provides the participants with tools to protect the land transportation infrastructure, including rail, mass transit and bus operations, and most importantly passengers and employees. See <http://www.fleetc.gov/training/programs/counterterrorism-division/land-transportation-antiterrorism-training-program-ltstp>, contact: MassTransitSecurity@dhs.gov.

Maritime Passenger Security Courses TSA's Port & Intermodal Security Division creates and distributes training courses for passenger vessel employees. The courses address topics to improve passenger vessel employees' security awareness in their operating environments and to increase the effectiveness of their responses to suspicious items and persons that they might encounter. Courses available include: "Security Awareness For Passenger Vessel Employees," "IED/VBIED Recognition and Response," and "Crowd Control." To order, contact TSA Port & Intermodal Security Division at Maritime@dhs.gov, (571) 227-3556.

Mass Transit and Passenger Rail - Bomb Squad Response to Transportation Systems Through training and scenario-based exercises, this program expands regional capabilities to respond to a threat or incident involving a suspected explosive device in mass transit and passenger rail systems. Bomb technicians from law enforcement forces in the system's operating area are placed in the mass transit or passenger rail environment to confront exercise situations necessitating coordinated planning and execution of operations to identify, resolve, and, if appropriate, render harmless improvised explosive devices. These joint activities build relationships and skills

in a challenging operational setting, advancing operational partnerships that enhance capabilities to accomplish the prevention and response missions. Contact: MassTransitSecurity@dhs.gov.

Mass Transit and Passenger Rail - Field Operational Risk and Criticality Evaluation (FORCE) The purpose of this process is to establish a threat-based, risk-managed protocol that is particularly effective for regional use. This risk assessment evaluates threat, vulnerability, and consequence from a variety of vantage points, focusing primarily on the rail and bus properties but also surveying intermodal and interdependent critical infrastructure and key resources. The approach for any given region will apply the methodology that best addresses the needs of the particular transit agencies. The results of this assessment aid agencies in setting risk mitigation priorities and completing requests for grant awards and advance regional security collaboration. It is also adaptable to assist with new start-up properties about to come online or transit agencies with aggressive future expansion initiatives as well as regions hosting special security events. For more information, contact MassTransitSecurity@dhs.gov.

Mass Transit Smart Security Practices

In mass transit and passenger rail, TSA has produced a compilation of smart security practices drawn from the results of the comprehensive security assessments completed under the Baseline Assessment for Security Enhancement (BASE) program that evaluate agencies posture in the Security and Emergency Management Actions Items. TSA coordinated the preparation of this compilation with each agency with one or more practices recognized in a BASE assessment, ensuring an accurate description of the practice the agency developed and implemented and securing contact information for an official in the agency that professional colleagues may consult for more information. This compilation fosters communication among security professionals in mass transit and passenger rail nationally with the specific objective of expanding adoption of these most effective practices, tailored as necessary to each agency's operating environment. With the December 2009 update, the compilation now consists of some 80 smart security practices, many of which focus on regional partnerships,

random security patrols, sweeps, and surges, and intelligence and security information sharing, and training and public awareness. For more information, please contact: MassTransitSecurity@dhs.gov.

Mass Transit Security Training Program Guidelines

Recognizing the vital importance of training frontline employees, TSA developed and implemented a focused security training initiative under the Transit Security Grant Program (TSGP) in February 2007. TSA coordinated development of this initiative through the Mass Transit SCC and the PAG. The resulting Mass Transit Security Training Program provides guidelines to mass transit and passenger rail agencies on the types of training to be provided by category of employee. The guidance further identifies specific courses developed under Federal auspices through the FTA, the Federal Emergency Management Agency, and TSA that are available to ensure employees are trained in the designated areas. Finally, the Department revised the eligible costs under the TSGP to allow coverage of overtime expenses incurred when employees receive training courses. For Mass Transit Security Training Program Guidelines, see http://www.tsa.gov/assets/pdf/TSGP_Training_IB243.pdf, for TSGP – Approved Training Programs List see http://www.tsa.gov/assets/pdf/approved_vendor_list.pdf. MassTransitSecurity@dhs.gov.

Operation Secure Transport (OST) is security awareness training for the Over-the-Road Bus industry. The training program will be available on CD and online. The training modules will be broken down into the following categories: Driver; Maintenance; Terminal Employees; Management; and Crisis Response. OST will have a link on the TSA Highway and Motor Carrier webpage in the near future: www.tsa.gov/highway. Contact TSA HMC with any questions at: highwaysecurity@dhs.gov.

Pipeline Security Awareness for the Pipeline Industry Employee Training CD and Brochures is a compact disc-based security awareness training program. The training is intended for distribution to interested pipeline companies and is centered on heightening pipeline employees' awareness of suspicious activity and their importance in keeping our nation's pipeline system secure. The training is useful to all pipeline company employees –

administrative, operations, and security personnel – who need a basic level of awareness and understanding of pipeline security. To further enhance the information contained in the pipeline security awareness training CD, TSA produced the brochures “Pipeline Security Awareness for Employees” and “Good Neighbors! A Pipeline Security Neighborhood Watch.” The CD and brochures may be requested on the TSA Pipeline Security web site at http://www.tsa.gov/what_we_do/tsnm/pipelines/training.shtm. For more information contact the Pipeline Security Division at PipelineSecurity@dhs.gov.

Public Transportation Emergency Preparedness

Workshop - Connecting Communities Program brings mass transit and passenger rail agencies' security and emergency management officials together with Federal, State, local, and tribal government representatives and the local law enforcement and first responder community to discuss security prevention and response efforts and ways to work together more effectively to prepare and protect their communities. The 2-day Workshops enable the participants to apply their knowledge and experiences to a range of security and emergency response scenarios. The overall purpose is to foster dialogue, advance cooperative planning efforts, review past experiences, analyze best practices, and improve overall interoperability, resource utilization, and prevention and response capabilities to address threats, security incidents, and natural disasters. See <http://www.connectingcommunities.net>, contact: MassTransitSecurity@dhs.gov.

School Transportation Security Awareness (STSA) was developed by TSA in conjunction with the National Association of State Directors of Pupil Transportation Services, the National Association of Pupil Transportation and the National School Transportation Association to provide much needed security awareness information and training to the school transportation industry. STSA focuses on terrorist and criminal threats to school buses, bus passengers and destination facilities. It is designed to provide school bus drivers, administrators, and staff members with information that will enable them to effectively identify and report perceived security threats, as well as the skills to appropriately react and respond to a security incident should it occur. See

http://www.tsa.gov/what_we_do/tsnm/highway/stsa.shtm, contact highwaysecurity@dhs.gov.

TSA Publications and Guidance

Federal Bureau of Investigation (FBI) Terrorism

Vulnerability Self-Assessment (Appendix B of the FTA SEPP guide – page 139 to 147). See <http://transit-safety.volpe.dot.gov/publications/security/PlanningGuide.pdf>. Contact the TSA Highway and Motor Carrier offices with any questions at: highwaysecurity@dhs.gov.

Federal Motor Carrier Safety Administration: Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials

See <http://www.fmcsa.dot.gov/safety-security/hazmat/security-plan-guide.htm>. Contact the TSA Highway and Motor Carrier offices with any questions at: highwaysecurity@dhs.gov.

General Aviation Security Guidelines In April 2003, TSA requested the Aviation Security Advisory Committee (ASAC) establish a Working Group made up of industry stakeholders to develop guidelines for security enhancements at the nation's privately and publicly owned and operated general aviation (GA) landing facilities. The resulting document constitutes a set of federally endorsed guidelines for enhancing airport security at GA facilities throughout the nation. It is intended to provide GA airport owners, operators, and users with guidelines and recommendations that address aviation security concepts, technology, and enhancements. For more information, visit: http://www.tsa.gov/what_we_do/tsnm/general_aviation/airport_security_guidelines.shtm

Keep the Nation's Railroad Secure (Brochure) assists railroad employees to recognize signs of a potential terrorist act. It is to be used in conjunction with a railroad company's existing security policies and procedures and may be modified to display the company's emergency contact information for ease of reference. See http://www.tsa.gov/what_we_do/tsnm/freight_rail/trainimg.shtm or contact freightrailsecurity@dhs.gov.

Laminated Security Awareness Driver Tip Card contains the following topics: Bus Operator Alerts; Hijacking; Evacuating the Vehicle; Awareness and What to Look For; and Possible Chemical/Biological Weapons. See http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm. Any questions can be sent to highwaysecurity@dhs.gov.

HAZMAT TRUCKING GUIDANCE: Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs)

See http://www.tsa.gov/what_we_do/tsnm/highway/hssm_sai.shtm. Contact the TSA Highway and Motor Carrier offices with any questions at: highwaysecurity@dhs.gov.

Highway and Motor Carrier Awareness Posters include Motorcoach Awareness Posters for terminals: "Watch for Suspicious Items" and "Watch for Suspicious Behaviors" for terminals as well as a School Transportation Employee Awareness poster. See http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm. Any questions can be sent to highwaysecurity@dhs.gov.

Mass Transit Employee Vigilance Campaign The "NOT ON MY SHIFT" program employs professionally-designed posters to emphasize the essential role that mass transit and passenger rail employees play in security and terrorism prevention in their systems. Adaptable templates enable each transit agency to tailor the product to its operations by including the system's logo, photographs of their own agency's employees at work, and quotes from the senior leadership, law enforcement and security officials, or frontline employees. The personalized approach has proven effective in gaining employees' attention and interest, supporting the participating transit and rail agencies' efforts to maintain vigilance for indicators of terrorist activity. TSA designs the posters based on the preferences of the particular mass transit or passenger rail agency. For more information contact: MassTransitSecurity@dhs.gov.

Mass Transit and Passenger Rail - Additional Guidance on Background Checks, Redress and Immigration Status The additional guidance on background checks, redress and immigration status supplement item 14 of the Security and Emergency Management Action Items, which recommends

that the operators of mass transit conduct background investigations, such as criminal history and motor vehicle records, on all new frontline operations and maintenance employees and those employees and contractors with access to sensitive security information and security critical facilities and systems. This guidance addresses factors to consider on the recommended scope of and procedures for voluntarily conducted background checks. See http://www.tsa.gov/assets/pdf/guidance_employee_background_checks.pdf, contact: MassTransitSecurity@dhs.gov.

MOTORCOACH GUIDANCE: Security and Emergency Preparedness Plan (SEPP) See <http://www.tsa.gov/assets/doc/sepp.doc>. Contact the TSA HMC offices with any questions at: highwaysecurity@dhs.gov.

Rail Security Rule Overview On November 26, 2008 the Department of Homeland Security published a regulation governing security in the freight rail industry. The regulation not only affects freight railroads, but their customers as well. This presentation provides a high-level overview of the Rail Security Rule and information regarding the requirements of the regulation. See http://www.tsa.gov/assets/pdf/rail_rule_overview_for_stakeholder_workshops_mar_09.pdf (pdf – 229 KB), for more information contact: Scott.Gorton@dhs.gov.

Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems incorporate insights and experience of industry stakeholders, including airport and airline representatives, planners, architects, baggage handling system designers, and equipment manufacturers. The PGDS is intended to assist planners and designers in developing cost-effective solutions and to convey TSA requirements for checked baggage inspection systems. The PGDS emphasizes best practices associated with screening system layouts and addresses other factors necessary to actively manage system costs and performance. For more information, see http://www.tsa.gov/press/happenings/updated_pgds.shtm or contact the TSA Contact Center, (866) 289-9673.

Pipeline and Hazardous Materials Safety Administration: Risk Management Self-Evaluation Framework (RMSEF) See <http://www.phmsa.dot.gov/hazmat/risk/rmsef>.

Contact the TSA HMC offices with any questions at: highwaysecurity@dhs.gov.

Recommended General Aviation Security Action Items for General Aviation Aircraft Operators” and “Recommended Security Action Items for Fixed Base Operators”. These voluntary action items are measures that aircraft operators and fixed base operators should consider when they develop, implement or revise security plans or other efforts to enhance security. For more information, see http://www.tsa.gov/what_we_do/tsnm/general_aviation/security.shtm.

Safeguarding America’s Transportation System Security Guides are available for Highway Passenger Security Motorcoach Personnel, Private and Contract Carrier Company Employees, Owner-Operator Independent Drivers Association (OOIDA) Members, School Transportation Industry Personnel, Tank Truck Carrier Employees, and Truck Rental Company Employees. You can access the guides by clicking on “Documents and Reports” on the main Highway and Motor Carrier page on the TSA web site at: www.tsa.gov/highway. Any questions can be sent to highwaysecurity@dhs.gov.

Transportation Security Administration Counterterrorism Guides are highway security counterterrorism guides for Highway Transportation security partners in the Trucking, Highway Infrastructure, Motorcoach and School Transportation industries. These guides are small flip-charts containing the following topics: Pre-Incident Indicators; Targets; Threats to Highway; Insider Threat; Cloned Vehicle; Hijacking Prevention; Suspicious Packages; Information on Explosive Devices; Prevention/Mitigation; Security Planning; Security Inspection Checklist; Security Exercises; Chemical/Biological/Nuclear/Radiological Incidents; and Federal, State and Local POCs. You can contact TSA HMC to order a copy, pending available inventory at highwaysecurity@dhs.gov.

Transportation Sector Network Management Highway and Motor Carrier Division Annual Report TSA Highway and Motor Carrier Division publishes an Annual Report and posts the document on the following web site:

http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm.

Transit Agency Security and Emergency Management Protective Measures is a compilation of recommended protective measures for threat levels under the Homeland Security Advisory System Jointly developed by TSA and FTA. The current recommended protective measures reflect the advantages of improved threat and intelligence information, security assessments conducted by FTA and TSA, operational experience since the 9/11 attacks that prompted the original version, and collective subject matter expertise and experience of Federal partners and the transit community. This product has been developed as a technical resource to transit agency executive management and senior staff assigned to develop security and emergency response plans and to implement protective measures for response to the HSAS threat conditions and emergencies that might affect a transit agency. See http://www.tsa.gov/assets/pdf/mass_transit_protective_measures.pdf, contact: MassTransitSecurity@dhs.gov.

User’s Guide on Security Seals for Domestic Cargo provides information on the different types of security seals available for use in securing and controlling containers, doors, and equipment. While this guide is not intended as a precise procedure for developing a comprehensive seal control program, instead, the objective is to provide information and procedures that will support the development of a seal control program that will meet site-specific requirements. The ‘User’s Guide on Security Seals’ document can be obtained by accessing this link: https://portal.navfac.navy.mil/portal/page/portal/NAVFAC/NAVFAC_WW_PP/NAVFAC_NFESC_PP/LOCKS/PDF_FILES/sealguid.pdf.

TSA Alerts and newsletters

Highway ISAC The TSA Trucking Security Program funds the First Observer™ domain awareness program as well as a Call-Center and Information Sharing and Analysis Center (ISAC). The Highway ISAC creates products and bulletins and e-mails them to a distribution list from TSA Highway

and Motor Carrier and the First Observer program. Contact First Observer at www.firstobserver.com.

TSA Alert System is an emergency notification alert system for Highway and Motor Carrier security partners. The system is capable of sending out a message via phone, e-mail or SMS (text) based on the person’s priority contact preference. Contact TSA by E-mail to become a TSA Alert subscriber at highwaysecurity@dhs.gov.

TSA Technical assistance and help

Comprehensive Security Assessments and Action Items encompass activities and measures that are critical to an effective security program. The 17 Action Items cover a range of areas including security program management and accountability, security and emergency response training, drills and exercises, public awareness, protective measures for the Homeland Security Advisory System threat levels, physical security, personnel security, and information sharing and security. TSA’s Transportation Security Inspectors-Surface conduct security assessments under the Baseline Assessment for Security Enhancement (BASE) program that evaluate the posture of mass transit and passenger rail agencies in the Action Items in a comprehensive and systematic approach to elevate baseline security posture and enhance security program management and implementation. The results of the security assessments inform development of risk mitigation programs and resource allocations, most notably security grants. See http://www.tsa.gov/assets/pdf/mass_transit_action_items.pdf. For additional information, contact MassTransitSecurity@dhs.gov.

General Aviation Secure Hotline serves as a centralized reporting system for general aviation pilots, airport operators, and maintenance technicians wishing to report suspicious activity at their airfield. Hotline phone number: 1-866-GA-SECUR (1-866- 427-3287).

Highway and Motor Carrier First Observer™ Call-Center "First Observer" trained specialists serve as the first line of communication for all matters related to this anti-terrorism and security awareness program. Well trained responders will provide nationwide first responder and

law enforcement contact numbers and electronic linkage to registered participants. Reported caller information is entered into a fully secured reporting system that allows for an electronic transfer to the Information Sharing and Analysis Center (ISAC) for further investigation by industry analysts. The call center may also be utilized during an incident of national significance. Call the center 24 x 7 (888) 217-5902. For more information see www.firstobserver.com.

Traveler Redress Inquiry Program (DHS TRIP) provides a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at airports, train stations, or crossing U.S. borders. To initiate an inquiry, please log onto DHS TRIP's interactive Web site www.dhs.gov/trip. For more information, contact the TSA Contact Center, (866) 289-9673.

TSA Programs and Services

Air Cargo Watch program The likelihood that office staff or managers will uncover the next terrorist is not high. The likelihood that an employee or contractor will see something that is out of the normal routine, the odd out of place person, activity or thing, is high. If it makes that employee feel uncomfortable or take notice, it should be reported to their supervisor immediately. The chance that a driver, dockworker, or cargo agent will be the person that uncovers the next attack is very likely. The Air Cargo Watch program involves all aspects of the supply chain reporting suspicious activity. TSA is collaborating with industry partners to increase security domain awareness so that individuals are empowered to detect, deter, and report potential or actual security threats. The resulting Air Cargo Watch campaign is consistent with U.S. Department of Homeland Security and TSA efforts. Air Cargo Watch has developed materials including a presentation, posters and a two-page guide, to encourage increased attention to potential security threats among several audiences. TSA encourages the display of posters and guides in public view to better attain its goal of maximizing security awareness along the entire air cargo supply chain. See http://www.tsa.gov/what_we_do/layers/aircargo/watch.shtm.

Cargo Certified Cargo Screening Program Effective August 1, 2010, 100 percent of cargo flown on passenger aircraft originating in the United States must be screened, per an act passed by Congress and signed into law by former President Bush following the 9/11 Commission Act of 2007. In response, TSA created the Certified Cargo Screening Program (CCSP) to provide a mechanism by which industry may achieve 100% screening without impeding the flow of commerce. Informational materials include: One-page overview of CCSP, CCSF and Chain of Custody Standards, Tri-Fold Brochure, Supplemental CCSP program material with at a glance program overview of the program Quick Hits overview with impact of 100% screening and supplemental CCSP materials. For more information visit: www.tsa.gov/ccsp, contact CCSP, ccsp@dhs.gov or the TSA Contact Center, (866) 289-9673.

Airspace Waivers The Office of Airspace Waivers manages the process and assists with the review of general aviation aircraft operators who request to enter areas of restricted airspace. For each waiver applicant, to support the vetting requirements, last name, first name, social security number, passport number, date of birth and place of birth, are collected. For applications for aircraft operating into, out of, within or overflying the United States, the waiver review process includes an evaluation of the aircraft, crew, passengers, and purpose of flight. The office then adjudicates the application and provides a recommendation of approval or denial to the FAA System Operations Security. For more information, see http://www.tsa.gov/what_we_do/tsnm/general_aviation/programs_aw.shtm#overview or contact (571) 227-2071.

DCA Access Standard Security Program (DASSP) TSA's Interim Final Rule, which was developed in coordination with other Department of Homeland Security agencies and the Department of Defense, takes into consideration the special security needs of Washington Reagan National Airport (DCA). Under TSA's security plan, a maximum of 48 flights in and out of DCA will be allowed each day. All aircraft will be required to meet the security measures set forth in the DCA Access Standard Security Program (DASSP). See http://www.tsa.gov/what_we_do/tsnm/general_aviation/programs_sp.shtm#dassp or contact (571) 227-2071.

General Aviation Maryland Three Program allows properly vetted private pilots to fly to, from, or between the three general aviation airports closest to the National Capital Region. These airports are collectively known as the "Maryland Three" airports, and include College Park Airport (CGS), Potomac Airfield (VKX) and Hyde Executive Field (W32.) These airports are all within the Washington, DC Air Defense Identification Zone (ADIZ) and the Washington, D.C. Flight Restricted Zone (FRZ). See http://www.tsa.gov/what_we_do/tsnm/general_aviation/programs_sp.shtm#maryland or contact (571) 227-2071

Homeland Security Information Network (HSIN) – Freight Rail Portal has been designed to provide consistent, real time information sharing capabilities in an integrated, secure, web-based forum to coordinate and collaborate directly with our security partners. Membership to the Freight Rail portal is provided once vetted by portal administrators. If you have questions, or for access please contact the HSIN Helpdesk at (866) 430-0162 or send an e-mail to HSIN.helpdesk@dhs.gov or Linda.Lentini@dhs.gov.

Homeland Security Information Network (HSIN) - Highway and Motor Carrier Portal is part of the Critical Sector part of the HSIN system (HSIN-CS). Membership to the HMC portal is provided once vetted by portal administrators. If you have questions, please contact the HSIN Helpdesk at (866) 430-0162 or send an e-mail to HSIN.helpdesk@dhs.gov.

Homeland Security Information Network – Public Transit Portal (HSIN-PT) Intelligence sharing between mass transit and passenger rail agencies and their Federal, State and local partners is further facilitated through TSA's Mass Transit Security Information Network's inter-agency communication and information sharing protocols. The HSIN-PT has been integrated into this network to provide one stop security information sources and outlets for security advisories, alerts and notices. TSA periodically produces and disseminates Mass Transit Security Awareness Messages that address developments related to terrorist activity and tactics against mass transit and passenger rail at the "for official use only" level. Additionally, TSA is actively involved in regional security forums and supports these collaborative efforts by sharing

intelligence products and related security information. Finally, a preplanned alert notification system enables access to mass transit and passenger rail law enforcement and security officials nationally with timely notification of threats or developing security concerns. Membership to the Public Transit portal is provided once vetted by portal administrators, contact MassTransitSecurity@dhs.gov.

Joint DHS/FBI Classified Threat and Analysis

Presentations A joint DHS Office of Intelligence and Analysis, TSA Office of Intelligence, and Federal Bureau of Investigation effort provides classified intelligence and analysis presentations to mass transit and passenger rail security directors and law enforcement chiefs in more than 20 metropolitan areas simultaneously through the Joint Terrorism Task Force (JTTF) network’s secure video teleconferencing system. These briefings advance two key strategic objectives - providing intelligence and security information directly to mass transit and passenger rail law enforcement chiefs and security directors and enhancing regional collaboration by bringing these officials together with their Federal partners to discuss the implications for their areas and coordinate to implement effective security solutions. The briefings occur on approximately quarterly to semi-annual basis, with additional sessions as threat developments may warrant. For more information, contact MassTransitSecurity@dhs.gov.

Mass Transit Security and Safety Roundtables TSA, The Federal Transit Administration (FTA), and the Federal Emergency Management Administration (FEMA) co-sponsor the semi-annual Transit Security and Safety Roundtables, bringing together law enforcement chiefs, security directors, and safety directors from the nation’s 50 largest mass transit and passenger rail agencies and Amtrak with Federal security partners to discuss specific terrorism prevention and response challenges and to work collaboratively in developing effective risk mitigation and security enhancement solutions. The Roundtables also provide a forum for agency safety and security officials to share effective practices and develop relationships to improve coordination and collaboration. For additional information, contact MassTransitSecurity@dhs.gov.

Mass Transit Security Technology Testing In coordination with TSA’s Office of Security Technology and DHS’s Office

of Science and Technology, the Mass Transit Division pursues development of multiple technologies to advance capabilities to detect and deter terrorist activity and prevent attacks. TSA partners with mass transit and passenger rail agencies to conduct pilot testing of various security technologies. These activities evaluate these capabilities in the varied operational environments that prevail in rail and bus operations across the country. Contact: MassTransitSecurity@dhs.gov.

Paperless Boarding Pass Pilot enables passengers to download their boarding pass on their cell phones or personal digital assistants (PDAs). This innovative approach streamlines the customer experience while heightening the ability to detect fraudulent boarding passes. For more information, see http://www.tsa.gov/approach/tech/paperless_boarding_pass_expansion.shtm or contact the TSA Contact Center, (866) 289-9673.

Screening Partnership Program (SPP) also known as Opt-Out, is a unique approach to providing security screening services for air passengers and baggage. Under the program, an airport operator may apply to have security screening conducted by personnel from a qualified private contractor working under Federal oversight. For more information, see http://www.tsa.gov/what_we_do/optout/index.shtm or contact the TSA Contact Center, (866) 289-9673.

Secure Fixed Base Operator is a public-private sector partnership program that allows Fixed Base Operators (FBOs) to check passenger and crew identification against manifests or Electronic Advance Passenger Information System (eAPIS) filings for positive identification of passengers and crew onboard general aviation aircraft. See http://www.tsa.gov/assets/pdf/sfbop_general_faq.pdf (pdf - 35KB). For additional information, contact tsnmfbo@dhs.gov.

Secure Flight is a behind the scenes program that enhances the security of domestic and international commercial air travel through the use of improved watch list matching. By collecting additional passenger data, it will improve the travel experience for all airline passengers, including those who have been misidentified in the past. Resources available for aviation stakeholders

include a communications toolkit, a brochure, privacy information, signage informational video. For more information, visit http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm, or contact the TSA Contact Center, (866) 289-9673.

Transportation Security Grant Programs provides security grants to transit systems, intercity bus companies, freight railroad carriers, ferries, and the trucking industry to help protect the public and the nation’s critical transportation infrastructure. The grants support high-impact security projects that have a high efficacy in reducing the most risk to our nation’s transportation systems. See www.tsa.gov/grants. For more information, contact TSAGrants@tsa.dhs.gov.

Transportation Worker Identification Credential (TWIC) is a security program designed to ensure that individuals who pose a security threat do not gain unescorted access to secure areas of the nation's maritime transportation system. The credential is a biometric card that ensures only vetted workers can enter without an escort to secure transportation areas. The TWIC Program is jointly administered by TSA and the U.S. Coast Guard. More information can be found at http://www.tsa.gov/what_we_do/layers/twic/index.shtm, or by contacting the TWIC Hotline, (866) 347-8942.

3-1-1 Liquid Restriction is a travel tip for passengers to remind them to pack liquids/gels in 3.4 oz bottles or less, to consolidate bottles into a one quart baggie and place them in a bin, outside of their carry-on to send through the X-ray for screening. See <http://www.tsa.gov/311/index.shtm> or contact the TSA Contact Center, (866) 289-9673.

Appendix A – Key Contacts

Component	Contact	E-mail	Phone
CBP	ACE Help Desk		(800) 927-8729
CBP	Air & Marine Operations Center (AMOC)		(951) 656-8000
CBP	Carrier Liaison Program	CLP@dhs.gov	(202) 344-3440.
CBP	CBP INFO Center		(877) CBP-5511
CBP	Client Representative Office		(571) 468-5000
CBP	Electronic System for Travel Authorization (ESTA)		(202) 344-3710
CBP	Global Entry	cbp.goes.support@dhs.gov	(866) 530-4172
CBP	Industry Partnership Program	industry.partnership@dhs.gov	(202) 344-1180
CBP	Intellectual Property Rights Help Desk	ipr.helpdesk@dhs.gov	(562) 980-3119 ext. 252
CBP	Intellectual Property Rights Policy and Programs	iprpolicyprograms@dhs.gov	
CBP	National Gang Intelligence Center		(703) 414-8600
CBP	Private Aircraft Travel Entry Programs	Private.Aircraft.Support@dhs.gov	
CBP	Secure Freight Initiative	securefreightinitiative@dhs.gov	
CRCL	Training	crcltraining@dhs.gov	(202) 357-8258
CRCL	Disability Preparedness	Disability.preparedness@dhs.gov	(202) 357-8483
CS&C	Control Systems Security Program (CSSP)	CSSP@dhs.gov	
CS&C	Cybersecurity Evaluation Tool	CSET@dhs.gov	
CS&C	Information Technology Sector	ncsd_cipcs@hq.dhs.gov	
CS&C	Office of Emergency Communications	oec@hq.dhs.gov	
CS&C	Software Assurance Program	software.assurance@dhs.gov	
CS&C	U.S. Computer Emergency Readiness Team (US-CERT)	info@us-cert.gov	(888) 282-0870
CS&C	US-CERT Secure Operations Center	soc@us-cert.gov	(888) 282-0870
DHS	Center for Faith-based and Community Initiatives	Infobfci@dhs.gov	
DHS	Homeland Security Information Network (HSIN)	hsin.helpdesk@dhs.gov	(866) 430-0162
DHS	Lessons Learned and information Sharing (LLIS)	feedback@llis.dhs.gov	(866) 276-7001
DHS	National Information Exchange Model (NIEM) Program	NIEMPMO@NIEM.gov	
DHS	Office of Small and Disadvantaged Business Utilization		(202) 447-5555

Appendix A – Key Contacts

DHS	Private Sector Office	Private.sector@dhs.gov	(202) 282-8484
FEMA	Center for Domestic Preparedness	Studentservices@cdpemail.dhs.gov	(866) 213-9553
FEMA	Centralized Scheduling and Information Desk	askcsid@dhs.gov	(800) 368-6498
FEMA	Citizen Corps	citizencorps@dhs.gov	
FEMA	Community Emergency Response Teams	cert@dhs.gov	
FEMA	Disaster Assistance		(800) 745-0243
FEMA	Emergency Lodging Assistance Program	femahousing@corplodging.com	(866) 545-9865
FEMA	FEMA Emergency Management Institute		(301) 447-1200
FEMA	FEMA Learning Resource Center	netclrc@dhs.gov	(800) 638-1821
FEMA	FEMA Private Sector Division	FEMA-Private-Sector-Web@dhs.gov	
FEMA	First Responder Training	askCSID@dhs.gov	(800) 368-6498
FEMA	Industry Liaison Support Center (contracting)		(202) 646-1895
FEMA	Maps Assistance Center	FEMAMapSpecialist@riskmapcde.com	(877) 336-2627
FEMA	National Incident Management System	FEMA-NIMS@dhs.gov	(202) 646-3850
FEMA	Regulations	FEMA-RULES@dhs.gov	
FEMA	Small Business Program	FEMA-SB@dhs.gov	
FEMA	Technical Assistance Program	FEMA-TARequest@fema.gov	(800) 368-6498
FEMA	U.S. Fire Administration		(301) 447-1000
FEMA	U.S. Fire Administration Publications	usfa-publications@dhs.gov	(800) 561-3356
FLETC	CRADA Program Office	FLETC-CRADAProgramOffice@dhs.gov	(912) 267-2100
I&A	DHS Open Source Enterprise	OSINTBranchMailbox@hq.dhs.gov	
I&A	Office of Intelligence and Analysis Private Sector Partnership Program	I&APrivateSectorCoordinator@hq.dhs.gov	(202) 447-3517 or (202) 870-6087
ICE	Victim Assistance Program		(866) 872-4973
ICE	Human Rights Violators and War Crimes Center	HRV.ICE@DHS.GOV	
ICE	ICE 24/7 Hotline		(866) DHS-2-ICE
ICE	ICE Mutual Agreement between Government and Employers Program (IMAGE)	IMAGE@dhs.gov	(202) 732-3064.
ICE	Intellectual Property Rights Center		(866) IPR-2060 or (866) 477-2060
ICE	National Incident Response Unit (NIRU)	niru@dhs.gov	
ICE	Privacy Office	ICEPrivacy@dhs.gov	(202) 732-3300
ICE	Public Affairs	PublicAffairs.IceOfficeOf@dhs.gov	(202) 732-4242
ICE	Student and Exchange Visitor Program (SEVP) Response Center	SEVIS.Source@DHS.gov	(703) 603-3400
IP	Chemical Facility Anti-Terrorism Standards (CFATS) Help Desk	csat@dhs.gov	(866) 323-2957

Appendix A – Key Contacts

IP	Chemical Facility Anti-Terrorism Standards Compliance Assistance Visit Requests	cscd.ieb@hq.dhs.gov	
IP	Chemical Sector Specific Agency	ChemicalSector@dhs.gov	(877) CHEMSEC
IP	CIKR Asset Protection Technical Assistance Program (CAPTAP)	ACAMS-info@hq.dhs.gov	(703) 235-3939
IP	Commercial Facilities Sector-Specific Agency	CFSteam@hq.dhs.gov	
IP	Critical Manufacturing Sector-Specific Agency	cm-ssa@dhs.gov	
IP	Dams Sector-Specific Agency	dams@dhs.gov	
IP	Emergency Services Sector-Specific Agency	ESSTeam@hq.dhs.gov	
IP	Infrastructure Data Taxonomy (IDT)	IICD@dhs.gov	
IP	Integrated Common Analytical Viewer (iCAV)	iCAV.info@hq.dhs.gov	(703) 235-4949
IP	IP Education and Learning Series	IP_Education@hq.dhs.gov	
IP	National Infrastructure Coordination Center (NICC)		(202) 282-9201
IP	National Infrastructure Protection Plan (NIPP)	NIPP@dhs.gov	(703) 603-5069
IP	Nuclear Sector-Specific Agency	nuclearSSA@hq.dhs.gov	
IP	Office for Bombing Prevention	OBP@dhs.gov	(703) 235-5723
IP	Protected Critical Infrastructure Information (PCII) Program	pcii-info@dhs.gov	(202) 360-3023
IP	Protective Security Advisor (PSA) Field Operations Staff	PSAFieldOperationsStaff@hq.dhs.gov	(703) 235-5724
IP	Sector Specific Agency Executive Management Office	SSAexecsec@dhs.gov	
IP	Vulnerability Assessments Branch	IPassessments@dhs.gov	
S&T	Commercialization Office	SandT_Commercialization@hq.dhs.gov	(202) 254-6749
S&T	Cyber Security Research and Development Center	csrdc@dhs.gov	
S&T	Office of University Programs	universityprograms@dhs.gov	(202) 254-6934
S&T	Project 25 Compliance Assessment Program (P25 CAP)	P25CAP@dhs.gov	
S&T	SAFECOM Program	SAFECOM@dhs.gov	
S&T	SAFETY Act	SAFETYActHelpDesk@dhs.gov	(866) 788-9318
TSA	Cargo Certified Cargo Screening Program	ccsp@dhs.gov	
TSA	Freight and Rail	freightrailsecurity@dhs.gov	
TSA	General Aviation Secure Hotline		1-866-GA-SECUR (1-866-427-3287)
TSA	Highway and Motor Carrier Division	highwaysecurity@dhs.gov	
TSA	Intermodal Security Training and Exercise Program (I-STEP)	i-step@dhs.gov	(571) 227-5150
TSA	Mass Transit	MassTransitSecurity@dhs.gov	
TSA	Office of Airspace Waivers		(571) 227-2071
TSA	Pipeline Security Division	PipelineSecurity@dhs.gov	

Appendix A – Key Contacts

TSA	Port & Intermodal Security Division	Maritime@dhs.gov	(571) 227-3556
TSA	Transportation Security Grant Programs	TSAGrants@tsa.dhs.gov	
TSA	TSA Contact Center		1-866-289-9673
CIS Ombudsman	CIS Ombudsman	cisombudsman@dhs.gov	
USCIS	E-Verify	E-Verify@dhs.gov	(888) 464-4218
USCIS	Office of Public Engagement	Public.Engagement@dhs.gov	

Appendix B – Index

A

Active Shooter - How To Respond, 25
Active Threat Recognition for the Shopping Center/Retail Security Officer, 23
Air Cargo Watch program, 41
AIRBUST program, 10
Airport Watch/AOPA Training, 37
Airspace Waivers, 41
Alert, 40
Alerts
 Chemical Sector Monthly Suspicious Activity Calls, 29
 Citizen Corps Email Alerts, 18
 Critical Infrastructure Information Notice, 15
 Current Cybersecurity Activity, 15
 Daily Open Source Infrastructure Report, 26
 DHS Open Source Enterprise – Daily Intelligence Reports, 6
 FEMA Private Sector E-alert, 18
 Highway ISAC, 40
 National Cyber Alert System, 15
 Private Sector Community Preparedness Updates, 5
 Technical Resource for Incident Prevention (TRIPwire), 32
 TSA Alert System, 40
 U.S. Border Patrol Blotter, Newsletter, and Alerts, 10
 U.S. Computer Emergency Readiness Team (US-CERT) Monthly Activity Summary, 15
Alien Flight/Flight School Training, 37
America’s Waterways Watch, 9
Are You Ready? An In-depth Guide to Citizen Preparedness, 17
Assistance
 Automated Commercial Environment (ACE) National Help Desk, 10
 Buffer Zone Protection Program (BZPP), 28
 Cargo Systems Messaging Service (CSMS), 10
 CBP Client Representatives, 10
 CBP INFO Center Self Service Q&A Database, 11
 Chemical Security Assessment Tool (CSAT), 31
 Chemical Security Compliance Assistance Visit (CAV) Requests, 29
 Comprehensive Security Assessments and Action Items, 40
 Computer-Based Assessment Tool (CBAT), 31
 Critical Infrastructure and Key Resource (CIKR) Asset Protection Technical Assistance Program (CAPTAP), 29
 Cyber Resiliency Review (CRR), 15
 Cyber Security Advisors (CSAs), 16
 Cyber Security Evaluation Program (CSEP), 16
 Cyber Security Evaluation Tool (CSET), 14

Cybersecurity Vulnerability Assessments, 16
 DisasterAssistance.gov, 18
 Emergency Lodging Assistance Program, 18
 Entry Process into United States, 11
 FEMA Map Assistance Center, 18
 FEMA Technical Assistance (TA) Program, 20
 General Aviation Secure Hotline, 40
 Highway and Motor Carrier First Observer™ Call-Center, 40
 Importing into the United States, 11
 Industrial Control Systems Technology Assessments, 16
 Intellectual Property Rights (IPR) Help Desk, 12
 National Center for Foreign Animal and Zoonotic Disease Defense (FAZD), 36
 Protective Security Advisor (PSA) Program, 30
 Radiological Voluntary Security Enhancements, 30
 Regional Resiliency Assessment Program (RRAP), 30
 Research and Test Reactors (RTRs) Voluntary Security Enhancement Program, 30
 Risk Self-Assessment Tool for Stadiums and Arenas, 32
 Security Outreach and Awareness Program (SOAP), 30
 Site Assistance Visit (SAV), 30
 The National Intellectual Property Rights Coordination Center, 22
 Traveler Redress Inquiry Program (DHS TRIP), 6, 41
 U. S. Computer Emergency Readiness Team (US-CERT) Operations Center, 15
 U.S. Immigration and Customs Enforcement (ICE) Victim Assistance Program, 22
 Unified Hazard Mitigation Assistance Grant Programs, 20
 Voluntary Chemical Assessment Tool (VCAT), 32
Assistance Commercialization Office, 5, 33
Automated Commercial Environment (ACE), 11
Automated Commercial Environment (ACE) National Help Desk, 10
Automated Commercial System (ACS), 11
Automated Critical Asset Management System, 31
Automated Export System (AES), 11
Automated Manifest System (AMS), 11

B

Bomb Event Management Web Training, 23
Bombing Prevention, 23, 24, 25, 27, 28, 31, 32
 Bombing Prevention Workshop, 23
 Bomb-making Materials Awareness Program (BMAP), 28
 Bomb-Making Materials Awareness Program (BMAP)/Suspicious Behavior Cards, 25
 Technical Resource for Incident Prevention (TRIPwire), 32

TRIPwire Community Gateway (TWCG), 32
Bombing Prevention Workshop, 23
Bomb-Making Materials Awareness Program (BMAP), 28
Bomb-Making Materials Awareness Program (BMAP)/Suspicious Behavior Cards, 25
Buffer Zone Protection Program (BZPP), 28

C

Cargo
 Automated Commercial Environment (ACE), 11
 Automated Manifest System (AMS), 11
 Secure Freight Initiative (SFI) and Importer Security Filing and additional carrier requirements (10+2), 13
Cargo Certified Cargo Screening Program, 41
Cargo Systems Messaging Service (CSMS), 10
Carrier Liaison Program (CLP), 11
CBP Client Representatives, 10
CBP Directives Pertaining to Intellectual Property Rights, 10
CBP INFO Center Self Service Q&A Database, 11
CBP Laboratories and Scientific Services, 12
CBP Trade Outreach, 13
Center for Domestic Preparedness (CDP), 17
Cesium Chloride In-Device Delay (Irradiator Hardening), 29
Chemical Facility Anti-Terrorism Standards (CATS) Chemical Facility Security Tip Line, 29
Chemical Facility Anti-Terrorism Standards (CFATS), 25
Chemical Facility Anti-Terrorism Standards (CFATS) Presentation, 25
Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS), 25
Chemical Sector Explosive Threat Awareness Training Program, 23
Chemical Sector Monthly Suspicious Activity Calls, 29
Chemical Security Assessment Tool (CSAT), 31
Chemical Security Compliance Assistance Visit (CAV) Requests, 29
Chemical Security Summit, 29
Chemical-Terrorism Vulnerability Information (CVI), 25
CIS Ombudsman Annual Reports to Congress, 8
CIS Ombudsman Updates, 8
CIS Ombudsman’s Community Call-In Teleconference Series, 8
Citizen Corps Email Alerts, 18
Civics and Citizenship Toolkit - A Collection of Educational Resources for Immigrants, 7
Commercial Facilities Sector Pandemic Planning Documents, 26
Commercial Facilities Training Resources Guide pamphlet, 23
Commercial Mobile Alert Service (CMAS), 33

Commercialization Office, 5, 33
Community Emergency Response Team (CERT), 17
Community Preparedness – Citizen Corps, 18
Comprehensive Security Assessments and Action Items, 40
Computer-Based Assessment Tool (CBAT), 31
Contact CBP
 1-800 BE ALERT, 10
Cooperative Research and Development Agreements (CRADAs), 5
Counterterrorism, 40
Counterterrorism Protective Measures Course, 23
Critical Infrastructure and Key Resource (CIKR) Asset Protection Technical Assistance Program (CAPTAP), 29
Critical Infrastructure and Key Resources (CIKR) Learning Series, 23
Critical Infrastructure and Key Resources (CIKR) Resource Center, 31
Critical Infrastructure and Key Resources (CIKR) Sector Snapshots, Fact Sheets and Brochures, 28
Critical Infrastructure and Key Resources (CIKR) Sector-Specific Plans, 28
Critical Infrastructure and Key Resources (CIKR) Training Module, 23
Critical Infrastructure Information Notice, 15
Customs-Trade Partnership Against Terrorism (C-TPAT), 11
Cyber Security Research and Development Center, 33
Cybersecurity
 Control Systems Security Program (CSSP), 16
 Control Systems Security Program (CSSP) Instructor-Lead Cybersecurity Training, 14
 Critical Infrastructure Information Notices, 15
 Critical Infrastructure Protection – Cyber Security (CIP-CS), 16
 Current Cybersecurity Activity, 15
 Cyber Education and Workforce Development Program (CEWD), 14
 Cyber Resiliency Review (CRR), 15
 Cyber Security Advisors, 16
 Cyber Security Evaluation Program (CSEP), 16
 Cyber Security Evaluation Tool (CSET), 14
 Cyber Security Research and Development Center, 33
 Cybersecurity Information Products and Recommended Practices, 14
 DHS/Commercial Facilities Training Resources Guide pamphlet, 23
 Industrial Control System Cybersecurity Standards and References, 14
 Industrial Control Systems Technology Assessments, 16
 Information Technology Sector Risk Assessment, 14
 Information Technology Sector Specific Plan (IT SSP), 14
 National Cyber Alert System, 15
 Public Trends and Analysis Report, 14

Software Assurance Program, 16
 US-CERT Monthly Activity Summary, 15
 US-CERT Operations Center, 15
 US-CERT Security Publications, 15
 Vulnerability Assessments, 16
 Vulnerability Notes Database, 15

D

Daily Open Source Infrastructure Report, 26
Dams Sector Consequence-Based Top Screen Fact Sheet, 26
Dams Sector Consequence-Based Top Screen Methodology, 31
Dams Sector Councils Fact Sheet, 26
Dams Sector Crisis Management Handbook, 26
Dams Sector Exercise Series (DSES), 29
Dams Sector Exercises Series Fact Sheet - 2009, 26
Dams Sector Overview Brochure, 26
Dams Sector Protective Measures Handbook, 26
Dams Sector Research & Development Roadmap: Development of Validated Damage and Vulnerability Assessment Capabilities for Aircraft Impact Scenarios, 26
Dams Sector Resources (For Official Use Only): The Dams Sector Security Awareness Handbook, 26
Dams Sector Security Awareness Guide, 26
Dams Sector Security Awareness Guide for Levees, 26
Dams Sector Security Awareness Handbook, 26
Dams Sector Standard Operating Procedures for Information Sharing, 26
Dams Sector Suspicious Activity Reporting Fact Sheet, 26
Dams Sector Suspicious Activity Reporting Tool, 31
Dams Sector Waterside Barriers Guide, 26
Data and Visual Analytics, 33
DCA Access Standard Security Program (DASSP), 41
Defense Technology Experimental Research (DETER), 33
DHS Center for Faith-Based and Community Initiatives, 5
DHS Center of Excellence
 Awareness & Location of Explosives-Related Threats (ALERT), 35
 Center for Maritime, Island, & Remote/Extreme Environment Security, 36
 National Center for Command, Control, and Interoperability (C2I), 36
 National Center for Food Protection and Defense (NCFPD), 35
 National Center for Foreign Animal and Zoonotic Disease Defense (FAZD), 36
 National Center for Risk and Economic Analysis of Terrorism Events (CREATE), 35
 National Consortium for the Study of Terrorism and Responses to Terrorism (START), 36
 National Transportation Security Center of Excellence (NTSCOE), 36

Preparedness and Catastrophic Event Response (PACER), 35
DHS Office of Infrastructure Protection (IP), 5
DHS Open Source Enterprise – Daily Intelligence Reports, 6
DHS Private Sector Office, 5
Disabilitypreparedness.gov, 5
DisasterAssistance.gov, 18
Domain Name System Security Extensions (DNSSEC) Deployment Coordinating Initiative, 33
Donations and Volunteers Information, 18

E

eAllegations, 11
Education, Outreach, and Awareness Snapshot, 26
Electronic Crimes Task Force (ECTF) Program, 5
Electronic System for Travel Authorization (ESTA), 11
Emergency Communications Guidance Documents and Methodologies, 14
Emergency Data Exchange Language (EDXL), 34
Emergency Food and Shelter National Board Program, 18
Emergency Lodging Assistance Program, 18
Emergency Services Personal Readiness Guide for Responders and Their Families, 26
Emergency Services Sector (ESS)Video, 26
Emergency Services Sector Training Catalog, 24
Enhanced Critical Infrastructure Protection (ECIP), 29
Entry Level Test Study Guides for CBP Job Applicants, 10
Entry Process into United States, 11
Evacuation Planning Guide for Stadiums, 26
E-Verify, 7
E-Verify and Unfair Labor Practices, 5
Exercises
 Dams Sector Exercise Series (DSES), 29
 Sector-Specific Agency Executive Management Office/Transportation Security Administration (TSA) Joint Exercise Programs, 30
 Security Seminar Exercise Series with State Chemical Industry Councils, 30
Expanding ESL, Civics, and Citizenship Education in Your Community: A Start-Up Guide, 7

F

Federal Bureau of Investigation (FBI) Terrorism Vulnerability Self-Assessment, 39
Federal Motor Carrier Safety Administration: Guide to Developing an Effective Security Plan for the Highway Transportation of Hazardous Materials, 39
FEMA Emergency Management Institute Independent Study Program, 17

FEMA Emergency Management Institute Programs, 17
 FEMA Industry Liaison Program, 18
 FEMA Learning Resource Center, 17
 FEMA Library, 18
 FEMA Map Assistance Center, 18
 FEMA Private Sector E-alert, 18
 FEMA Regulatory Materials, 18
 FEMA Small Business Program, 19
 First Observer™ Training, 37
 Forced Labor Resources, 21
 Freight Rail Security Grant Program, 19

G

General Aviation, 39, 40, 41
 General Aviation Maryland Three Program, 41
 General Aviation Secure Hotline, 40
 General Aviation Security Guidelines, 39
 General Information on Sector-Specific Agency Executive Management Office (SSA EMO) Critical Infrastructure and Key Resources (CIKR) Sectors and Programs, 31
 Global Entry, 12
 Global Supply Chain Risk Management (GSCRM) Program, 16
 Grants
 Freight Rail Security Grant Program, 19
 Intercity Bus Security Grant Program, 19
 Intercity Passenger Rail Grant Program, 19
 Nonprofit Security Grant Program, 19
 Port Security Grant Program, 19
 Transit Security Grant Program, 20
 Transportation Security Grant Programs, 42
 Unified Hazard Mitigation Assistance Grant Programs, 20
 Guide to Critical Infrastructure and Key Resources (CIKR) Protection at the State, Regional, Local, Tribal, & Territorial Level, 26
 Guide to Naturalization, 7

H

Hazmat Motor Carrier Security Action Item Training (SAIT) Program, 37
 Hazmat Motor Carrier Security Self-Assessment Training Program, 37
 HAZMAT TRUCKING GUIDANCE: Highway Security-Sensitive Materials (HSSM) Security Action Items (SAIs), 39
 Highway and Motor Carrier Awareness Posters, 39
 Highway and Motor Carrier First Observer™ Call-Center, 40
 Highway ISAC, 40
 Homeland Security Information Network, 41

Homeland Security Information Network – Public Transit Portal (HSIN-PT), 41
 Homeland Security Information Network (HSIN), 5
 Homeland Security Information Network (HSIN) – Freight Rail Portal, 41
 Homeland Security Information Network (HSIN) - Highway and Motor Carrier Portal, 41
 Homeland Security Information Network-Critical Sectors (HSIN-CS), 31
 HOMEPORT, 9
 Hotel and Lodging Advisory Poster, 27
 Human Rights Violators and War Crimes Center, 21
 Human Trafficking
 Awareness Resources, 21
 Hidden in Plain Sight, 21
 Indicators Pamphlet, 21
 Trafficking in Persons (TIP) Card, 21

I

ICE LINK Portal, 21
 IED Recognition and Detection for Railroad Industry Employees Training (CD), 37
 If You Have the Right to Work, Don't Let Anyone Take it Away Poster, 7
 Importer Self Assessment – Product Safety Pilot (ISA-PS), 12
 Importer Self-Assessment Program (ISA), 12
 Importing into the United States, 11
 Improvised Explosive Device (IED) Awareness / Bomb Threat Management Workshop, 24
 Improvised Explosive Device (IED) Awareness Web Training, 24
 Improvised Explosive Device (IED) Search Procedures Workshop, 24
 Independent Study Course IS 870: Dams Sector: Crisis Management Overview, 24
 Independent Study Course IS-821 Critical Infrastructure and Key Resources (CIKR) Support Annex, 24
 Independent Study Course IS-860.a National Infrastructure Protection Plan (NIPP), 24
 Industrial Control Systems Technology Assessments, 16
 Information Sharing
 Comprehensive Security Assessments and Action Items, 40
 DHS Open Source Enterprise Daily Intelligence Reports, 6
 Highway ISAC, 40
 Homeland Security Information Network – Public Transit Portal (HSIN-PT), 41
 Homeland Security Information Network (HSIN), 5
 Homeland Security Information Network (HSIN) – Freight Rail Portal, 41
 Intelligence and Analysis Private Sector Partnership Program, 6
 Lessons Learned and Information Sharing (LLIS.gov), 6

Mass Transit Smart Security Practices, 38
 National Gang Intelligence Center, 12
 National Infrastructure Protection Plan (NIPP) Sector Partnership, 29
 NIPP in Action Stories, 27
 NIPP Information Sharing Snapshot, 27
 Protected Critical Infrastructure Information (PCII) Program, 30
 Soft Target Awareness Course, 24
 USCG HOMEPORT, 9
 Informed Compliance Publications, 10
 Infrastructure Data Taxonomy (IDT), 27
 Infrastructure Protection Report Series (IPRS), 27
 Integrated Common Analytical Viewer (iCAV), 32
 Integrated Common Analytical Viewer (iCAV) Web-based Training, 24
 Intellectual Property Rights (IPR)
 CBP Directives Pertaining to Intellectual Property Rights, 10
 Continuous Sample Bond, 12
 e-Recordation and IPR Search, 12
 Intellectual Property Rights (IPR) Help Desk, 12
 Intellectual Property Rights (IPR) and Restricted Merchandise Branch, 12
 IPR Enforcement
 A Priority Trade Issue, 12
 IPR Seizure Statistics, 10
 U.S. – EU Joint Brochure and Web Toolkit for Trademark, Copyright Owners, 12
 Intelligence and Analysis
 Open Source Enterprise Daily Intelligence Reports, 6
 Private Sector Partnership Program, 6
 Intelligence and Analysis Private Sector Partnership Program, 6
 Intercity Bus Security Grant Program, 19
 Intercity Passenger Rail Grant Program, 19
 Intermodal Security Training and Exercise Program, 37
 International Issues for Critical Infrastructure and Key Resources (CIKR) Protection, 27

J

Joint DHS/FBI Classified Threat and Analysis Presentations, 42

K

Keep the Nation's Railroad Secure (Brochure), 39

L

Laminated Security Awareness Driver Tip Card, 39
 Land Transportation Antiterrorism Training Program (LTATP), 37
 Lessons Learned and Information Sharing (LLIS.gov), 6

Long Range Broad Agency Announcement, 34

M

Mariner Credentialing

USCG National Maritime Center (NMC), 9

Maritime Passenger Security Courses, 37

Mass Transit and Passenger Rail - Additional Guidance on Background Checks, Redress and Immigration Status, 39

Mass Transit and Passenger Rail - Bomb Squad Response to Transportation Systems, 37

Mass Transit and Passenger Rail - Field Operational Risk and Criticality Evaluation (FORCE), 38

Mass Transit Employee Vigilance Campaign, 39

Mass Transit Security and Safety Roundtables, 42

Mass Transit Security Technology Testing, 42

Mass Transit Security Training Program Guidelines, 38

Mass Transit Smart Security Practices, 38

Money Laundering and Operation Cornerstone, 22

MOTORCOACH GUIDANCE: Security and Emergency Preparedness Plan (SEPP), 39

Multi-Jurisdiction Improvised Explosive Device (IED) Security Plan (MJIEDSP), 27

N

National Critical Infrastructure and Key Resources (CIKR) Protection Annual Report Snapshot, 27

National Cyber Alert System, 15

National Dam Safety Program, 19

National Emergency Communications Plan, 15

National Flood Insurance Program, 19

National Gang Intelligence Center, 12

National Incident Management System (NIMS), 19

National Information Exchange Model (NIEM) Program, 6

National Infrastructure Advisory Council (NIAC), 29

National Infrastructure Protection Plan (NIPP) 2009, 27

National Infrastructure Protection Plan (NIPP) 2009 Overview Snapshot, 27

National Infrastructure Protection Plan (NIPP) Brochure, 27

National Infrastructure Protection Plan (NIPP) Information Sharing Snapshot, 27

National Infrastructure Protection Plan (NIPP) Sector Partnership, 29

National Interoperability Field Operations Guide, 15

National Response Framework (NRF), 19

National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management (BIDM), 34

National Vessel Movement Center (NVMC):, 9

NIPP in Action Stories, 27

Nonprofit Security Grant Program, 19

O

Office of Infrastructure Protection, 5

Office of Infrastructure Protection (IP) and National Infrastructure Protection Plan (NIPP) booths, 30

Office of Small and Disadvantaged Business Utilization (OSDBU), 6

Operation Secure Transport (OST), 38

P

Paperless Boarding Pass Pilot, 42

Partnership, 42

Personnel Screening Guide for Owners and Operators, 26

Physical Security Measures for Levees Brochure, 26

Pipeline and Hazardous Materials Safety Administration: Risk Management Self-Evaluation Framework (RMSEF), 39

Pipeline Security Awareness for the Pipeline Industry Employee Training CD and Brochures, 38

Planning for 2009 H1N1 Influenza: A Preparedness Guide for Small Business, 27

Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems, 39

Port Security Grant Program, 19

Portals

Homeland Security Information Network (HSIN), 5

Homeland Security Information Network-Critical Sectors (HSIN-CS), 31

Lessons Learned and Information Sharing (LLIS.gov), 6

National Vulnerability Database (NVD), 16

Technical Resource for Incident Prevention (TRIPwire), 32

TRIPwire Community Gateway (TWCG), 32

Private Aircraft Travel Entry Programs, 13

Private Sector Community Preparedness Updates, 5

Private Sector Counterterrorism Awareness Workshop, 24

Private Sector Office, 5

Procurement

FEMA Industry Liaison Program, 18

FEMA Small Business Program, 19

Office of Small and Disadvantaged Business Utilization (OSDBU), 6

Project 25 Compliance Assessment Program (P25 CAP), 34

Project Shield America, 22

Protected Critical Infrastructure Information (PCI) Program, 30

Protective Measures Guide for U.S. Sports Leagues, 28

Protective Security Advisor (PSA) Program, 30

Public Transportation Emergency Preparedness Workshop - Connecting Communities Program, 38

Q

QuakeSmart, 20

R

Radiological Emergency Preparedness Program (REP), 20

Radiological Voluntary Security Enhancements, 30

Rail Security Rule Overview, 39

Ready Business, 6, 20

Recommendations by the CIS Ombudsman (Previous), 8

Recommendations to the CIS Ombudsman, 8

Recommended General Aviation Security Action Items, 40

Regional Resiliency Assessment Program (RRAP), 30

Reporting

AIRBUST program, 10

America's Waterways Watch, 9

CBP - 1-800 BE ALERT, 10

Dams Sector Suspicious Activity Reporting Tool, 31

eAllegations, 11

Forced Labor, 21

The National Intellectual Property Rights Coordination Center, 22

Traveler Redress Inquiry Program (DHS TRIP), 6

U. S. Computer Emergency Readiness Team (US-CERT) Operations Center, 15

U.S. Immigration and Customs Enforcement (ICE) Tip-Line, 22

Research and Test Reactors (RTRs) Voluntary Security Enhancement Program, 30

Retail Security Webinar, 31

Retail Video: "What's in Store - Ordinary People/Extraordinary Events", 24, 26

S

SAFECOM Guidance for Federal Grant Programs, 15

SAFECOM Program, 16

Safeguarding America's Transportation System Security Guides, 40

School Transportation Security Awareness (STSA), 38

Science & Technology Basic Research Focus Areas, 34

Screening Partnership Program, 42

Sector-Specific Agency Executive Management Office/Transportation Security Administration (TSA) Joint Exercise Programs, 30

Sector-Specific Pandemic Influenza Guides (Sector-Specific Agency Executive Management Office (SSA EMO) Sectors), 28

Secure Fixed Base Operator, 42

Secure Flight, 42

Secure Freight Initiative (SFI) and Importer Security Filing and additional carrier requirements (10+2), 13
SECURE™ Program, 34
 Security Awareness for Levee Owners Brochure, 26
Security Outreach and Awareness Program (SOAP), 30
 Security Seminar, Exercise Series with State Chemical Industry Councils, 30
Site Assistance Visit (SAV), 30
Soft Target Awareness Course, 24
Software Assurance (SwA) Program, 16
Sports Leagues, 28
State and Local Implementation Snapshot, 28
Student and Exchange Visitor Program, 22
Submit a Case Problems to the CIS Ombudsman, 8
Summary of the NIPP and SSPs, 28
Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act), 34
Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff Course, 25
Surveillance Detection Training for Municipal Officials, State and Local Law Enforcement Course, 25
Surveillance Detection Web Training, 25

T

Technical Assistance (TA) Program, 20
Technical Resource for Incident Prevention (TRIPwire), 32
Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition, 35
Technology Transfer Program, 35
The National Intellectual Property Rights Coordination Center, 22
The Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT), 34
Threat Detection and Reaction by Retail Staff (Point of Sale), 25
Tornado Safety Initiative, 20
Training
 Retail Video: "What's in Store - Ordinary People/Extraordinary Events", 24
 20-Minute Retail Security Webinar, 31
 Active Threat Recognition for the Shopping Center/Retail Security Officer, 23
 Airport Watch/AOPA Training, 37
 Alien Flight/Flight School Training, 37
 Are You Ready? An In-depth Guide to Citizen Preparedness, 17
 Awareness & Location of Explosives-Related Threats (ALERT), 35
 Bomb Event Management Web Training, 23
 Bombing Prevention Workshop, 23
 Center for Domestic Preparedness (CDP), 17

Chemical Sector Explosive Threat Awareness Training Program, 23
 Community Emergency Response Team (CERT), 17
 Control Systems Security Program (CSSP) Instructor-Lead Cybersecurity Training, 14
 Counterterrorism Protective Measures Course, 23
 Critical Infrastructure and Key Resources (CIKR) Learning Series, 23
 Critical Infrastructure and Key Resources (CIKR) Training Module, 23
 Cyber Education and Workforce Development Program (CEWD), 14
 DHS 90-Minute Retail Security Webinar, 31
 DHS/Commercial Facilities Training Resources Guide pamphlet, 23
 Disability Preparedness, 5
 Emergency Services Sector Training Catalog, 24
 E-Verify and Unfair Labor Practices, 5
 FEMA Emergency Management Institute Independent Study Program, 17
 FEMA Emergency Management Institute Programs, 17
 FEMA Learning Resource Center, 17
 First Observer™ Training, 37
 H1N1 Training for transit agency managers and employees, Educational opportunities in transportation, 36
 Hazmat Motor Carrier Security Action Item Training (SAIT) Program, 37
 Hazmat Motor Carrier Security Self-Assessment Training Program, 37
 Human Causes and Consequences of Terrorism. *See* DHS Center of Excellence: National Consortium for the Study of Terrorism and Responses to Terrorism (START)
 IED Recognition and Detection for Railroad Industry Employees Training (CD), 37
 Improvised Explosive Device (IED) Awareness / Bomb Threat Management Workshop, 24
 Improvised Explosive Device (IED) Awareness Web Training, 24
 Improvised Explosive Device (IED) Search Procedures Workshop, 24
 Independent Study Course IS 870
 Dams Sector
 Crisis Management Overview, 24
 Independent Study Course IS-821 Critical Infrastructure and Key Resources (CIKR) Support Annex, 24
 Independent Study Course IS-860.a National Infrastructure Protection Plan (NIPP), 24
 Integrated Common Analytical Viewer (iCAV) Web-based Training, 24
 Intermodal Security Training and Exercise Program, 37
 Land Transportation Antiterrorism Training Program (LTATP), 37

Maritime Passenger Security Courses, 37
 Mass Transit and Passenger Rail - Bomb Squad Response to Transportation Systems, 37
 Mass Transit and Passenger Rail - Field Operational Risk and Criticality Evaluation (FORCE), 38
 Mass Transit Security Training Program Guidelines, 38
 Mass Transit Smart Security Practices, 38
 National Center for Command, Control, and Interoperability (C2I), 36
 National Center for Food Protection and Defense (NCFPD), 35
 National Center for Foreign Animal and Zoonotic Disease Defense (FAZD), 36
 National Center for Risk and Economic Analysis of Terrorism Events (CREATE), 35
 National Information Exchange Model (NIEM) Program, 6
 Operation Secure Transport (OST), 38
 Pipeline Security Awareness for the Pipeline Industry Employee Training CD and Brochures, 38
 Private Sector Counterterrorism Awareness Workshop, 24
 Public Transportation Emergency Preparedness Workshop - Connecting Communities Program, 38
 School Transportation Security Awareness (STSA), 38
 Soft Target Awareness Course, 24
 Surveillance Detection Training for Commercial Infrastructure Operators and Security Staff Course, 25
 Surveillance Detection Training for Municipal Officials, State and Local Law Enforcement Course, 25
 Surveillance Detection Web Training, 25
 Threat Detection and Reaction by Retail Staff (Point of Sale), 25
 Training Video "Check It!: Protecting Public Spaces", 24
 U.S. Fire Administration's National Fire Academy Residential Training Programs, 17
 Web-Based Chemical Security Awareness Training Program, 25
Transit Agency Security and Emergency Management Protective Measures, 40
Transportation Sector Network Management Highway and Motor Carrier Division Annual Report, 40
Transportation Security Administration Counterterrorism XE "Counterterrorism" Guides, 40
Transportation Security Grant Programs, 42
Transportation Worker Identification Credential (TWIC), 42 travel, 6, 41, 42
Traveler Redress Inquiry Program (DHS TRIP), 6, 41
TRIPwire Community Gateway (TWCG), 32
Trusted Traveler Programs (TTP), 13
TSA Alert System, 40

U

U. S. Computer Emergency Readiness Team (US-CERT) Operations Center, 15
 U.S. Border Patrol Blotter, 10
 U.S. Border Patrol Checkpoints Brochure, 10
 U.S. Citizenship and Immigration Services (USCIS) Resources, 7
 U.S. Citizenship and Immigration Services (USCIS) Information for Employers and Employees, 7
 U.S. Citizenship and Immigration Services (USCIS) Ombudsman, 8
 U.S. Civics and Citizenship Online Resource Center for Instructors, 7
 U.S. Coast Guard Auxiliary, 9
 U.S. Coast Guard Maritime Information eXchange (“CGMIX”), 9
 U.S. Coast Guard Navigation Center, 9
 U.S. Fire Administration Fire Prevention and Safety Campaigns, 19

U.S. Fire Administration Publications, 19
 U.S. Fire Administration’s National Fire Academy Residential Training Programs, 17
 U.S. Immigration and Customs Enforcement (ICE) Mutual Agreement between Government and Employers Program, 22
 U.S. Immigration and Customs Enforcement (ICE) Office of Public Affairs, 22
 U.S. Immigration and Customs Enforcement (ICE) Privacy Office, 22
 U.S. Immigration and Customs Enforcement (ICE) Tip-Line, 22
 U.S. Immigration and Customs Enforcement (ICE) Victim Assistance Program, 22
 U.S. Secret Service, 5
 Unified Hazard Mitigation Assistance (HMA) Grant Programs, 20
 USCG National Maritime Center (NMC), 9
 USCIS Asylum Program, 7
 USCIS Genealogy Program, 7

USCIS Office of Public Engagement (OPE), 7
 User’s Guide on Security Seals for Domestic Cargo, 40

V

Vessel Documentation (US Flag Vessels), 9
 Video Quality in Public Safety (VQiPS), 35
 Visa Waiver Program (VWP), 13
 Voluntary Chemical Assessment Tool (VCAT), 32

W

Web-Based Chemical Security Awareness Training Program, 25
 Welcome to the United States: A Guide for New Immigrants, 7
 Western Hemisphere Travel Initiative (WHTI), 13
 Who’s Who in Chemical Sector Security (October 2008), 28
 Who’s Who in Emergency Services Sector, 28



S&T Commercialization: An Overview

The DHS Science and Technology's commercialization efforts are headed by the Chief Commercialization Officer (CCO), a position created in August 2007 within the Transition Office in S&T. The CCO works with a small staff comprised of one Federal Employee and three SETA support contractors. Commercialization is broadly defined as the process of developing markets and producing and delivering products or services for sale.

The CCO is responsible for creating initiatives that identify, evaluate and commercialize technology for the specific goal of rapidly developing and deploying products and services that meet the specific operational requirements of the Department of Homeland Security's operating components and its stakeholders such as first responders. Developing and driving the implementation of DHS S&T's outreach with the private sector to establish and foster mutually beneficial working relationships to facilitate cost-effective and efficient product/service development efforts is also a critical job responsibility. Recognizing that many DHS solutions require widely distributed products or services, the CCO works to leverage the private sector's resources to develop COTS products aligned specifically to meet DHS operational requirements for later potential procurement.

The CCO assists the private sector by enabling them to learn about DHS business opportunities, and plays a vital role internal to DHS to coach, teach and assist project managers, transition managers and division heads in developing detailed operational requirements through recently published books, tutorials and teaching materials he has spearheaded. In addition, he works closely with the Deputy Secretary and operating components on initiatives and programs to identify and define the operational needs for capability gaps throughout the entire Department.

MISSION

The mission of the CCO is to develop and execute programs and processes that identify, evaluate and commercialize widely-distributed products or services that meet the operational requirements of the Department of Homeland Security's operating components, first responder community and other Department stakeholders when required. Developing and managing DHS S&T's outreach effort with the private sector to establish and foster mutually-beneficial working relationships leading to the fielding of technologies to secure the Nation is a primary, day-to-day function of the CCO.

MAJOR POLICY/PROGRAM INITIATIVES

- **“Developing Operational Requirements (Version 2.0)”** a 353 page book that assists in the communication of needs throughout the Department and externally to the private sector when appropriate. The development of detailed operational requirements for DHS projects will ensure that efficacious products, systems or services are developed to address specific, well articulated needs.
- **The Development and Implementation of a Commercialization Process for DHS** combines the benefits of a pure government Acquisition process and a pure private sector commercialization process into a process that guides product development in a cooperative strategic partnership between the public and private sector in which all parties benefit, resulting in positive benefits for the taxpayers.
- **The SECURE Program** is an efficient and cost-effective program to foster cooperative "win-win" partnerships between DHS and the private sector. This innovative program has

http://www.dhs.gov/xres/programs/gc_1211996620526.shtm.

- **The FutureTECH Program** is reserved for those critical research/innovation focus areas that could be inserted eventually into Department of Homeland Security acquisition or commercialization programs when development reaches TRL-6 based on metrics and milestones more specific than those of a broad technology need statement alone, yet not as specific as a detailed C-ORD. The objective of the FutureTECH Program is to establish mutually-beneficial partnerships with the private sector, national laboratories, university community and other Research and Development (R&D) organizations to develop technologies/capabilities that address the long-term needs of the Department and its stakeholders. See http://www.dhs.gov/files/programs/gc_1242058794349.shtm.
- **Public Relations and Outreach** efforts to inform the public on “How to do Business with DHS” is receiving positive feedback from the private sector and media. Outreach efforts center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department. Several articles have been written about our commercialization efforts. Outreach efforts are conducted through invited talks to trade conventions, reaching small, medium and large businesses. Efforts also extend to meet with minority, disadvantaged and HUB Zone groups on a regular basis.
- **A detailed company overview database** containing non-proprietary information about companies’ capabilities, technologies and products aligned to DHS needs has been created. The database provides a given company’s alignment to specific capability gaps found in the “High Priority Technology Needs” document (May 2009), as well as possible use by the DHS operating components. This information has been compiled from responses received as part of our private sector outreach efforts and is useful to identify possible solution providers for a known set of requirements.



Requirements Development Initiative

The requirements development initiative is spearheaded by the Chief Commercialization Officer (CCO) in the Science and Technology Directorate. The goal of this initiative is to improve the articulation and communication of detailed operational requirements to facilitate efficient and cost-effective product development and procurement activities.

BACKGROUND

The mission of the development of operational requirements across the Department is to ensure the accurate and timely development and deployment of products and services to aid in the implementation of the mission critical objectives of the operating components and first responders. Requirements define the detailed problems and needs that will close existing capability gaps.

Requirements provide criteria against which solutions can be tested and evaluated, ensuring informed purchasing decisions on products, systems or services that achieve the stated operational goals. A detailed requirements analysis can uncover hidden requirements as well as discover common problems across programs and various DHS Components. Detailed operational requirements will guide product development so that solutions specifications actively solve the stated problems. This analysis also facilitates market and technology scans to determine if feasible solutions current exist, saving DHS significant time and money on unnecessary new product development efforts.

CURRENT STATUS

The requirements development initiative has yielded the publication of six books to assist in the development of requirements. *Requirements Development Guide*, *Developing Operational Requirements*, *Developing Operational Requirements (Version 2.0)*, *Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good: DHS's Entry into Commercialization*, *First Responder Capstone IPT: Delivering Solutions to First Responders*, and *Critical Infrastructure Key Resources: Using Commercialization to Develop Solutions Efficiently and Effectively* were written, published and approved for public release as a resource on requirements hierarchy, elicitation and the role that requirements play in the product development life cycle. These books are being distributed throughout DHS by the CCO, Private Sector Office, Office of Public Affairs and the DHS Librarian.

In addition to the requirements development books, training courses with a detailed curriculum and background materials have been created for instructor-led learning opportunities for DHS employees.

Commercialization processes and programs are included in the future Acquisition Management Directive MD102-01.



SECURE™ Program

The SECURE Program – DHS Science and Technology’s innovative business initiative that enables collaboration of public and private entities to develop products and services rapidly to protect the Homeland to the benefit of the American taxpayer, private sector and DHS. The goal of the SECURE Program is to leverage the resources of the private sector to develop solutions aligned with and tested against DHS/first responder-sponsored detailed operational requirements at using the private sector’s money and resources. DHS components can make better-informed purchasing decisions on products or services specifically aligned to their operational needs. The SECURE Program is managed by the Chief Commercialization Officer and operates under the budget for Science and Technology’s Director of Transition for FY10. See http://www.dhs.gov/xres/programs/gc_1211996620526.shtm.

BACKGROUND

With the initiation of the SECURE Program in June 2008, the Department began posting detailed operational requirements documents on its website site that provide information outlining specific operational needs and a conservative estimate of the potential available market of a given product, system or service to private sector entities. Private sector entities can make a business case for development of solutions and conduct third party independent test and evaluation (T&E) by recognized labs against the given C-ORD at their cost and DHS will validate the company’s T&E results. DHS components and first responders will be able to make informed purchasing decisions on successful products or services aligned to the given C-ORD.

The benefits of this program are far reaching. DHS benefits from gaining a better understanding of its needs and by leveraging the free-market system to have multiple private sector entities offering possible solutions, all aligned to DHS’ specific needs and at a speed-of-execution not typically seen in the public sector. The private sector receives from DHS critical information in order to develop business cases to begin development of solutions to a given DHS-sponsored C-ORD with the possibility of gaining access to significant potential available markets found throughout DHS and its ancillary markets. The American taxpayer also benefits when DHS components receive technology solutions to enhance their mission capabilities, developed in a cost-effective and efficient manner.

CURRENT STATUS

The SECURE Program has resulted in the development of eight C-ORDs, which are posted on dhs.gov, outlining detailed operational needs for DHS end-users. On a similar note, over twenty additional C-ORDs are in the process of being developed, eighty three potential private sector partners have expressed interest in the SECURE Program and the C-ORDs currently posted on dhs.gov, and three CRADAs have been signed to date.

The CCO continues to meet with DHS operating components and first responders to identify capability gaps and develop C-ORDs that detail the requirements to fill those needs. The CCO has also coordinated efforts with economists in the Private Sector Office (PSO) to begin development of PAM estimates, as well as efforts with the DHS Test & Evaluation and Standards Division (TSD) regarding evaluation by recognized third-party testing data related to proposed solutions.

The SECURE Program already appears successful despite its infancy, operating ahead of schedule with greater-than-expected impact. The program has been embraced by Senior DHS Management including Deputy Secretary (S2) and the leaders of the “Gang of Seven (G-7)” operating components. S2 has directed the G-7 to work with the CCO through the SECURE Program to develop C-ORDs based on needs for additional possible commercial solutions from the private sector.

The Commercialization Office has conducted a series of SECURE Program Working Group meetings to develop the detailed process for the execution of the SECURE Program. These productive meetings provided useful feedback and comments to improve the flow process for the program. Detailed work flows, swim lanes, and roles and responsibilities were discussed and approved by the Working Group. Supporting documents were also compiled in a library of resources to assist those proposed to be involved in the SECURE Program process. The Commercialization Office will provide a brief to the Under Secretary based on the results received from the participants of the SECURE Program Working Group. Members of the working group include: DOT, OGC, TSD, OAD, APMD and Tech Transfer.

The voluntary participation and contribution to the program by DHS and the private sector who view the SECURE Program as a “best practice” reflects the enormous benefits that the program brings to DHS, the private sector and the American taxpayer.



FutureTECH™ Program

The FutureTECH Program – The objective is to establish mutually-beneficial partnerships with the private sector, national laboratories, university community and other Research and Development organizations to develop technologies/capabilities that address the long-term needs of the Department and its stakeholders. FutureTECH identifies and focuses on the future needs of the Department as fully deployable technologies and capabilities, in many cases, are not readily available in the private sector or federal government space.

FutureTECH outlines focus areas for which current technology only exists at earlier stages on the technology readiness scale (TRL 1-6). Its "sister program" SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) is for fully deployable technology readiness level nine products and services. See http://www.dhs.gov/files/programs/gc_1242058794349.shtm.

BACKGROUND

With the initiation of the FutureTECH Program in May 2009, DHS S&T is able to efficiently and cost-effectively leverage the resources, skills, experience and productivity of the private sector and other non-DHS entities to develop technologies/capabilities in alignment with research/innovation focus areas obtained from DHS S&T. These technologies/capabilities can ultimately be used by DHS, the first responder community, critical infrastructure/key resources owners/operators and other DHS stakeholders. In essence, FutureTECH provides a "window of visibility" or "preview" of research/innovation focus areas that DHS and its stakeholders believe are essential in future products and services where detailed operational requirements documents can not be fully developed at this time. The program also provides insight into areas where Independent Research and Development (IRAD) monies could be spent by firms possessing funding to address DHS research/innovation focus areas.

To state it simply, the SECURE Program focuses on product/service development to create products and services to protect our nation in the shorter term, while FutureTECH will focus on critical research/innovation focus areas at lower TRLs for eventual deployment. Like all of the Commercialization Office's programs, all parties "win" in the FutureTECH Program--the private sector and others by receiving valuable insight into future research/innovation focus areas needed by DHS and its stakeholders. DHS "wins" because it will leverage the valuable skills, experience and resources of the private sector and other non-DHS entities to expedite efficient and cost-effective technology development; the non-DHS entities "win" because they receive valuable information useful for their own strategic plans; and most importantly, all American taxpayers "win" because this innovative partnership yields valuable technologies/capabilities aligned with research/innovation focus areas developed in a more cost-effective and efficient way saving taxpayer money.

CURRENT STATUS

As of April 2010, the FutureTECH Program is still in its pilot phase and ten research/innovation focus area documents have been drafted, approved, sponsored and placed on the DHS website. All ten focus on technologies that detect or prevent the detonations of improvised explosive devices. On a similar note, five potential private sector partners have expressed interest in the FutureTECH Program and the research/innovation focus area documents currently posted on

dhs.gov. As of April 2010, the Commercialization Office via the FutureTECH Program has not entered into a CRADA agreement with any potential private sector partner.

The FutureTECH Program has experienced moderate success despite its infancy. The program has been embraced by Senior DHS Management including Deputy Secretary (S2) and the leaders of the “Gang of Seven (G-7)” operating components. S2 has directed the G-7 via Management Directive 102-01 to work with the CCO through the FutureTECH Program to develop research/innovation focus area documents based on needs for additional possible commercial technologies/capabilities from the private sector.

Due to the success of the SECURE Working Group, the Commercialization Office received feedback on this “sister program.” The FutureTECH Program’s primary focus is on the non-federal first responders and critical infrastructure/key resources (CIKR) owners and operators. The FutureTECH Program is reserved for those research/innovation focus areas that could be inserted eventually into DHS acquisition or commercialization programs when development reaches TRL-6, which is described as a representative model or prototype system that is tested in a relevant environment. The Commercialization Office is responsible for the management and oversight of the program and will work closely with all participants in the process. Members of the working group include: DOT, DOR, DOI, OGC, TSD, OAD, APMD and Tech Transfer.

The objective of the FutureTECH Working Group is to develop an established process for the following:

- Technical subject matter experts can review basic research/innovation focus area documents
- Review statements of work and developmental test plans (potentially insert into a CRADA agreement between DHS and private sector entity)
- Review private sector T&E data to validate that a “technology/capability does what it claims to do” and that the technology/capability meets/exceeds the stated needs in the basic research/innovation focus area

The Commercialization Office believes that the working group should strike a balance between satisfying legitimate needs for a detailed, defensible and fair process; one that “breathes” to allow for creativity; and one that assists (not burdens) project managers as an additional “tool in their toolbox”. At the moment, DOI and various project managers remain concerned about the FutureTECH flow process and the increased work load for S&T project managers.

After receiving input from TSD, the Commercialization Office will engage the assistance of FFRDCs or potential contractors in order to expedite the timely review of T&E data to efficiently and effectively develop technologies and capabilities at minimum cost to the Department.

The CCO continues to meet with DHS operating components and first responders to identify capability gaps and develop research/innovation focus area documents that detail the preliminary requirements to fill those needs. The CCO has also coordinated efforts with economists in the Private Sector Office (PSO) as well as efforts with the DHS Test & Evaluation and Standards

Division (TSD) regarding evaluation by recognized third-party testing data related to proposed technologies/capabilities.

The voluntary participation and contribution to the program by DHS and the private sector who view the FutureTECH Program as a “best practice” reflects the enormous benefits that the program brings to DHS, the private sector and the American taxpayer.



Commercialization Process Overview

The development and implementation of a commercialization process for DHS, led by the S&T Commercialization Office, combines the benefits of a pure government Acquisition model and a pure private sector commercialization model into a process that guides product development in a cooperative strategic partnership between the public and private sector in which all parties benefit, resulting in positive benefits for the taxpayers.

BACKGROUND

The development and implementation of a commercialization process for DHS is an opportunity for DHS to work closely with the private sector to develop widely distributed products/services aligned to the needs of DHS and its ancillary markets such as first responders and CI/KR owners and operators. DHS leverages the significant potential available markets for homeland security technology applications, along with detailed operational requirements from DHS stakeholders to encourage private sector investment and development of products/services for potential procurement by DHS. The benefits of this partnership extend to both the public and private sectors who receive considerable resources from one another; DHS receives products/services aligned to its needs through a highly competitive open market system, and the private sector receives detailed information on requirements and market potential. In addition, American taxpayers benefit as product development costs are borne by the private sector, saving the DHS money and delivering quality products used in protecting the Homeland.

CURRENT STATUS

The Commercialization process has begun to create a “commercialization mindset” at DHS in which S&T program managers actively seek opportunities to articulate the needs of their customers (DHS operating components, first responders, CI/KR owners and operators, etc.) for the purpose of providing that information to the private sector along with a conservative estimate of the potential available market of a given need/requirement. Through the execution of the SECURE and FutureTECH Programs, the Commercialization Office has created a vehicle by which DHS can present information on requirements and potential available markets to potential solution providers in a free-market system. The Commercialization Office has been working to incorporate its practices into an upcoming Management Directive to affect the Department’s Acquisition processes.

H.R. 4842, released in March 2010, will authorize appropriations for DHS S&T for fiscal years 2011 and 2012, and for other purposes. This bill also authorizes the formal establishment of an "Office of Public-Private Partnerships," which will fall under DHS S&T. Objectives of the Office of Public-Private Partnerships include:

- Provide guidance on how to pursue proposals to develop or deploy homeland security technology, including persons associated with small business
- Coordinate with components of the Department to issue announcements seeking unique and innovative homeland security technology
- Promote interaction between homeland security researchers and private sector companies to accelerate transition research or a prototype into a commercial product
- Conduct technology research assessment and market place analysis



Private Sector Outreach Overview

The private sector outreach efforts of the Commercialization Office in the Science and Technology Directorate are designed to provide information to the public on “How to do Business with DHS.” Efforts demonstrate the value of engaging in mutually beneficial relationships to provide business opportunities to produce products/services to DHS components and ancillary markets such as first responders and critical infrastructure/key resources owners and operators.

BACKGROUND

The private sector outreach efforts of the Commercialization Office center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department. Outreach efforts are conducted through invited talks to trade conventions, reaching small, medium and large businesses. Efforts also extend to meet with minority, disadvantaged and HUB Zone groups on a regular basis. As of April 2010, the Commercialization Office has written six books on requirements development and commercialization that have been released to the public, and over 20 articles. Several articles have been written about the commercialization efforts in domestic and international publications. The Commercialization Office maintains two websites, one of which is open to the public, for information dissemination.

CURRENT STATUS

Current private sector outreach efforts have yielded significant positive feedback from the private sector interested in learning more about business opportunities that exist at DHS. As of April 2010, a database of company overviews submitted to the Commercialization Office has collected and aligned over 480 companies offering over 2,500 technologies/products/services aligned to DHS needs. The Chief Commercialization Officer speaks regularly at conferences, engages with regional business development networks and continues to spread the word about commercialization efforts both to public audiences, as well as with internal DHS operating components and leadership. In addition to internal and external DHS websites, the Commercialization Office has a presence on business-oriented social networking sites such as LinkedIn as well as video sharing websites such as YouTube.

As of April 2010, the Commercialization Office conservatively estimates that 60,625 organizations/entities/etc. have been exposed to DHS Commercialization outreach efforts; 12,126 Full Response Packages have been sent to private sector and non-DHS entities; 2,425 Full Response Packages have been closely reviewed by private sector and non-DHS entities; and 485 completed company profiles have been received by Commercialization Office. Please note that these numbers do not include the millions of people who are made aware of Commercialization activities through various forms of media such as television, print media, websites, etc.

In late August 2009, Los Angeles County faced its largest wild land fire in recorded history and the Commercialization Office visited and worked with the CAL FIRE Deputy Chief in order to better understand the challenges faced in fighting wild land fires, especially in the urban interface. Due to the wealth of information received from the visit, the Commercialization Office has continued to work closely with CAL FIRE to write and edit operational requirements documents to help first responders describe a number of problems that technology could solve.

Opportunities for the Private Sector



June 2010

Thomas A. Cellucci, Ph.D., MBA

Chief Commercialization Officer

U.S. Department of Homeland Security

Email: SandT_Commercialization@dhs.gov

Website: <http://bit.ly/commercializationresources>

Discussion Guide

- Overview of Department of Homeland Security
- Commercialization Office Initiatives at DHS
- Capstone Integrated Product Teams (IPTs)
- Market Potential is Catalyst for Rapid New Product Development
- Getting on the Same Page
- SECURE Program
- Safety Act Protection
- TechSolutions
- SBIR Opportunities
- Getting Involved
- Effecting Change in Government
- Summary



Homeland
Security

Homeland Security Mission

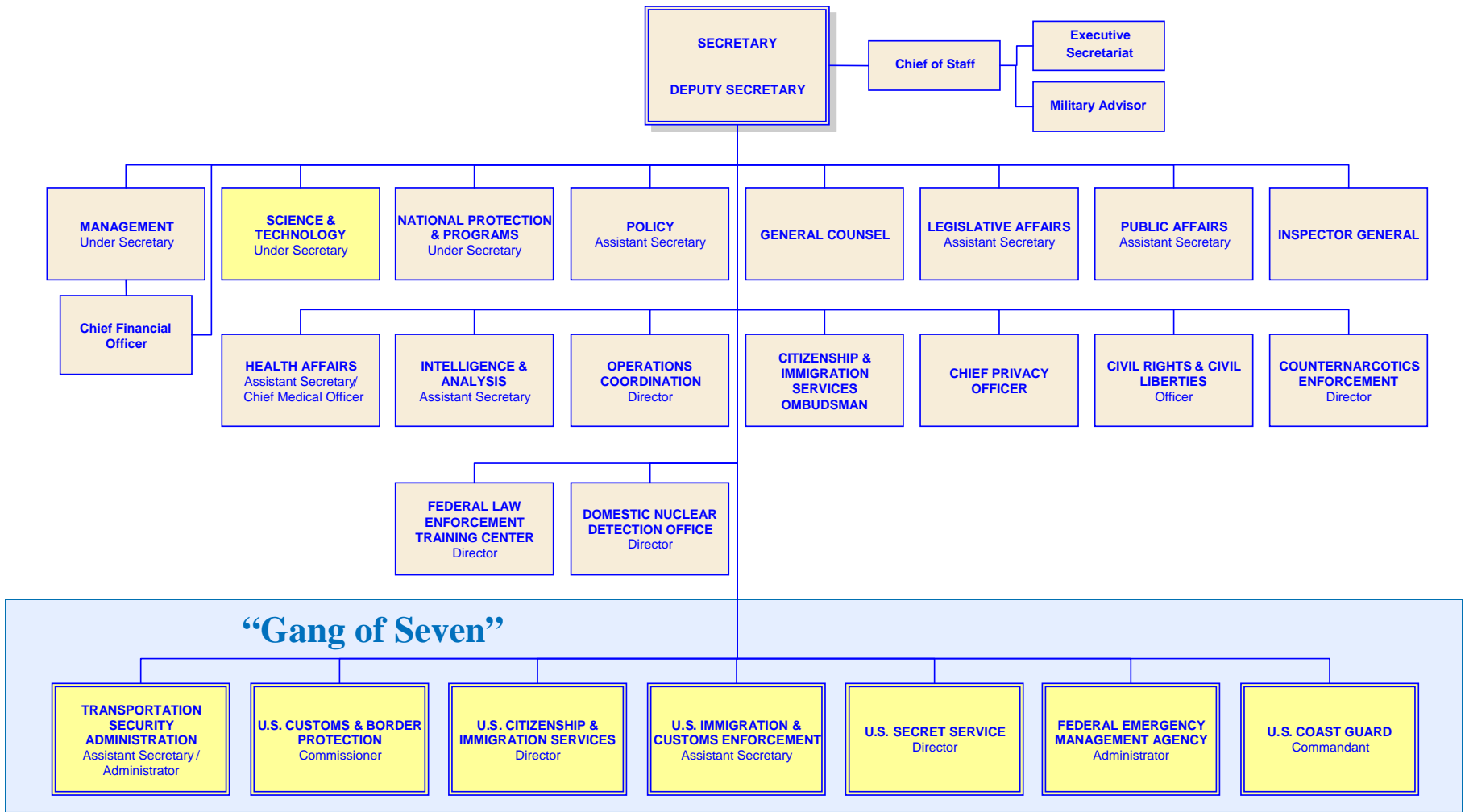


- Lead Unified National Effort to Secure America
- Prevent Terrorist Attacks Within the U.S.
- Respond to Threats and Hazards to the Nation
- Ensure Safe and Secure Borders
- Welcome Lawful Immigrants and Visitors
- Promote Free Flow of Commerce



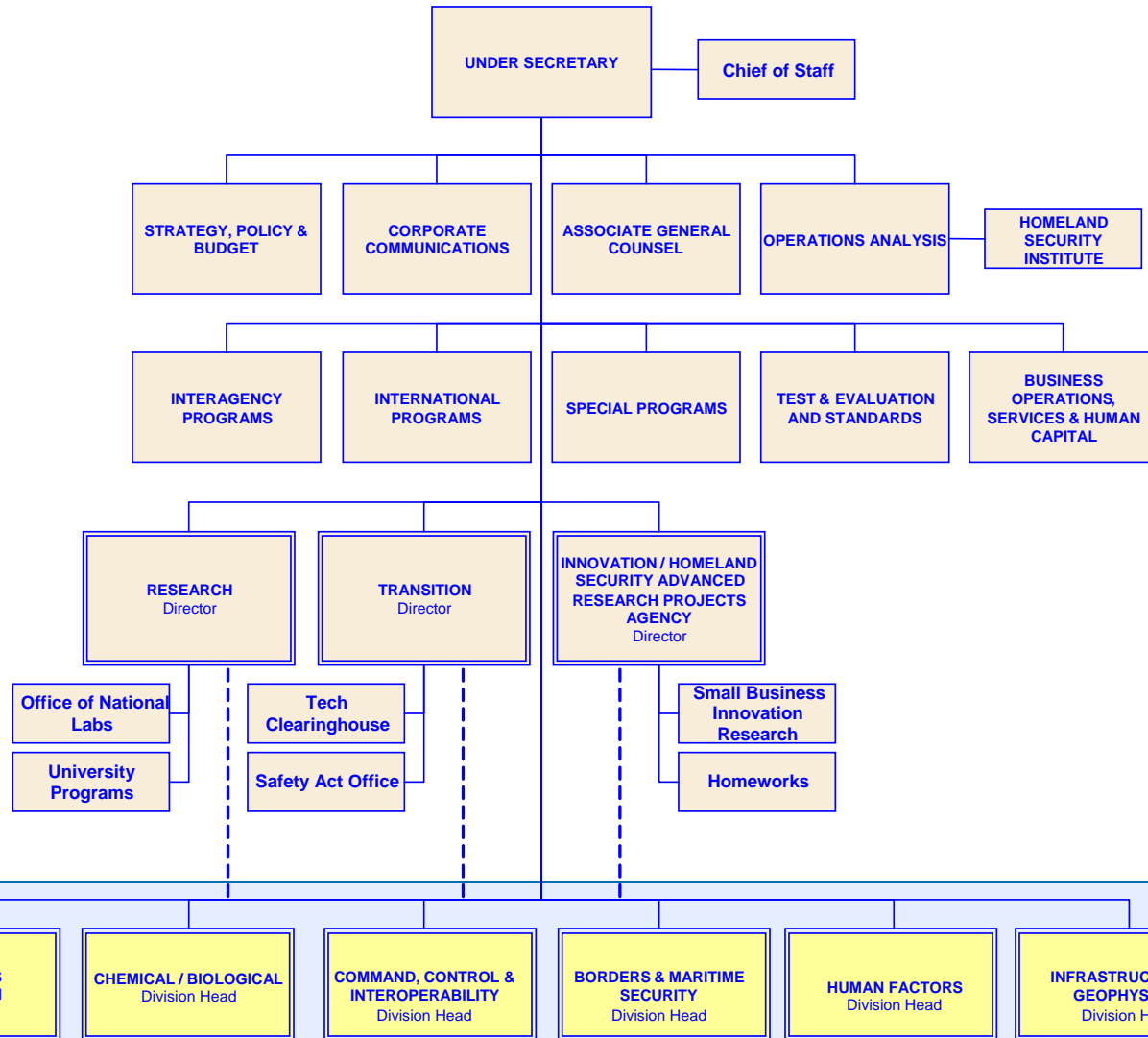
**Homeland
Security**

U.S. Department of Homeland Security



Homeland Security

Office of the Under Secretary for Science and Technology



Divisions Drive S&T Interactions with Customers

DHS S&T Goals

Consistent with the Homeland Security Act of 2002

- **Accelerate the delivery of enhanced technological capabilities** to meet the requirements and fill capability gaps to support DHS agencies in accomplishing their mission.
- Establish a lean and agile world-class S&T management team to deliver the technological advantage necessary to ensure DHS Agency mission success and prevent technological surprise.
- Provide leadership, research and educational opportunities and resources to develop the necessary intellectual basis to enable a national S&T workforce to secure the homeland.



**Homeland
Security**

DHS S&T Investment Portfolio

Balance of Risk, Cost, Impact, and Time to Delivery

Product Transition (0-3 yrs) <ul style="list-style-type: none">▪ Focused on delivering near-term products/enhancements to acquisition▪ Customer IPT controlled▪ Cost, schedule, capability metrics	Innovative Capabilities (1-5 yrs) <ul style="list-style-type: none">▪ High-risk/High payoff▪ “Game changer/Leap ahead”▪ Prototype, Test and Deploy▪ HSARPA
Basic Research (>8 yrs) <ul style="list-style-type: none">▪ Enables future paradigm changes▪ University fundamental research▪ Gov’t lab discovery and invention	Other (0-8+ yrs) <ul style="list-style-type: none">▪ Test & Evaluation and Standards▪ Laboratory Operations & Construction▪ Required by Administration (HSPDs)▪ Congressional direction/law

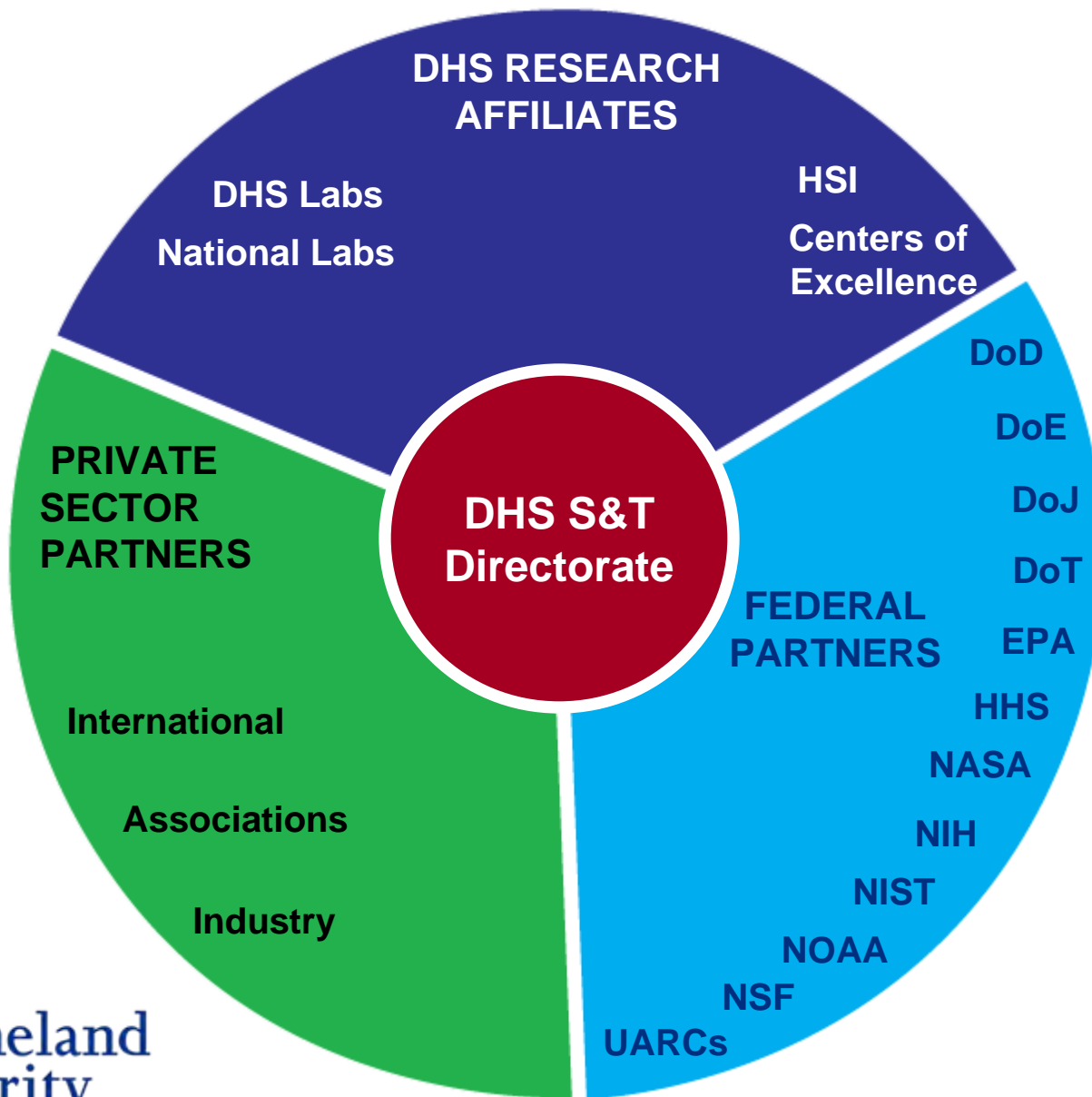
Customer Focused, Output Oriented



**Homeland
Security**

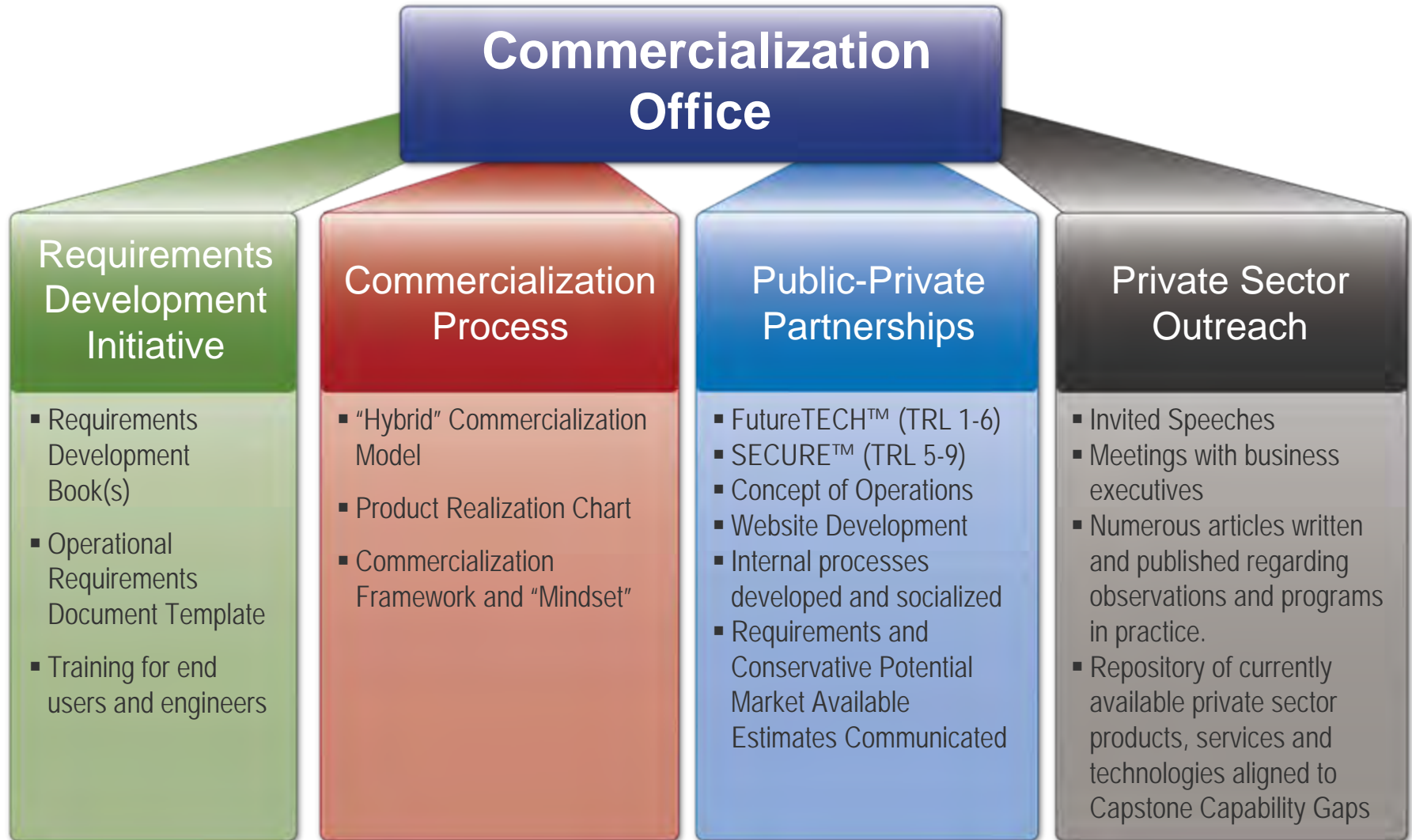


Homeland Security S&T Enterprise



Homeland Security

Commercialization Office: Major Activities



**Homeland
Security**

[http://www.dhs.gov/xabout/structure/
gc_1234194479267.shtm](http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm)

Commercialization Office Highlights:

- White House Office of Science and Technology Policy briefings (Chief Technology Officer Aneesh Chopra)
- Homeland Security Council: Recommended priority for FY11-15 for transportation security: SECURE Program
- Inclusion of Commercialization processes into DHS Acquisition Management Directive MD 102-01 (scheduled release September 2009)
- Homeland Security Advisory Council, Essential Technology Task Force Report June 2008
- Council on Competitiveness, Chief Commercialization Officer is first Federal Government Representative
- “Big Bang Economics”: CNN Feature Video with Jeanne Meserve
- “Burned, Baked and Blown Up”: Reuters Video with Rob Muir
- Two Federal Certification Programs developed and implemented—SECURE™ and FutureTECH™: Innovative public-private partnerships
- Published Five books (and more than 20 articles) on requirements development and public-private partnerships



**Homeland
Security**

Three Step Approach:

Keep it Simple and Make it Easy

1

Develop Detailed Requirements
And Relay Conservative Market Potential

2

Establish Strategic Partnerships

- Business Case Information
- Open Competition
- Detailed Mutual Responsibilities

3

Deliver Products!



Homeland
Security

Two Models for Product Realization

Big-A Acquisition

1. Requirements derived by Government
2. RFP and then cost-plus contract(s) with developer(s) (which incentivizes long intervals)
3. Focus on technical performance
4. Production price is secondary (often ignored)
5. Product price is cost-plus
6. Product reaches users via Government deployment

Performance is King

Relationship between end users and product developer is usually remote



Is there a
“Middle Ground”

Pure Commercialization

1. Requirements derived by Private Sector
2. Product development funded by the developer (which incentivizes short intervals)
3. Technical performance secondary (often reduced in favor of price)
4. Focus on price point
5. Product price is market-based
6. Product reaches users via marketing and sales channels

Performance/Price is King

Relationship between end users and product developer is crucial



**Homeland
Security**

A new model for Commercialization...

1. Development of Operational Requirements Document (ORD)
2. Assess addressable market(s)
3. Publish ORD and market assessment on public DHS web portal, soliciting interest from potential partners
4. Execute no-cost agreement (streamlined CRADA) with multiple Private Sector entities, transferring technology (if necessary)
5. Develop supporting grants and standards as necessary
6. Assess T&E after product is developed
7. New Commercial off the Shelf (COTS) product marketed by Private Sector with DHS support

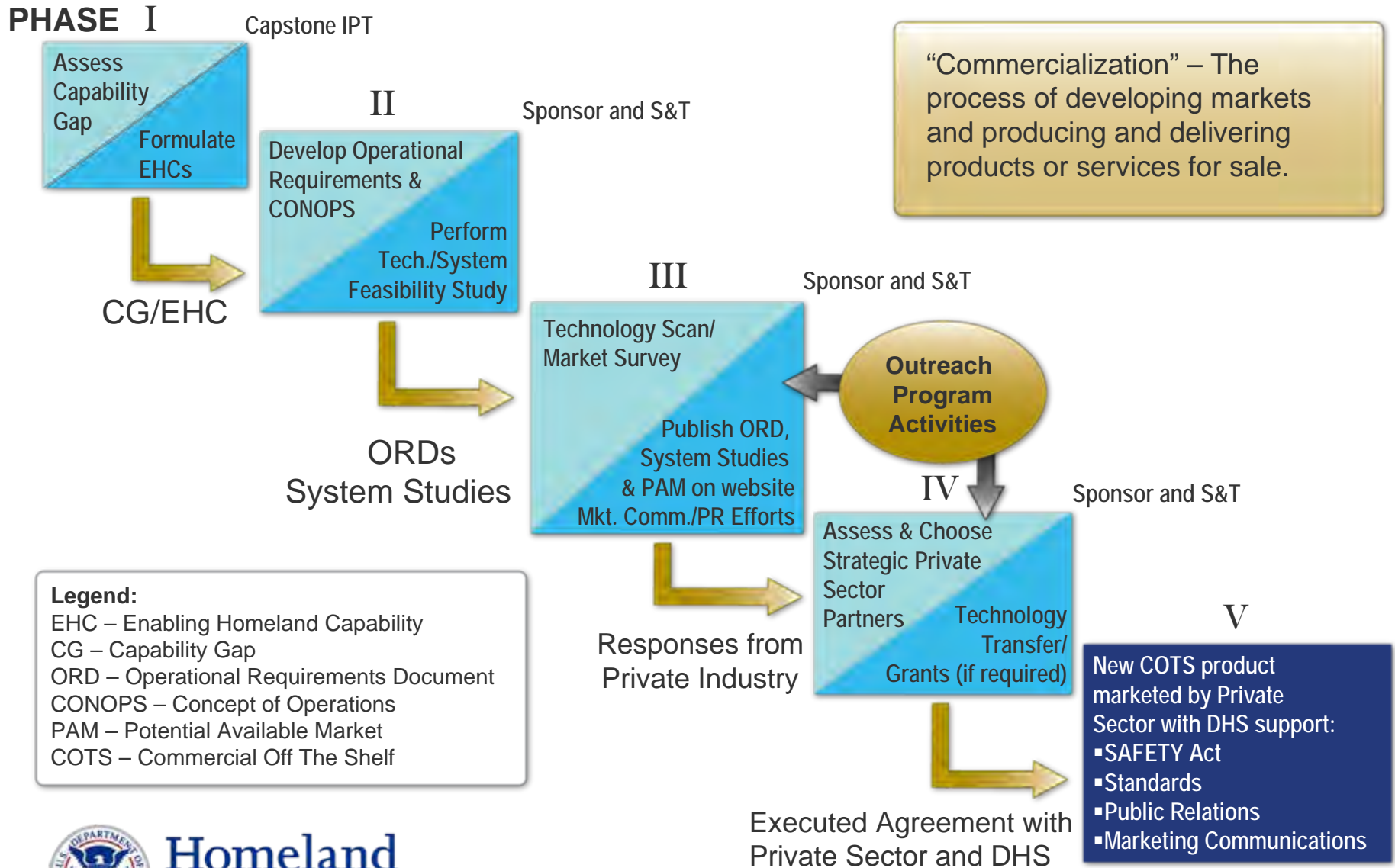
Differences from the Acquisition model:

- **Primary criteria for partner selection is market penetration, agility, and performance/price ratio**
- **Product development is not funded by DHS**
- **Government involvement is limited to inherently governmental functions (e.g., Grants and Standards)**

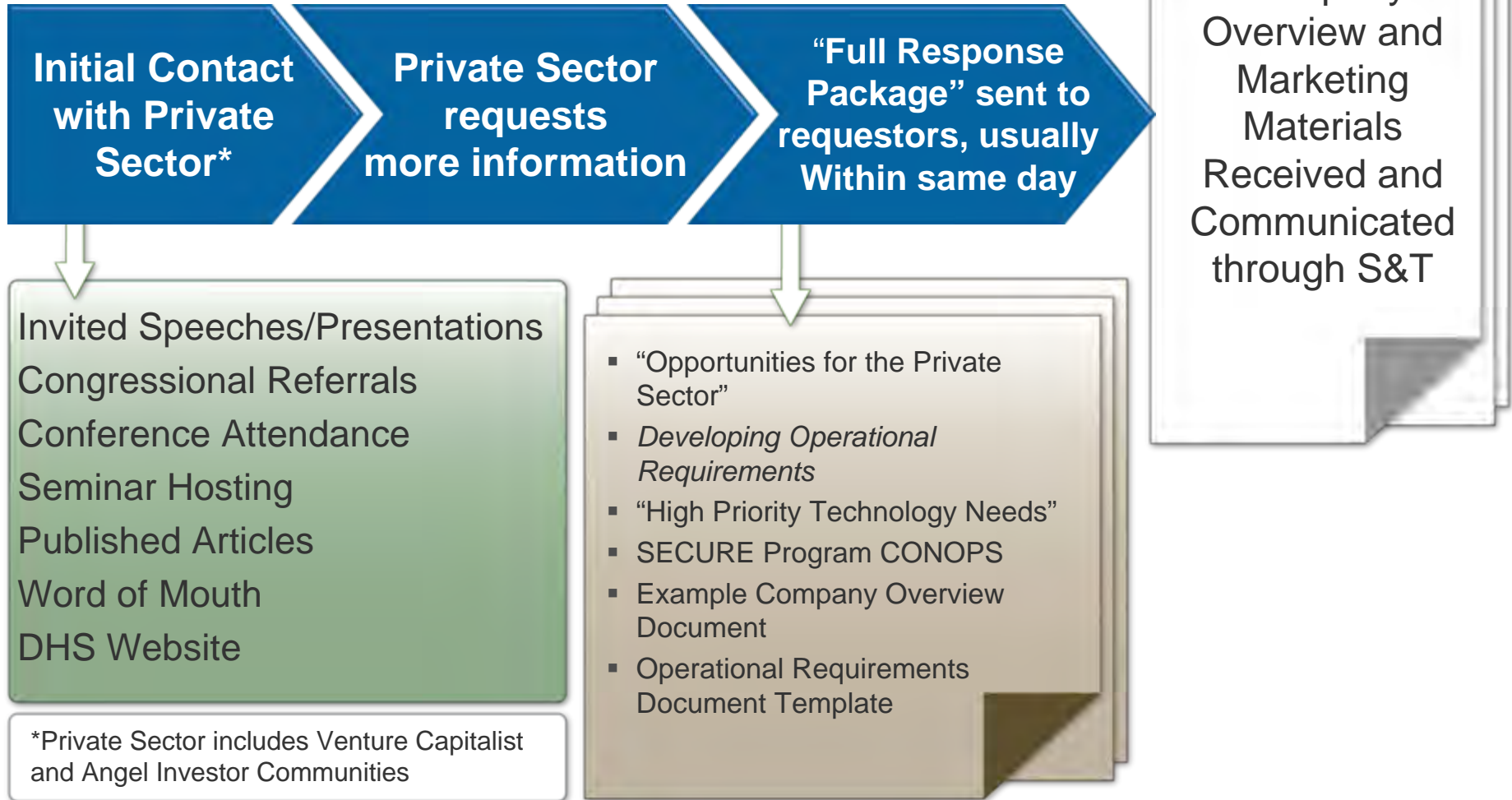


**Homeland
Security**

Commercialization Process

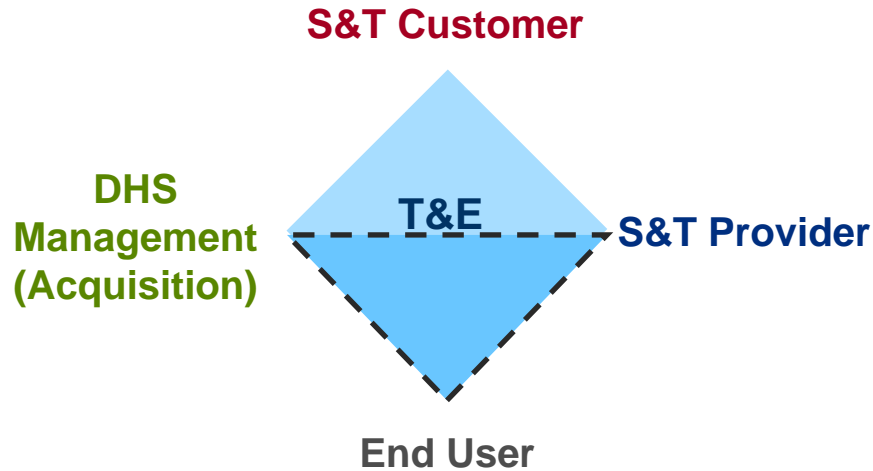


Contact with the Private Sector

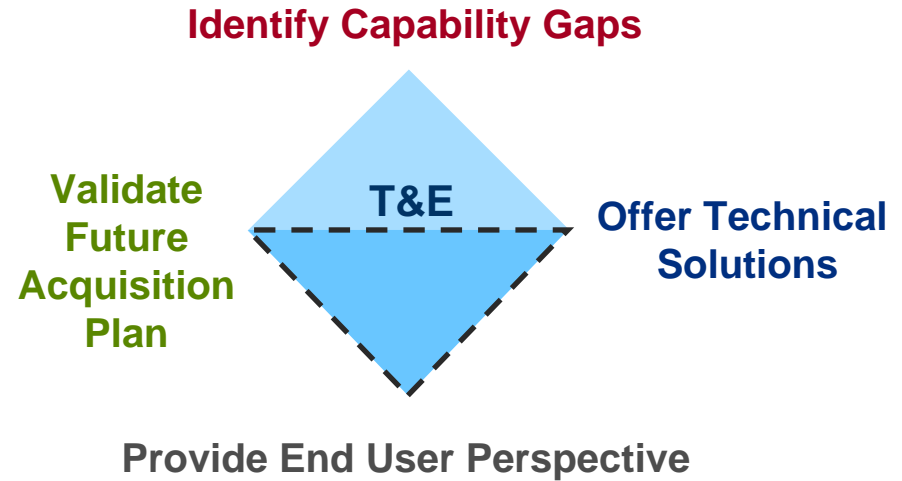


S&T Transition Capstone IPTs

Members and Function



- Industry Board of Directors Model
- Consensus-driven Process



End Result :
Prioritized Investments in S&T

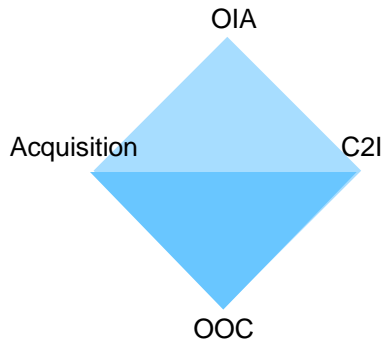


Homeland
Security

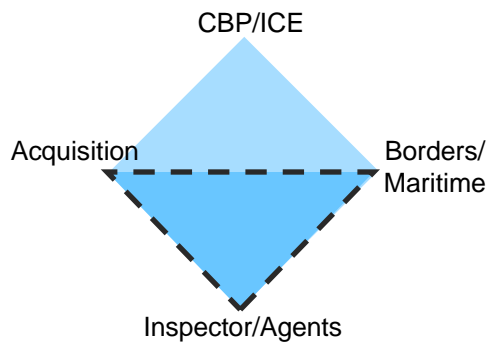
DHS S&T Capstone IPTs

Gathering Mechanism for Customer Requirements:

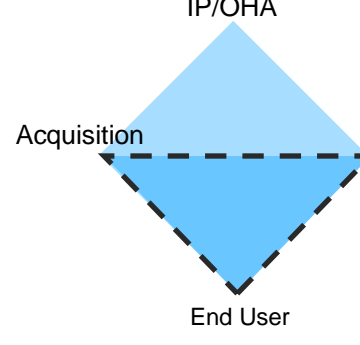
Information Sharing/Mgmt



Border Security

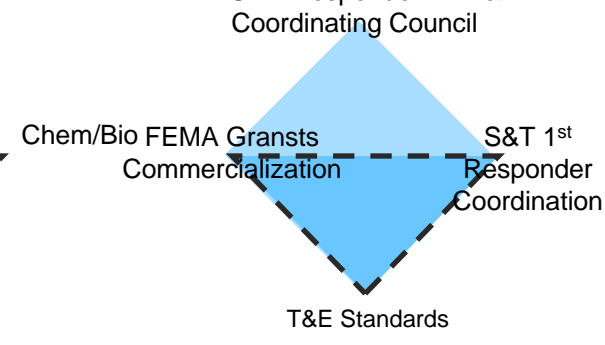


Chem/Bio

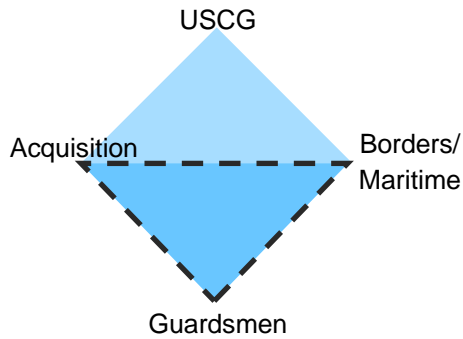


First Responders

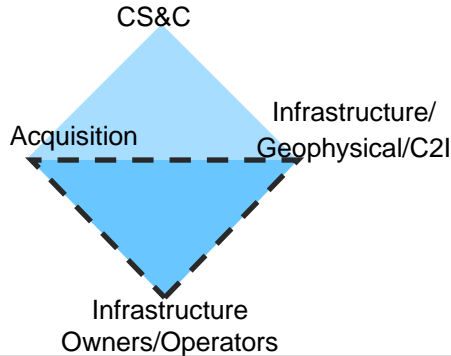
DHS 1st Responder RDT&E
Coordinating Council



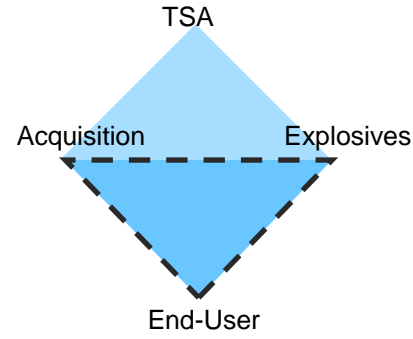
Maritime Security



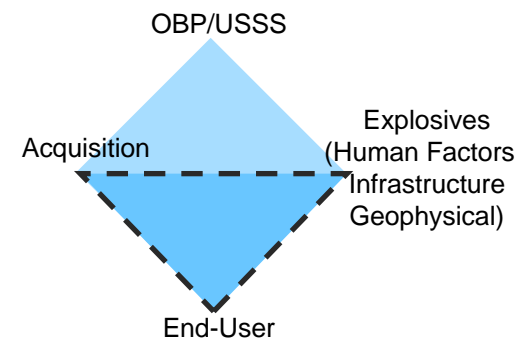
Cyber Security



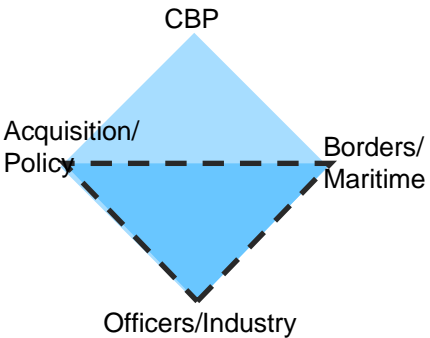
Transportation Security



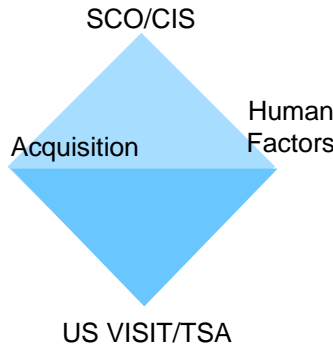
Counter IED



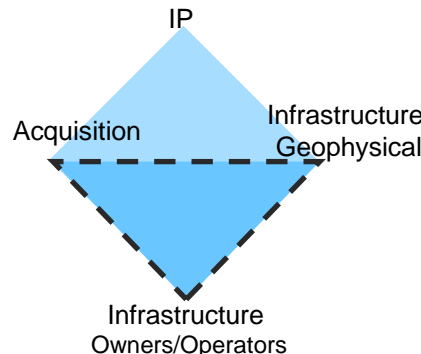
Cargo Security



People Screening

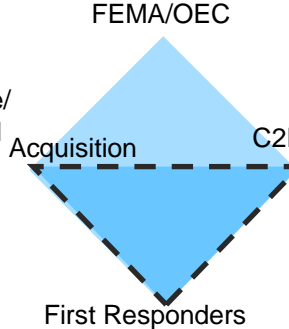


Infrastructure Protection

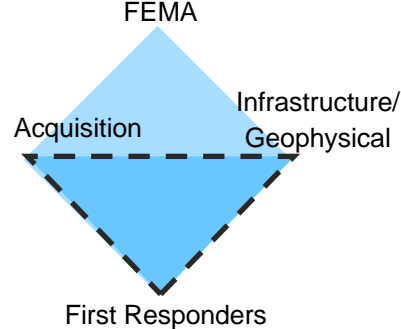


Incident Management

Interoperability



Prep & Response



Cargo Security

Representative Technology Needs



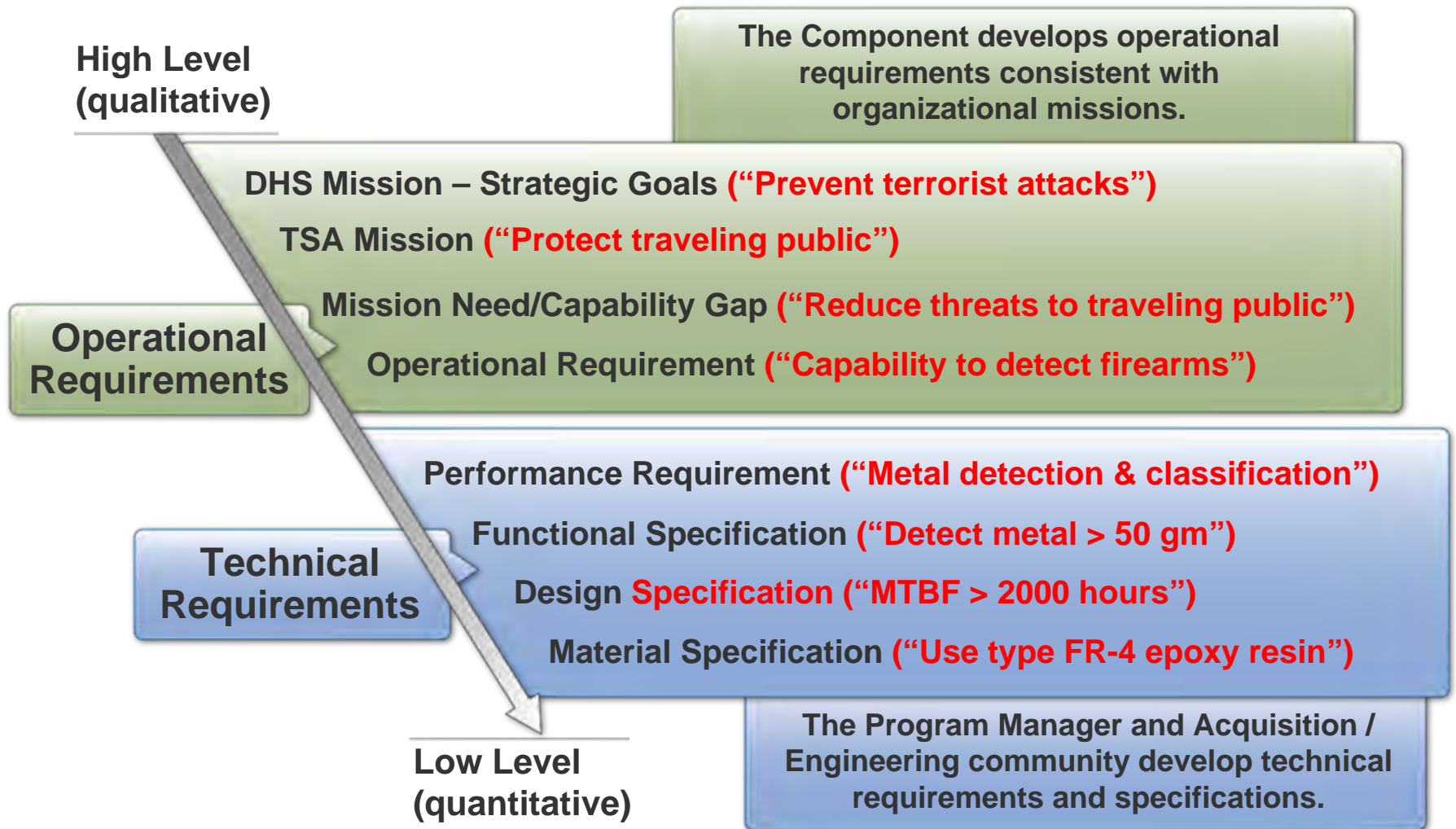
- Enhanced screening and examination by non-intrusive inspection
- Increased information fusion, anomaly detection, Automatic Target Recognition capability
- Detect and identify WMD materials and contraband
- Capability to screen 100% of air cargo
- Test the feasibility of seal security; detection of intrusion
- Track domestic high-threat cargo
- Harden air cargo conveyances and containers
- Positive ID of cargo and detection of intrusion or unauthorized access



Homeland
Security

Source: S&T High Priority Technology Needs, May 2007

Requirements Hierarchy (TSA example)



Each lower-level requirement must be traceable to a higher-level requirement.



Homeland Security

ORD: Operational Requirements Document

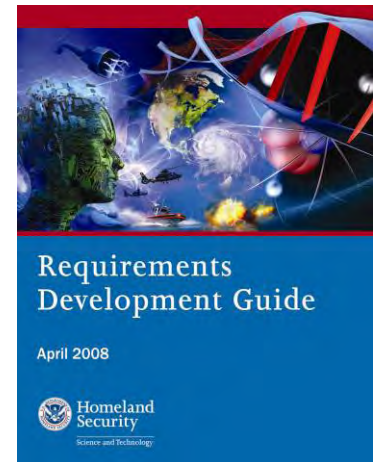
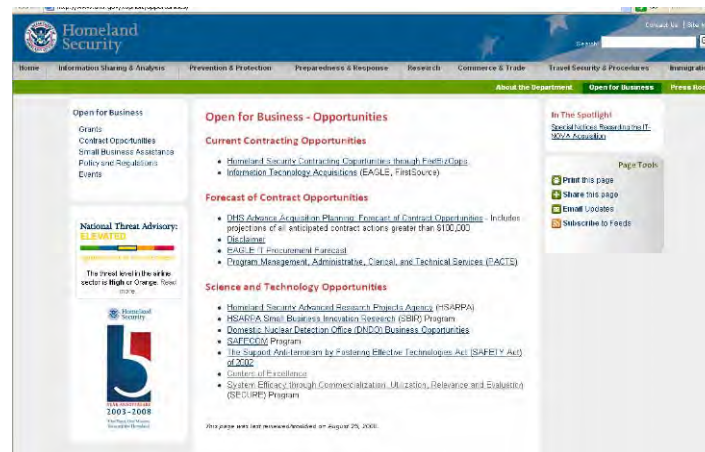
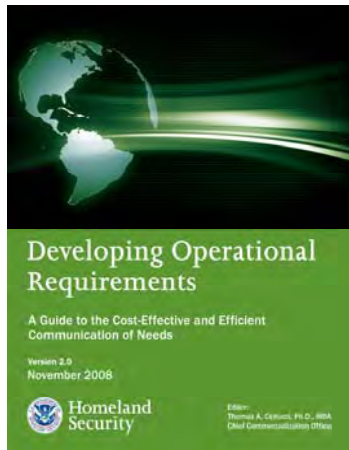
What: ORDs provide a clear definition and articulation of a given problem.

How: Training materials have been developed to assist drafting an ORD.

- *Developing Operational Requirements*, 353pp. Available online: http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf

When: For Use in Acquisition, Procurement, Commercialization and Outreach Programs –Any situation that dictates detailed requirements (e.g. RFQ, BAA, RFP, RFI, etc.)

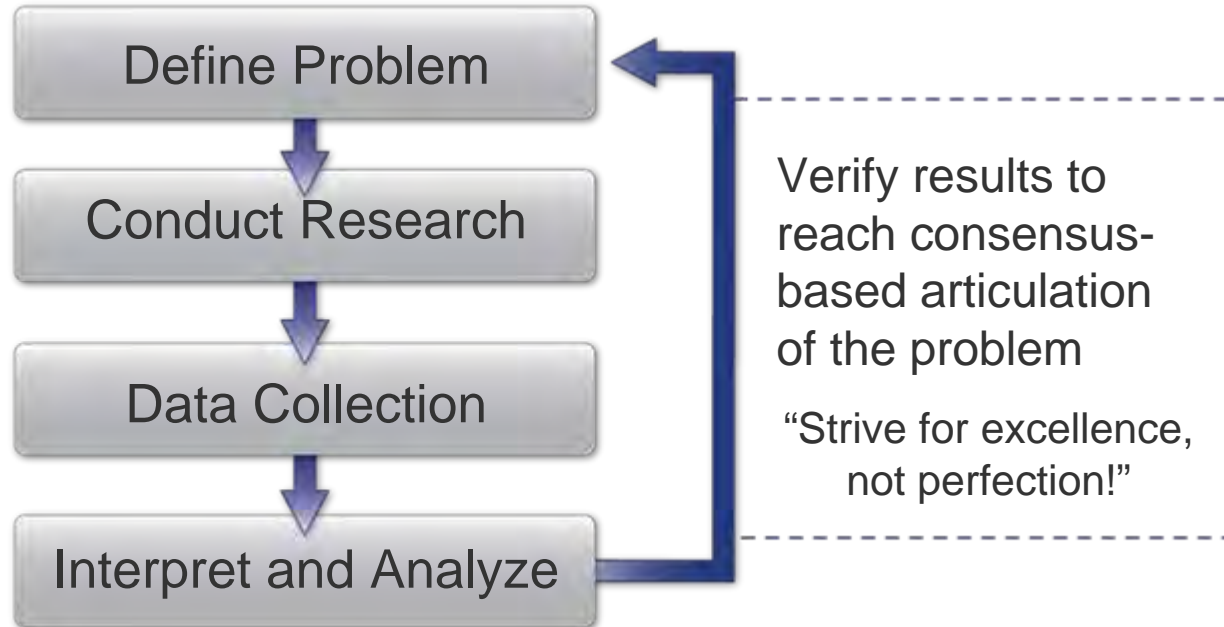
Why: It's cost-effective and efficient for both DHS and all of its stakeholders.



**Homeland
Security**

Generating “Good” ORDs

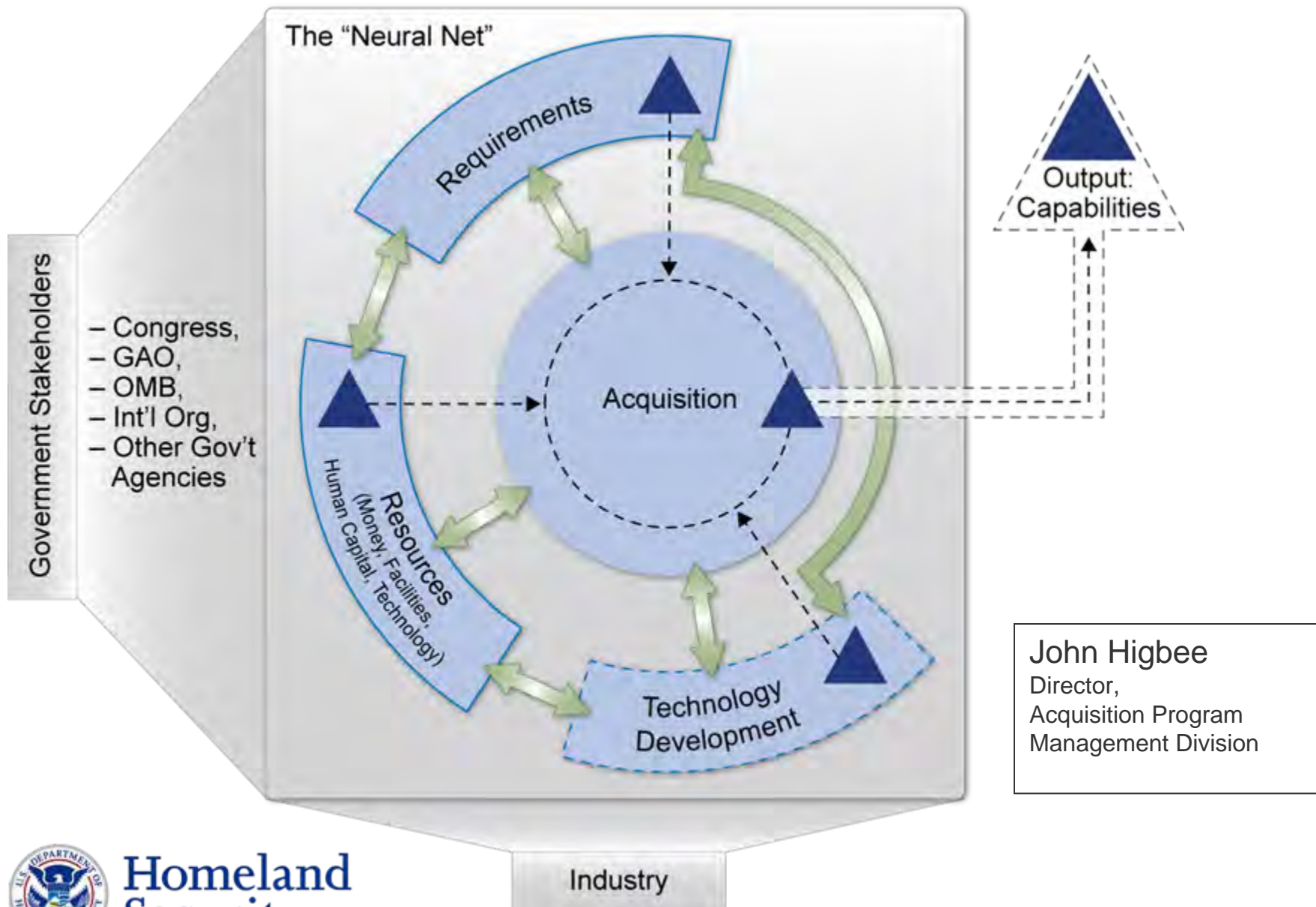
- Solution Agnostic
- Take into account the varying needs and wants of markets/market segments



**Homeland
Security**

Source: Kaufman, et. al.

Interlinking Mechanisms Create Conversations Pipelines



Homeland Security

John Higbee
Director,
Acquisition Program
Management Division

Evolution of Change:

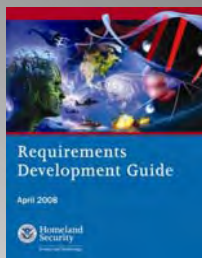
DHS Providing Better Information about its Needs

DoD, DoE, DHS,
DoJ, DoT, etc.

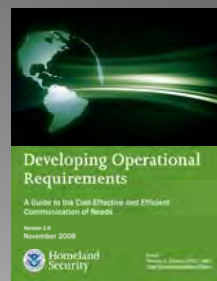
DHS, First Responders, CI/KR
Federal Stakeholders



Capstone
IPT
Process
(August 2006)



*Requirements
Development
Guide (May 2008)*



*Developing
Operational
Requirements
(Nov. 2008)*



*Harnessing the Valuable
Experience and
Resources of the Private
Sector (Feb. 2009)*



Semantic Web 3.0
(The Future)

Industry

Business, Venture Capital/Angel Investment, Strategic Partnerships

Does this look familiar?!



How the customer explained it



How the Project Leader understood it



How the Analyst designed it



How the Programmer wrote it



How the Business Consultant described it



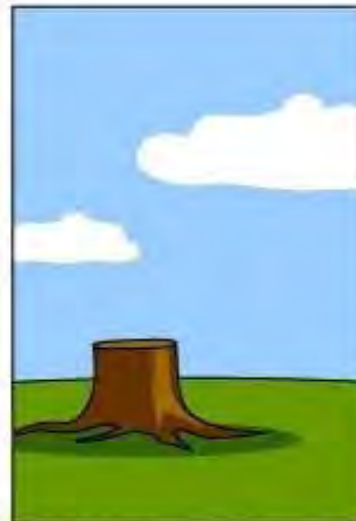
How the project was documented



What operations installed



How the customer was billed



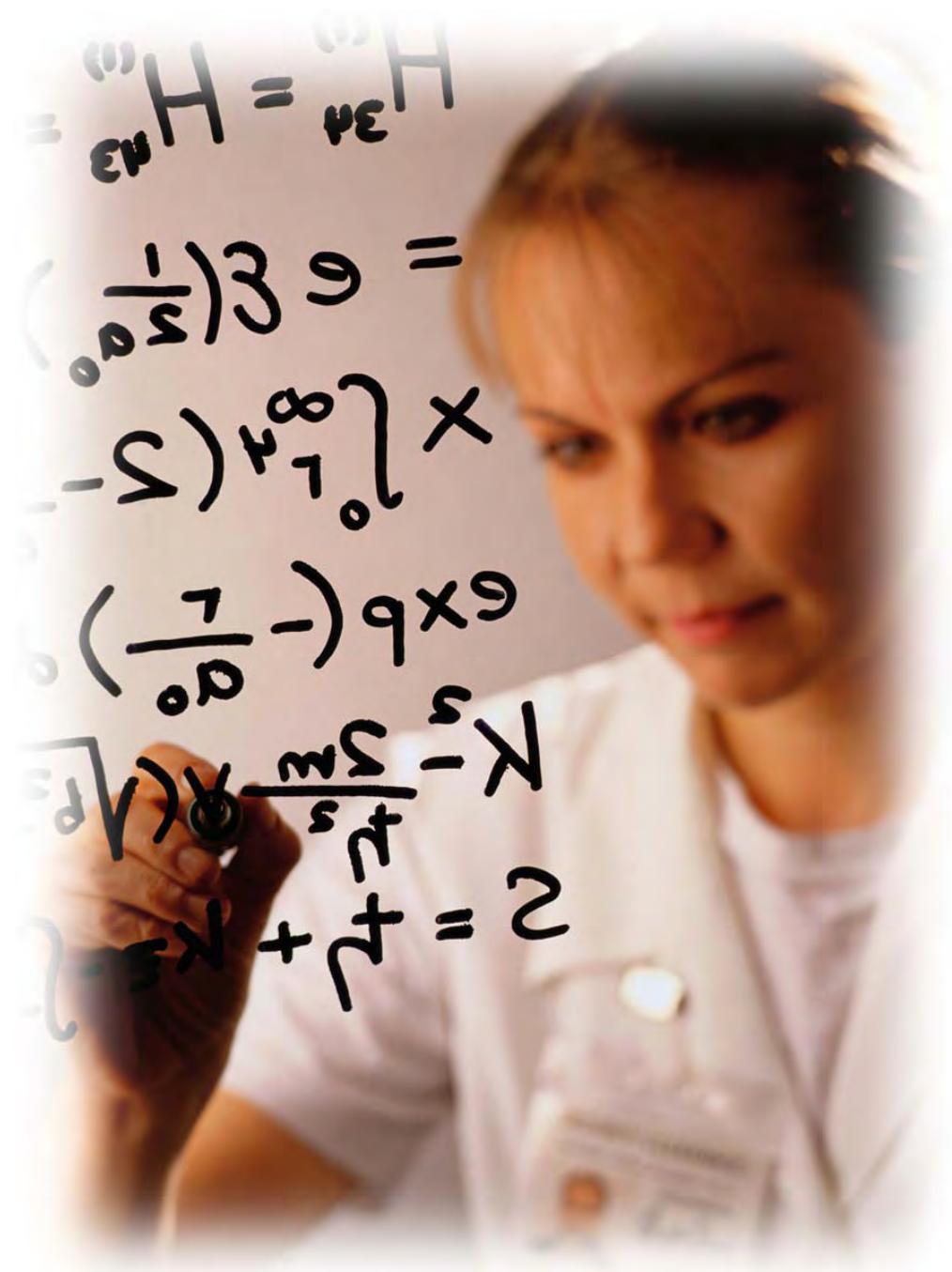
How it was supported



What the customer really needed

Getting on the “Same Page”

- Historical Perspective
- Language is Key
- Communication is Paramount



Homeland
Security

Technology Readiness Levels (TRLs): Overview

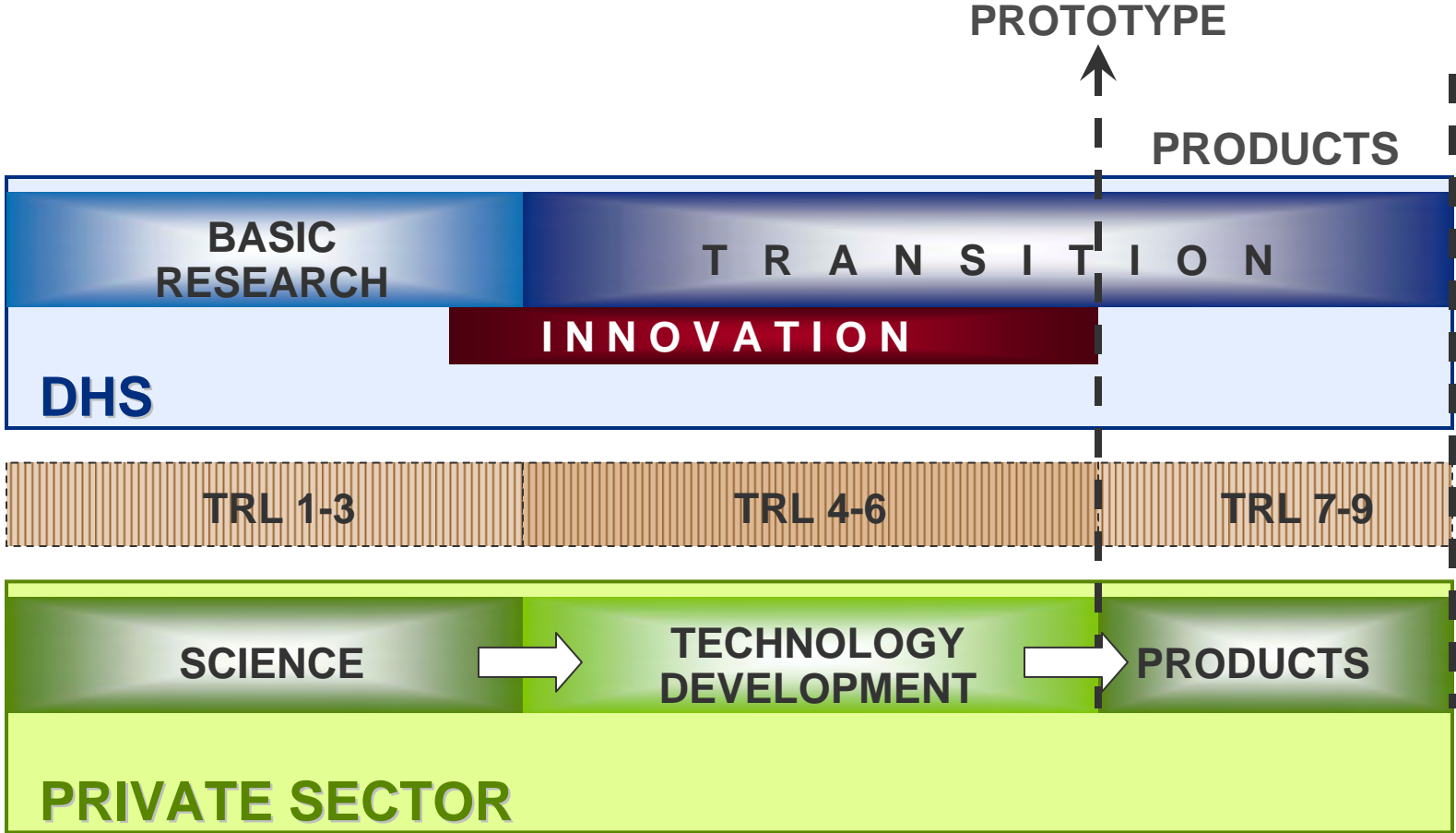
TRLs are NASA-generated and Used Extensively by DoD

Basic principles observed and reported	1	Basic
Technology concept and/or application formulated	2	
Analytical and experimental critical function and/or characteristic	3	
Component and/or breadboard validation in laboratory environment	4	Advanced
Component and/or breadboard validation in relevant environment	5	
System/subsystem model or prototype demonstration in a relevant environment	6	Applied
System prototype demonstration in a operational environment	7	
Actual system completed and 'flight qualified' through test and demonstration	8	
Actual system 'flight proven' through successful mission operations	9	

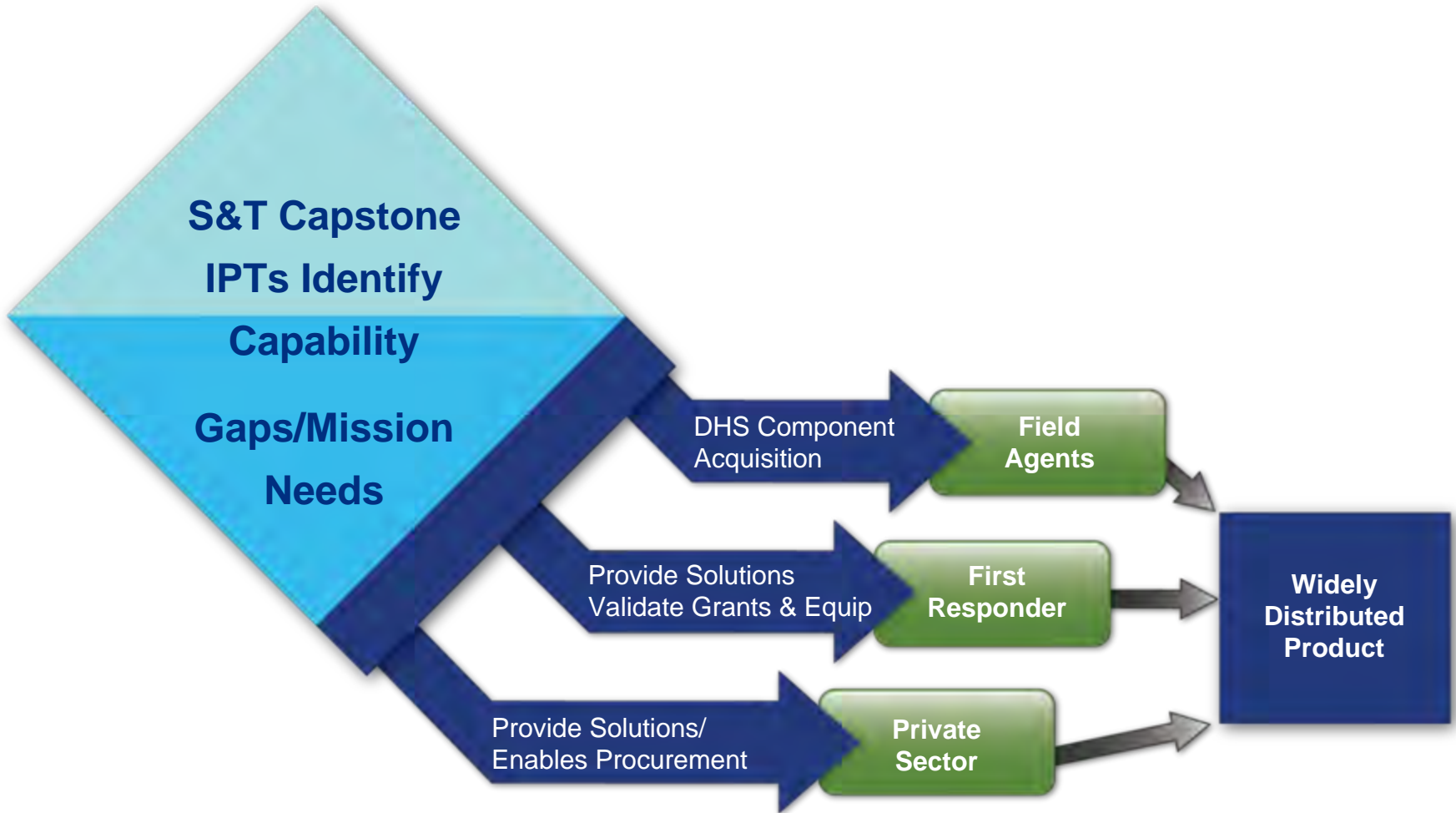


**Homeland
Security**

TRL Correlation: DHS and Private Sector

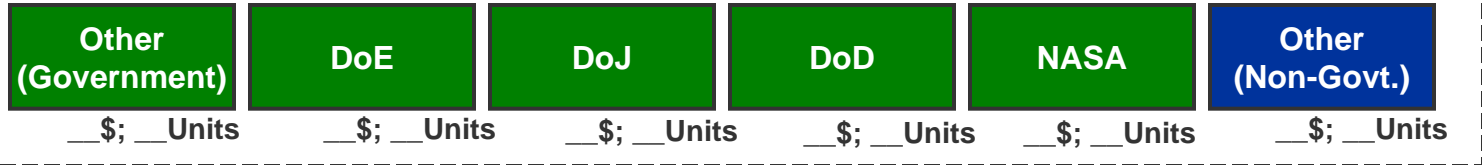


Transition Approaches



**Homeland
Security**

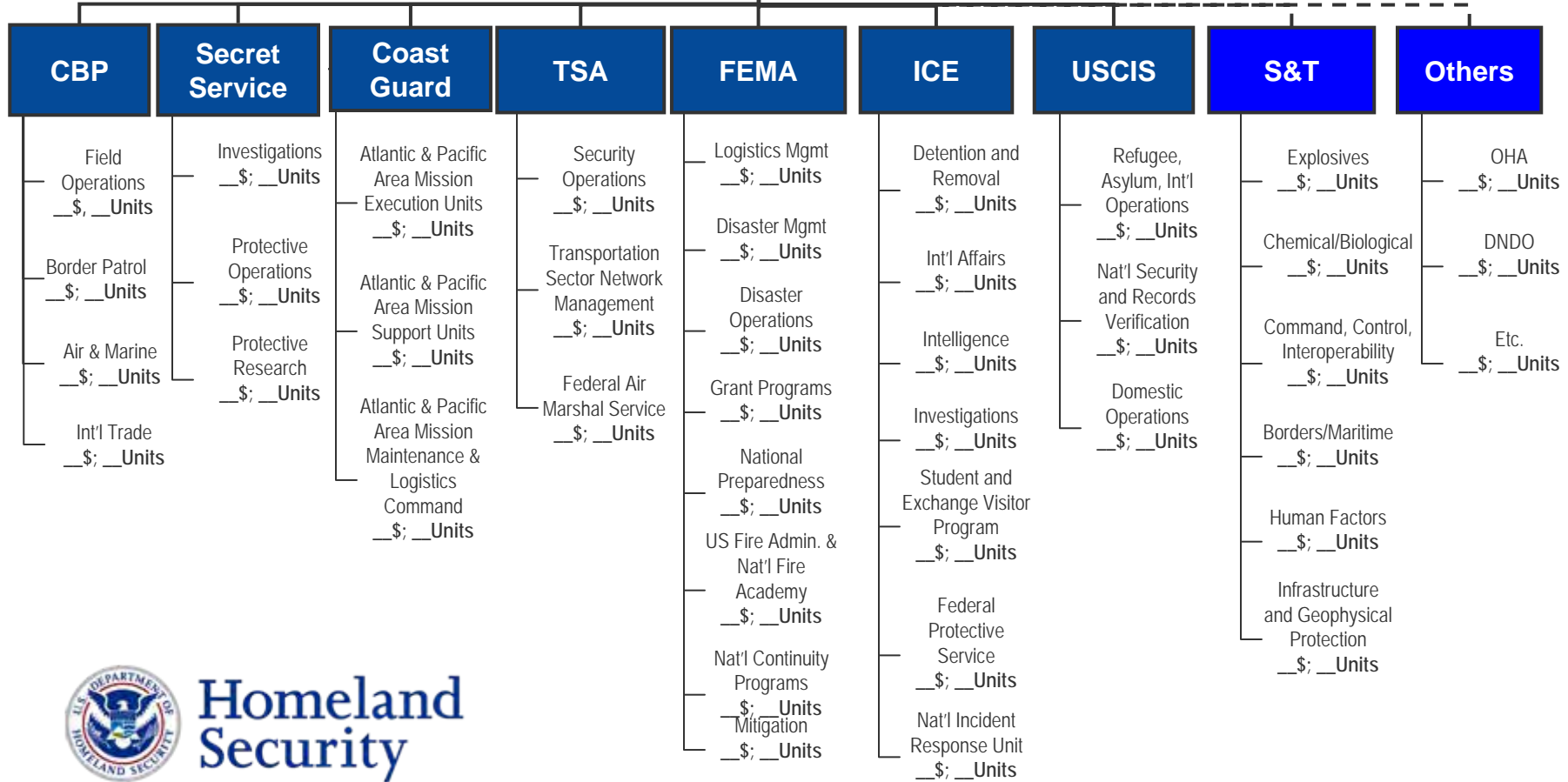
Market Potential Template



DHS

Ancillary Markets

First Responders



Homeland Security

Conservative Estimate: Number of First Responders in the US

- Homeland Security Presidential Directive 8
- Steve Golubic (FEMA)

Total: > 25.3 Million Individuals



FIRE



POLICE



EMT



BOMB
DISPOSAL

Front Line > 2.3 Million

Support to Front Line > 23 Million

Port Security

Public Health

Hospitals

Transportation

Emergency
Management

Clinics

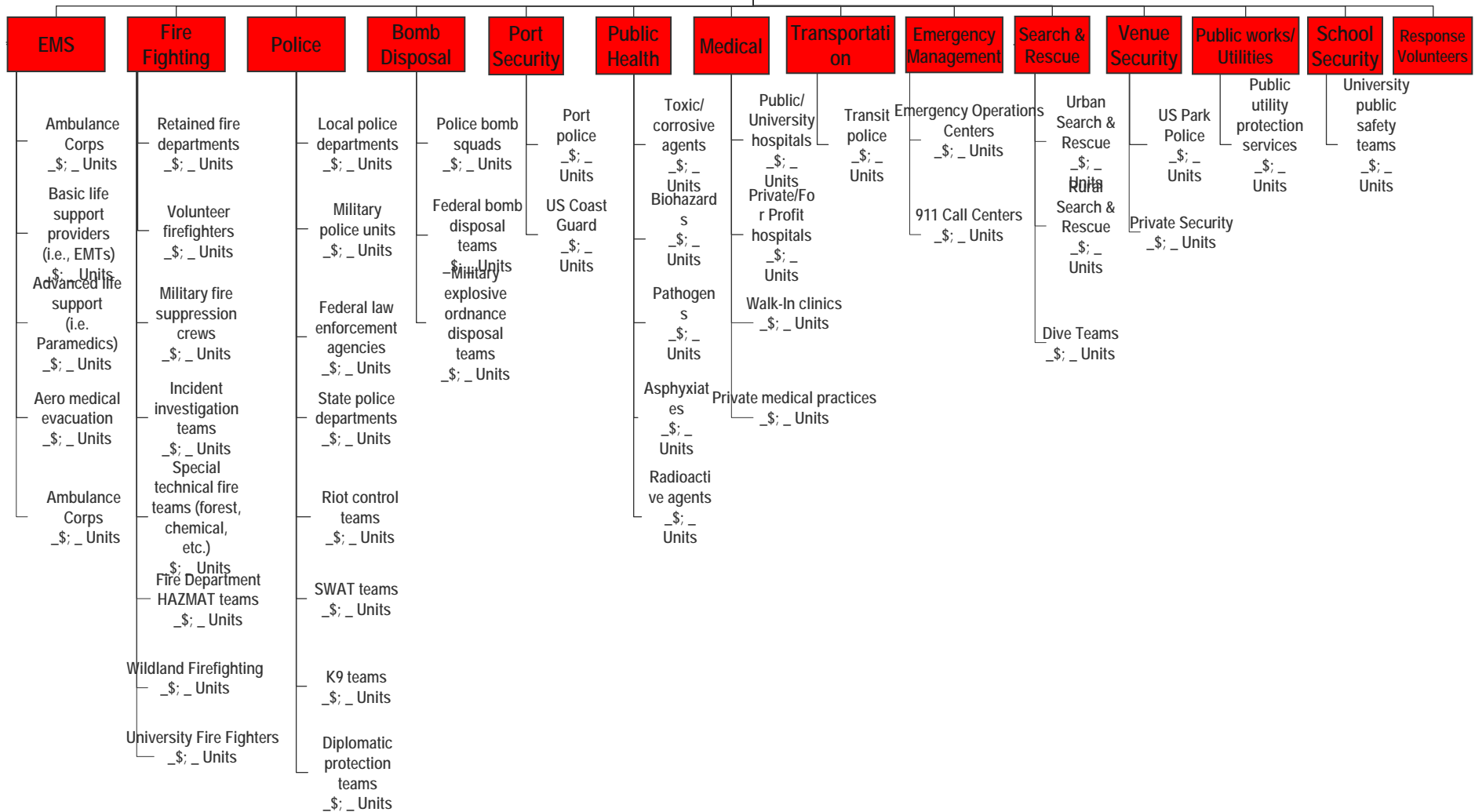
Venue Security

Public
Works/Utility

School Security

Response
Volunteers

First Responders



Homeland Security

Critical Infrastructure Key Resources (CIKR)

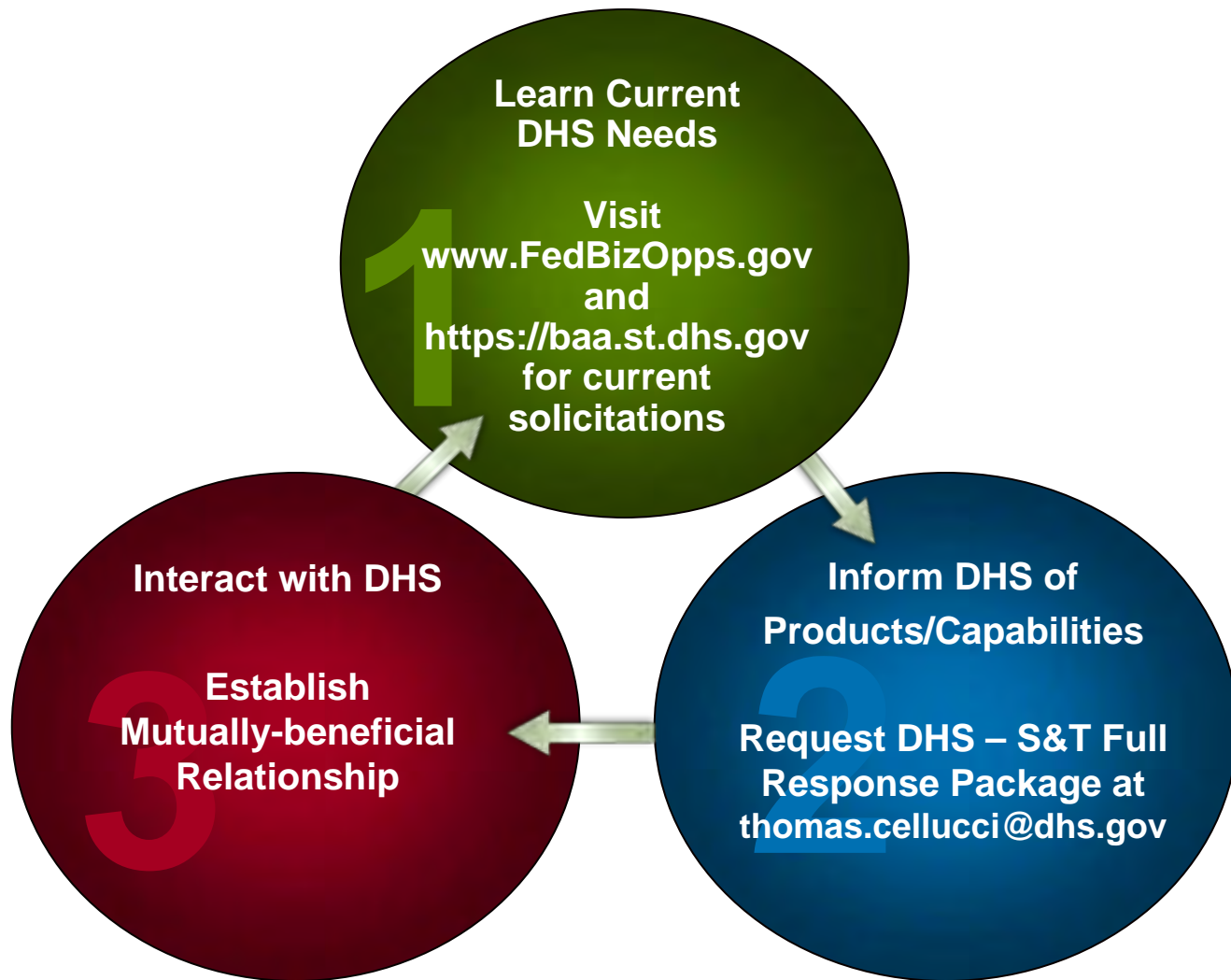
Agriculture and Food	Defense Industrial Base	Energy	Public Health and Healthcare	National Monuments and Icons	Banking and Finance	Water	Chemical	Commercial facilities	Emergency Services	Materials, Reactors and	Telecommunications	Critical Manufacturing	Postal and Shipping Services	Transportation	Information Technology
Food Retail _ \$; _ Units	Defense Contractors _ \$; _ Units	Coal mining operations _ \$; _ Units	Public/University hospitals _ \$; _ Units	Guided tour services _ \$; _ Units	Credit lending institutions _ \$; _ Units	Public utilities _ \$; _ Units	Inorganic chemical production _ \$; _ Units	Hotels _ \$; _ Units	Fire Departments _ \$; _ Units	Electric utilities _ \$; _ Units	Telephone/Cellular services _ \$; _ Units	Iron and Steel mills _ \$; _ Units	United States Postal Service _ \$; _ Units	AMTRAK _ \$; _ Units	Hardware providers _ \$; _ Units
Farm Equipment _ \$; _ Units	Industry analysts _ \$; _ Units	Coal power plants _ \$; _ Units	Private/For Profit hospitals _ \$; _ Units	Travel services _ \$; _ Units	Commercial banking _ \$; _ Units	Desalination plants _ \$; _ Units	Organic industrial production _ \$; _ Units	Shopping centers _ \$; _ Units	Law enforcement agencies _ \$; _ Units	Reactor and associated materials _ \$; _ Units	Satellite data transmission _ \$; _ Units	Aluminum production and processing _ \$; _ Units	High volume document and parcel shipping _ \$; _ Units	Commuter rail _ \$; _ Units	IT Conglomerates _ \$; _ Units
Meat/Poultry Processing _ \$; _ Units	Think tanks/research institutions _ \$; _ Units	Coal equipment manufacturers _ \$; _ Units	Clinics _ \$; _ Units	Lodging/Hotels _ \$; _ Units	Private equity _ \$; _ Units	Treatment plants _ \$; _ Units	Ceramics _ \$; _ Units	Stadiums and sport arenas _ \$; _ Units	Search and rescue teams _ \$; _ Units	University and educational institutions _ \$; _ Units	Broadcasting entities _ \$; _ Units	Nonferrous metal production and processing _ \$; _ Units	Container shipping services _ \$; _ Units	Intracity rail services _ \$; _ Units	Semiconductor production _ \$; _ Units
Food Processing _ \$; _ Units	University partnership programs _ \$; _ Units	Hydroelectric _ \$; _ Units	Private medical practices _ \$; _ Units	Guest services/tourist hospitality _ \$; _ Units	Consumer banking _ \$; _ Units	Equipment manufacturers _ \$; _ Units	Petrochemicals _ \$; _ Units	Schools _ \$; _ Units	Ambulance companies _ \$; _ Units	Control systems _ \$; _ Units	Broadcast equipment manufacturing _ \$; _ Units	Engine, Turbine and Power transmission _ \$; _ Units	Marine shipping _ \$; _ Units	Commercial airline _ \$; _ Units	Electronics manufacture _ \$; _ Units
Dairy Processing _ \$; _ Units	National laboratories _ \$; _ Units	Dam operations _ \$; _ Units	Medical laboratories _ \$; _ Units	People moving services _ \$; _ Units	Building societies/ Private banks _ \$; _ Units	Pipe and water control device manufacturers _ \$; _ Units	Agrochemicals _ \$; _ Units	Commercial office buildings _ \$; _ Units	Mine rescue teams _ \$; _ Units	Other technical rescue teams _ \$; _ Units	Radio equipment manufacturing _ \$; _ Units	Other equipment manufacturing _ \$; _ Units	Trucking industry _ \$; _ Units	Private air services _ \$; _ Units	IT services _ \$; _ Units
Dairy Farms _ \$; _ Units		Wind power _ \$; _ Units	Pharmaceutical _ \$; _ Units	Queueing equipment makers _ \$; _ Units	Merchant banks _ \$; _ Units		Polymers _ \$; _ Units	Museums _ \$; _ Units	Other units _ \$; _ Units	Nuclear safety systems _ \$; _ Units	Internet equipment manufacturing _ \$; _ Units	Electrical Equipment manufacturing _ \$; _ Units	Airborne shipping _ \$; _ Units	Cruise lines _ \$; _ Units	Server and network hardware _ \$; _ Units
Ranching _ \$; _ Units		Solar power _ \$; _ Units	Health insurance _ \$; _ Units	Global financial services firms _ \$; _ Units	Community development institutions _ \$; _ Units		Elastomer production _ \$; _ Units	Zoos and Aquariums _ \$; _ Units	Bomb disposal units _ \$; _ Units	Waste disposal services _ \$; _ Units	High speed data transmission _ \$; _ Units	Motor Vehicle manufacturing _ \$; _ Units	Trucking _ \$; _ Units	Subway systems _ \$; _ Units	Display/digital TV _ \$; _ Units
Organic Farming/Sustainable Agriculture _ \$; _ Units		Public utilities companies _ \$; _ Units	Medical material providers _ \$; _ Units	Private security _ \$; _ Units	Community banks _ \$; _ Units		Oleochemicals _ \$; _ Units	Public Libraries _ \$; _ Units	Blood/Organ transplant supply _ \$; _ Units	Uranium processors _ \$; _ Units	Internet service providers _ \$; _ Units	Aerospace product & parts manufacturing _ \$; _ Units	Airborne shipping _ \$; _ Units	Long-haul maritime shipping _ \$; _ Units	Software production _ \$; _ Units
Traditional Planting _ \$; _ Units		Oil companies _ \$; _ Units	Medical equipment manufacturers _ \$; _ Units		Savings and Loans _ \$; _ Units		Explosives _ \$; _ Units	Amusement parks _ \$; _ Units	Amateur radio emergency comms _ \$; _ Units	Protective garment manufacturers _ \$; _ Units	Print media _ \$; _ Units	Railroad rolling stock _ \$; _ Units	Distribution services _ \$; _ Units	Trucking _ \$; _ Units	Gaming _ \$; _ Units
Commercial fishing _ \$; _ Units			Medical technology manufacturers _ \$; _ Units		Credit unions _ \$; _ Units		Fragrance production _ \$; _ Units		Public utility protection providers _ \$; _ Units	Other _ \$; _ Units	Internet technology providers _ \$; _ Units	Other Transportation equipment _ \$; _ Units	Trucking _ \$; _ Units	Bus services _ \$; _ Units	Information security _ \$; _ Units
			Biotechnology _ \$; _ Units		Insurance companies _ \$; _ Units		Chemical wholesale _ \$; _ Units		Road services _ \$; _ Units				Freight rail service _ \$; _ Units	Automobile travel _ \$; _ Units	Semiconductor equipment _ \$; _ Units
					Insurance brokerages _ \$; _ Units		Exotic chemicals _ \$; _ Units		Emergency Social services _ \$; _ Units				Freight rail service _ \$; _ Units	Roads, Highways, bridges and tunnels _ \$; _ Units	
					Reinsurance companies _ \$; _ Units				Disaster relief _ \$; _ Units						
					Stock brokerages _ \$; _ Units				Famine relief teams _ \$; _ Units						
					Capital market banks _ \$; _ Units				Poison Control units _ \$; _ Units						
					Custody services _ \$; _ Units				Animal control teams _ \$; _ Units						
					Angel investment _ \$; _ Units				Wildlife services _ \$; _ Units						
					Venture capital _ \$; _ Units										



Homeland Security

Call to Action: Mutual Benefits

Create “Win-Win-Win” Relationships



**Homeland
Security**

SECURE™ Program

Developing Solutions in Partnership with the Private Sector

- ‘Win-Win-Win’ Public-Private Partnership program benefits DHS’s stakeholders, private sector and –most importantly- the American Taxpayer
- Saves time and money on product development costs leveraging the free-market system and encouraging the development of widely distributed products for DHS’s stakeholders
- Detailed articulation of requirements (using MD 102-01 ORD template) and T&E review provides assurance to DHS, First Responders and private sector users (like CIKR) that products/services perform as prescribed



http://www.dhs.gov/xres/programs/gc_1211996620526.shtm

SECURE™ Program

Concept of Operations

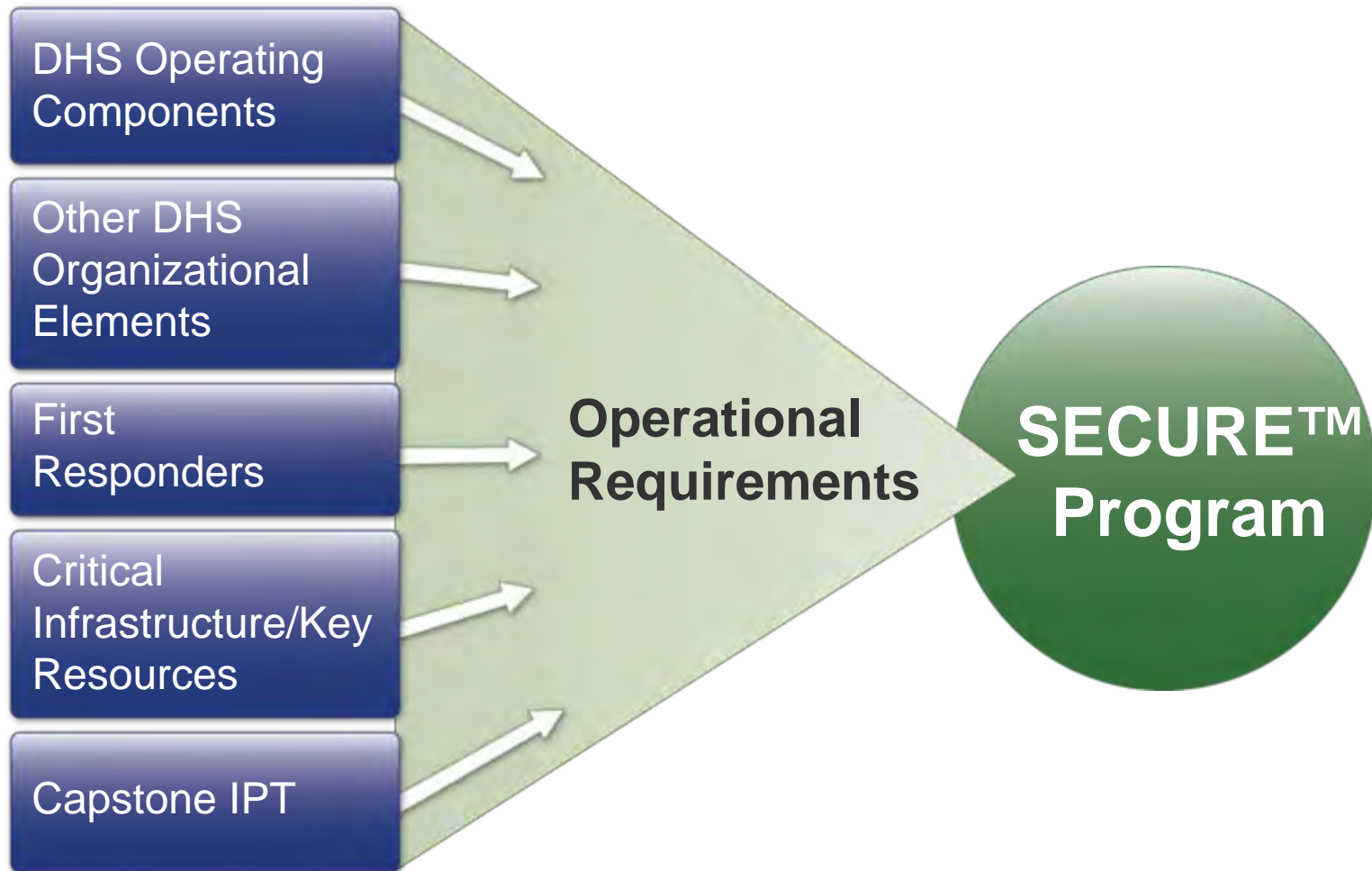


- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored on internal DHS metrics
- Agreement – One-page streamlined CRADA document. Outlines milestones and exit criteria
- Publication of Results – Independent Third-Party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal

Benefits:

- Successful products/technologies share in the imprimatur of DHS
- DHS Operating Components and First Responders make informed decisions on products/technologies aligned to their stated requirements
- DHS spends less on acquisition programs → Taxpayers win.

Multiple Sources of ORDs for SECURE™



Why SECURE™ Program

▪ **Multi-Use**

- Provides private sector, in an open and transparent way, with what they need most—Business Opportunities
- Provides assurance to DHS, First Responders and private sector users (like CI/KR) that products/services perform as prescribed (and provides vehicle for First Responders, CI/KR owners and operators to voice their requirements)
- Augments the value of the SAFETY Act

▪ **Saves Money**

- Private Sector uses its own resources to develop products and services to the benefit of the taxpayer and the Federal Government

▪ **Creates Jobs**

- Detailed articulation of requirements coupled with funded large, potential available markets yield OPPORTUNITY that yields Job Creation (it's better to teach a person to fish than to give them a fish)
- Enables small firms with innovative technologies to partner with larger firms, VCs and angel investors because of the credibility of having government show detailed requirements with associated market potential (instead of just their own business plans).

▪ **Efficient Use of Government Funds**

- Articulating detailed requirements saves time and money. It is better for Government to spend funds to procure products or services that are available for sale and rigorously tested compared to spending money and time to develop new solutions for ill-defined problems.



**Homeland
Security**

SECURE™ Program

Benefit Analysis “Win-Win-Win”

Taxpayers	Private Sector	Public Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Save significant time and money on market and business development activities	1. Improved understanding and communication of needs
2. Tax savings realized through Private Sector investment in DHS	2. Firms can genuinely contribute to the security of the Nation	2. Cost-effective and rapid product development process saves resources
3. Positive economic growth for American economy	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work	3. Monies can be allocated to perform greater number of essential tasks
4. Possible product “spin-offs” can aid other commercial markets	4. Significant business opportunities with sizeable DHS and DHS ancillary markets	4. End users receive products aligned to specific needs
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. Commercialization opportunities for small, medium and large business	5. End users can make informed purchasing decisions with tight budgets



FutureTECH™ Program

Addressing the Future Needs of DHS

- ‘Win-Win-Win’ Public-Private Partnership program benefits DHS stakeholders, private sector and –most importantly- the American Taxpayer
- 5W template provides detailed overview of Critical Research/Innovation Focus Areas
- Critical Research/Innovation Focus Areas provide universities, national labs and private sector R&D organizations insight into the future needs of DHS stakeholders
- Partnership program encourages R&D organizations to work on development of technology solutions up to TRL-6 to address long-term DHS needs.



http://www.dhs.gov/xres/programs/gc_1242058794349.shtm

FutureTECH™ Program

Concept of Operations



- Expression of Interest – Seeking technologies aligned with posted DHS Critical Research and Innovation Focus Areas
- Acceptance–Technologies TRL-6 or below, scored on internal DHS metrics
- CRADA– One-page CRADA document. Outlines milestones and exit criteria
- Publication of Results – Independent Third-Party T&E conducted on TRL-6 technology. Results verified by DHS, posted on DHS web-portal

Benefits:

- Insight into future needs of DHS Stakeholders
- Increased speed-of-execution of technology development and transition
- DHS spends less on technology development → Taxpayers win.



**Homeland
Security**

FutureTECH™ Program

Critical Research & Innovation Focus Areas

- Improvised Explosive Devices Detect & Defeat Countermeasures:
 - Waterborne IEDs
 - Vehicle Borne IEDs
 - Radio Controlled IEDs
 - Person Borne IEDs
 - IED Assessment and Diagnostics
 - IED Access and Defeat
 - Homemade Explosives
- IED Threat Characterization
- IED Mitigation: Alert/Warning System
- IED Deter and Predict: Network Attack and Analysis



**Homeland
Security**



Anyelina
Immigration Information
Officer, USCIS



Home Counterterrorism Border Security Preparedness, Response, Recovery Immigration Unified DHS About

I Want to

- Contract with the Department
- Find small business resources
- Find contracting opportunities
- Register to do business with the Department



Open for Business

Open for Business

Contracting Opportunities

- [Contracting with the Department of Homeland Security](#)
- [Advance Acquisition Planning: Forecast of Contract Opportunities](#)
- [Homeland Security Contracting Opportunities through FedBizOpps](#)
- [More Contracting Opportunities »](#)

Small Business

- [Prime Contractors](#)
- [Mentor-Protégé Program](#)
- [Connect with Small Business Specialists in the Department](#)
- [More Small Business »](#)

Events

- [Vendor Outreach Sessions](#)
- [Office of Small and Disadvantaged Business Utilization Conferences](#)

Policy and Regulations

- [Homeland Security Acquisition Regulation \(HSAR\)](#)
- [Forms](#)
- [Reports and Notices](#)
- [More Acquisition Policies and Regulations »](#)

Grants

- [State Contacts and Grant Award Information](#)
- [FEMA Grants and Assistance Programs](#)
- [Transportation Security Administration Grant Programs](#)
- [More Grants >>](#)

Resources

- [Support Anti-terrorism by Fostering Effective Technologies \(SAFETY\) Act](#)
- [System Efficacy through Commercialization, Utilization, Relevance and Evaluation \(SECURE\)](#)
- [E-Verify, the employee eligibility program](#)

Homeland Security Components

- Directorate for Management
- Private Sector Office

Page Tools

- Print this page
- Share this page
- Feedback
- Help

SECURE Program

More from Homeland Security

- [Economic Recovery Act of 2009](#)
- [E-Verify Designated as Employment Eligibility Verification](#)
- [E-Verify](#)
- [Links for Businesses](#)
- [Office of Multimedia](#)
- [Exhibit 300: Capital Asset Plan and Business Case Summaries](#)
- [Rights-of-Way Permission for Telecommunications Projects](#)

Federal Business Opportunities

Sites where the Office of Procurement Operations (OPO) posts opportunities for prospective suppliers to offer solutions to DHS – S&T's needs:

- www.FedBizOpps.gov
- <https://baa.st.dhs.gov/>
- <https://www.sbir.dhs.gov/>
- www.Grants.gov

take advantage of...

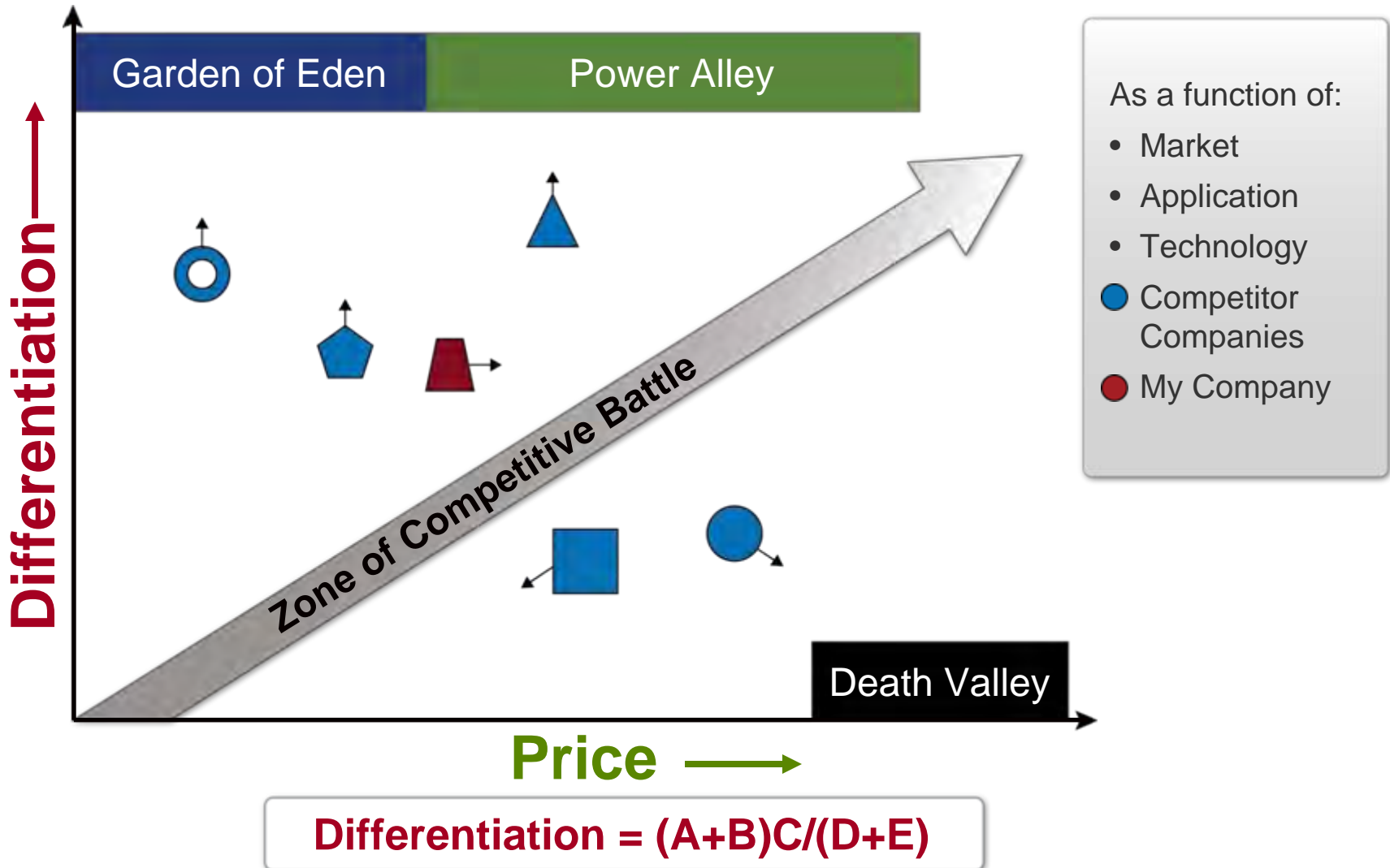
- **Vendor Notification Service:** Sign up to receive procurement announcements and solicitations/BAA amendment releases, and general procurement announcements.
<http://www.fedbizopps.gov>
- **S&T's Solicitation Portal:** The Department of Homeland Security Science and Technology Directorate currently has several active Solicitations on a broad range of topics. Relevant information is posted and access to the teaming portal, conference registration and white paper/proposal registration and submission is provided, as applicable. In addition, historical information about past Solicitations and Workshops is maintained.
<https://baa.st.dhs.gov>
- **Truly Innovative and Unique Solution:** Refer to Part 15.6 of the Federal Acquisition Regulation (FAR) which provides specific criteria that must be met before a unsolicited proposal can be submitted to Diane Osterhus.
http://www.acquisition.gov/far/current/html/Subpart%2015_6.html
- **EAGLE Contract** will serve as a department-wide platform for acquiring IT service solutions.
http://www.dhs.gov/xopnbiz/opportunities/editorial_0700.shtm

Contact Information:

Diane Osterhus
Department of Homeland Security
Office of the Chief Procurement Officer
245 Murray Dr., Bldg. 410
Washington, DC 20528
unsolicited.proposal@dhs.gov
202-447-5576

Show Us the Difference...

Hall's Competitive Model





More Opportunities with DHS Science and Technology

SAFETY Act

Support Anti-Terrorism by Fostering Effective Technologies Act of 2002

- Enables the development and deployment of qualified anti-terrorism technologies
- Provides important legal liability protections for manufacturers and sellers of effective technologies
- Removes barriers to industry investments in new and unique technologies
- Creates market incentives for industry to invest in measures to enhance our homeland security
- The SAFETY Act liability protections apply to a vast range of technologies, including:
 - Products
 - Services
 - Software and other forms of intellectual property (IP)

Examples of eligible technologies:

- Threat and vulnerability assessment services
- Detection Systems
- Blast Mitigation Materials
- Screening Services
- Sensors and Sensor Integration
- Vaccines
- Metal Detectors
- Decision Support Software
- Security Services
- Data Mining Software

Protecting You, Protecting U.S.

Additional SAFETY Act information...

Online: www.safetyact.gov Email: helpdesk@safetyact.gov Toll-Free: 1-866-788-9318

Long Range Broad Agency

Announcement

(Contact: Adrian.Groth@hq.dhs.gov | <https://baa.st.dhs.gov/>)

- Peer or scientific review of proposals in Basic Research and Applied Technology in science and engineering.
- Research to promote revolutionary changes in technologies; advance the development, testing, and deployment of security technologies; and to accelerate the prototyping and deployment of technologies.
- Streamlined and flexible funding mechanism. Open to all DHS-relevant ideas, no submission deadlines, no ceiling on potential funding.
- Public Solicitation identifies science and technology target areas as does the S&T publication “High Priority Technology Needs” dated May 2009, as amended. This document may be obtained by accessing <https://baa.st.dhs.gov> and by following the link for “*Representative High Priority Technology Needs*”.

*** Peer or Scientific Reviews ***

*** Basic or Applied Research ***

*** Maximum Flexibility: Schedules, Subjects, Funding ***



**Homeland
Security**

Technology Transfer

Transfer federally owned/originated technology to State and local governments and the private sector, ensuring the widest dissemination and impact of Federal research investments.

DOD 1401 Program Liaison

- Push DHS requirements to DOD
- Pull DOD technologies into DHS for first responders
- Assess technology suitability and adaptations for DHS applications
- Create DHS & DoD Program Manager partnerships to maximize technology enhancements for our nation's first responders



Office of Research and Technology Applications (ORTA)

- Manage all technology transfer mechanisms used in DHS
 - Cooperative Research and Development Agreements (CRADAs)
 - Licensing Agreements
 - Other Transaction Agreements (OTAs)
 - Commercial Test Agreements
 - Work for Others
 - Partnership Intermediaries
- Capture Intellectual Property and licensing in DHS
- Assess R&D projects for potential commercial applications
- Train engineers and scientists for Technology Transfer and Intellectual Property
- Represent DHS in the Federal Laboratory Consortium



Homeland Security

Contact: Marlene Owens, Marlene.Owens@dhs.gov

https://www.sbir.dhs.gov

- SBIR Home
- News and Events
- Solicitation Deadlines
- Proposal Submission
- SBIR Solicitations
- Awards
- Awardee Portal
- SBIR Contact Information
- FAQ
- Links
- Topic Recommendations
- Presentations
- Site Search
- Privacy Policy
- Mailing List



[Homeland Security](#) | [Science & Technology](#) | [HSARPA BAA](#) | [OSDBU](#) | [SBA](#) | [SAFETY Act](#) | [Contact Us](#) | [Privacy Policy](#) | [Join HSARPA Mailing List](#)

The DHS S&T SBIR FY08.2 solicitation closed on July 8, 2008.

**Department of Homeland Security
Science and Technology Directorate (S & T Directorate)
Small Business Innovation Research (SBIR) Program**

The DHS S&T SBIR Program was initiated in 2004. For the DHS S&T SBIR Program, two solicitations are issued per year. Generally, they will be issued in November and May.

Solicitation topics are developed by Program Managers in each of the Science and Technology (S&T) Divisions, and from time to time, by the Offices of Innovation and Basic Research. The annual solicitations consist of topics that are relevant to the Chemical and Biological, Borders and Maritime Security, Human Factors, Explosives, Infrastructure and Geophysical, and Command, Control and Interoperability Divisions.

Similar to the R&D programs of the S&T Directorate, the SBIR topics generally address the needs of the seven DHS Operational Units, i.e., U.S. Coast Guard, U.S. Transportation Security Administration, U.S. Customs and Border Protection, Federal Emergency Management Agency, U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, and U.S. Secret Service, as well as First Responders.

For the Phase II SBIR effort, the DHS S&T SBIR Program has a Cost Match feature for SBIR projects that attract matching cash from an outside investor. The purpose is to focus SBIR funding on those projects that are most likely to be developed into viable new products that DHS and others will buy and that will thereby make a major contribution to homeland security and/or economic capabilities. Click here for more information about the [Cost Match feature](#).

The DHS S&T SBIR Program has several processes in place to accelerate the Phase I and Phase II award process to further satisfy operational requirements and commercial application.

- Phase I awards are typically made within 90 days of selection.
- Invited Phase II projects will be reviewed and awards will be made incrementally, as quickly as possible under the Jump Start feature, to maintain the momentum of the Phase I effort. The Phase II proposal invitation process expeditiously identifies those Phase I awardees deserving of Phase II awards.

To learn more about the SBIR Program, please visit <http://www.sba.gov/SBIR/indexsbir-sttr.html>.

[Click Here to Print](#)

WARNINGWARNING**WARNING**

Safety Act

Other Funding Opportunities

Topic Recommendations



TechSolutions

The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders

- Field prototypical solutions in 12 months
- Cost should be commensurate with proposal but less than \$1M per project
- Solution should meet 80% of identified requirements
- Provide a mechanism for Emergency Responders to relay their capability gaps
 - Capability gaps are gathered using a web site (www.dhs.gov/techsolutions)
- Gaps are addressed using existing technology, spiral development, and rapid prototyping
- Emergency Responders partner with DHS from start to finish

Rapid Technology Development

Target: Solutions Fielded within 1 year, at <\$1M



**Homeland
Security**

Getting Involved: S&T Contacts

Division	Email
Jim Tuttle	SandT.Explosives@dhs.gov
Beth George	SandT.ChemBio@dhs.gov
David Boyd	SandT.CCI@dhs.gov
Anh Duong	SandT.BordersMaritime@dhs.gov
Sharla Rausch	SandT.HFD@dhs.gov
Chris Doyle	SandT.IGD@dhs.gov
Rich Kikla	SandT.Transition@dhs.gov
Starnes Walker	SandT.Research@dhs.gov
Roger McGinnis	SandT.Innovation@dhs.gov



Homeland
Security

Summary

Detailed Requirements

Sizeable Market Potential

Delivered Products – PERIOD!

How Can You Afford NOT to Partner with DHS?

Questions/Comments:

Thomas A. Cellucci, Ph.D., MBA

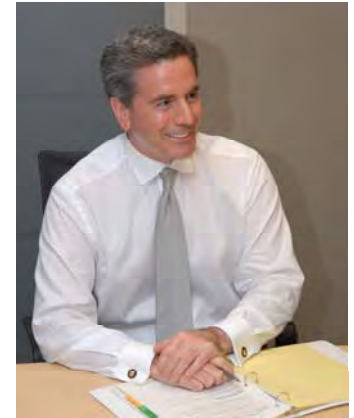
SandT_Commercialization@dhs.gov



**Homeland
Security**

U.S. Department of Homeland Security: Science and Technology Directorate's Chief Commercialization Officer

Dr. Cellucci accepted a five-year appointment from the Department of Homeland Security in August 2007 as the Federal Government's first Chief Commercialization Officer (CCO). He is responsible for initiatives that identify, evaluate and commercialize technology for the specific goal of rapidly developing and deploying products and services that meet the specific operational requirements of the Department of Homeland Security's Operating Components and other DHS stakeholders such as First Responders and Critical Infrastructure/Key Resources owners and operators. Cellucci has also developed and continues to drive the implementation of DHS-S&T's outreach with the private sector to establish and foster mutually beneficial working relationships to facilitate cost-effective and efficient product/service development efforts. His efforts led to the establishment of the DHS-S&T Commercialization Office in October 2008. The Commercialization Office is responsible for four major activities; a requirements development initiative for all DHS stakeholders, the development and implementation of a commercialization process for DHS, development and execution of private sector partnership programs such as SECURE and leading the private sector outreach for the S&T directorate.



Since his appointment, he has published three comprehensive guides [*Requirements Development Guide* (April 2008), *Developing Operational Requirements* (May 2008), and *Developing Operational Requirements, Version 2* (November 2008)] dealing with the development of operational requirements, developed and implemented a commercialization model for the entire department and established the SECURE Program—an innovative public-private partnership to cost-effectively and efficiently develop products and services for DHS's Operating Components and other DHS stakeholders. In addition, he has written over 25 articles and a compilation of works [*Harnessing the Valuable Experiences and Resources of the Private Sector for the Public Good*, (February 2009)] geared toward the private sector to inform the public of new opportunities and ways to work with DHS. Cellucci has received recognition for his outreach efforts and engagement with the small and disadvantaged business communities who learn about potential business opportunities and avenues to provide DHS with critical technologies and products to help secure America. Cellucci is an accomplished entrepreneur, seasoned senior executive and Board member possessing extensive corporate and VC experience across a number of worldwide industries. Profitably growing high technology firms at the start-up, mid-range and large corporate level has been his trademark. He has authored or co-authored over 139 articles on Requirements development, Commercialization, Nanotechnology, Laser physics, Photonics, Environmental disturbance control, MEMS test and measurement, and Mistake-proofing enterprise software. He has also held the rank of Lecturer or Professor at institutions like Princeton University, University of Pennsylvania and Camden Community College. Cellucci also co-authored ANSI Standard Z136.5 "The Safe Use of Lasers in Educational Institutions". Dr. Cellucci is also a commissioned Admiral and Commander of a Squadron in Texas responsible for civil defense and has been a first responder for over twenty years. As a result of his consistent achievement in the commercialization of technologies, Cellucci has received numerous awards and citations from industry, government and business. In addition, he has significant experience interacting with high ranking members of the United States government—including the White House, US Senate and US House of Representatives—having provided executive briefs to three Presidents of the United States and ranking members of Congress. Cellucci represents DHS as the first Federal Government member on the U.S. Council on Competitiveness.

Cellucci earned a PhD in Physical Chemistry from the University of Pennsylvania, an MBA from Rutgers University and a BS in Chemistry from Fordham University. He has also attended and lectured at executive programs at the Harvard Business School, MIT Sloan School, Kellogg School and others. Dr. Cellucci is regarded as an authority in rapid time-to-market new product development and is regularly asked to serve as keynote speaker at both business and technical events.



Homeland Security

Commercialization Office: Providing Value through Efficiency and Cost-Effectiveness



June 2010

Thomas A. Cellucci, Ph.D., MBA

Chief Commercialization Officer
U.S. Department of Homeland Security

Email: SandT_Commercialization@dhs.gov

Website: <http://bit.ly/commercializationresources>

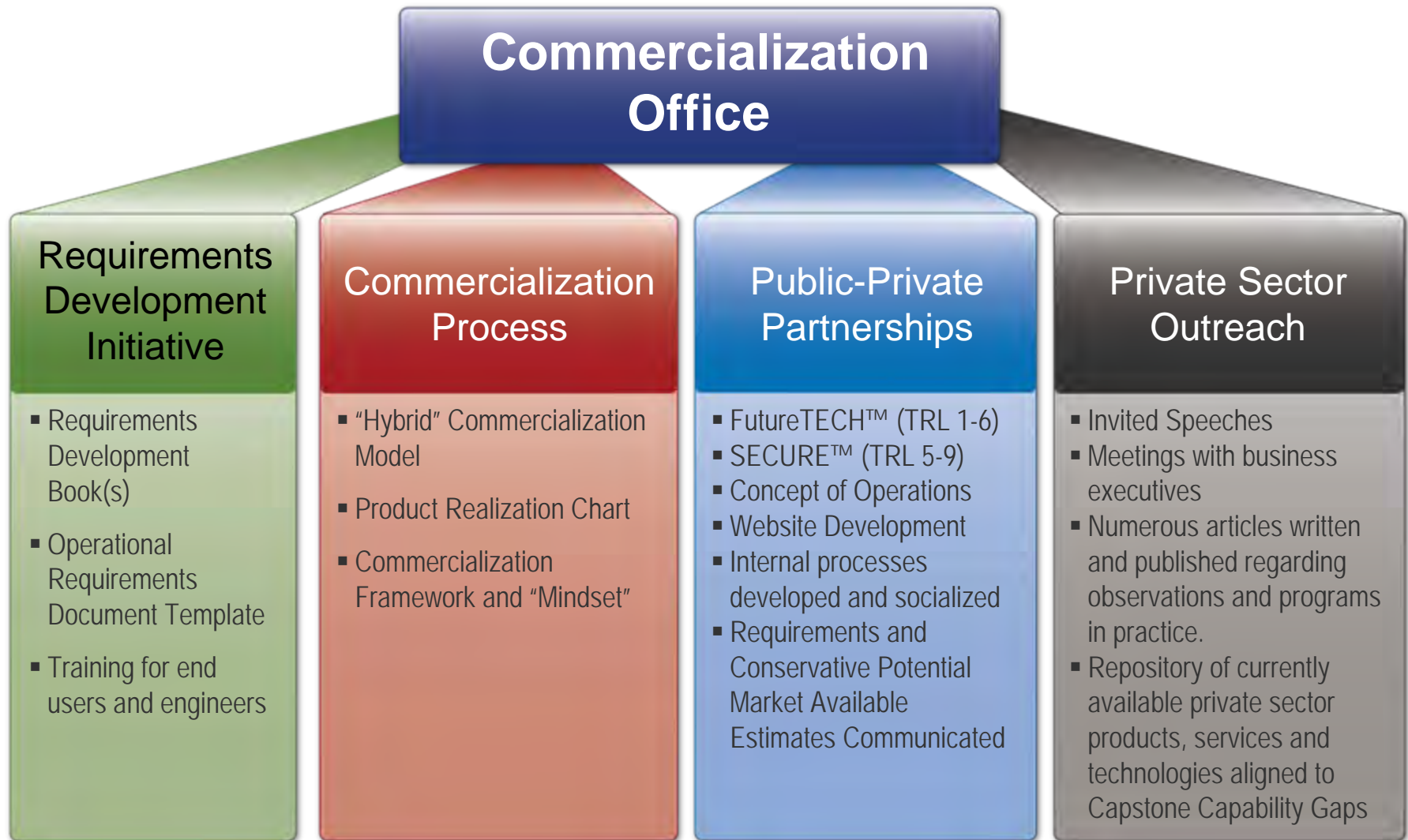
Discussion Guide

- Commercialization Office Initiatives at DHS
- New Commercialization Process
- Outreach Efforts
- SECURE Program
- Benefits for Taxpayers, DHS and Private Sector



Homeland
Security

Commercialization Office: Major Activities



**Homeland
Security**

[http://www.dhs.gov/xabout/structure/
gc_1234194479267.shtm](http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm)

Why a Commercialization Office?: Creating and Demonstrating Value

S&T Commercialization Office -- Four Major Activities

Parameter	Requirements Development Initiative	Commercialization Process	SECURE Program	S&T Private Sector Outreach
1) Increases speed-of-execution of DHS programs/projects	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2) DHS and its stakeholders receive products more closely aligned to specific requirements/needs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3) Increases effective and efficient communication	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4) End users can make informed purchasing decisions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5) Large savings of cost and time for DHS and its stakeholders	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6) Increases goodwill between taxpayers, private sector and DHS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7) Fosters more opportunities for small, medium and large businesses	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8) Large taxpayer savings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9) Possible product "spin-offs" can aid other commercial markets	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10) Promotes open and fair competition	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



Homeland Security

Return-on-DHS Investment is LARGE!

Two Models for Product Realization

Big-A Acquisition

1. Requirements derived by Government
2. RFP and then cost-plus contract(s) with developer(s) (which incentivizes long intervals)
3. Focus on technical performance
4. Production price is secondary (often ignored)
5. Product price is cost-plus
6. Product reaches users via Government deployment

Performance is King

Relationship between end users and product developer is usually remote



Is there a
“Middle Ground”

Pure Commercialization

1. Requirements derived by Private Sector
2. Product development funded by the developer (which incentivizes short intervals)
3. Technical performance secondary (often reduced in favor of price)
4. Focus on price point
5. Product price is market-based
6. Product reaches users via marketing and sales channels

Performance/Price is King

Relationship between end users and product developer is crucial



**Homeland
Security**

A New Model for Commercialization

1. Development of Operational Requirements Document (ORD)
2. Assess addressable market(s)
3. Publish ORD and market assessment on public DHS web portal, soliciting interest from potential partners
4. Execute no-cost agreement (streamlined CRADA) with multiple Private Sector entities, transferring technology (if necessary)
5. Develop supporting grants and standards as necessary
6. Assess T&E after product is developed
7. New Commercial off the Shelf (COTS) product marketed by Private Sector with DHS support

Differences from the Acquisition model:

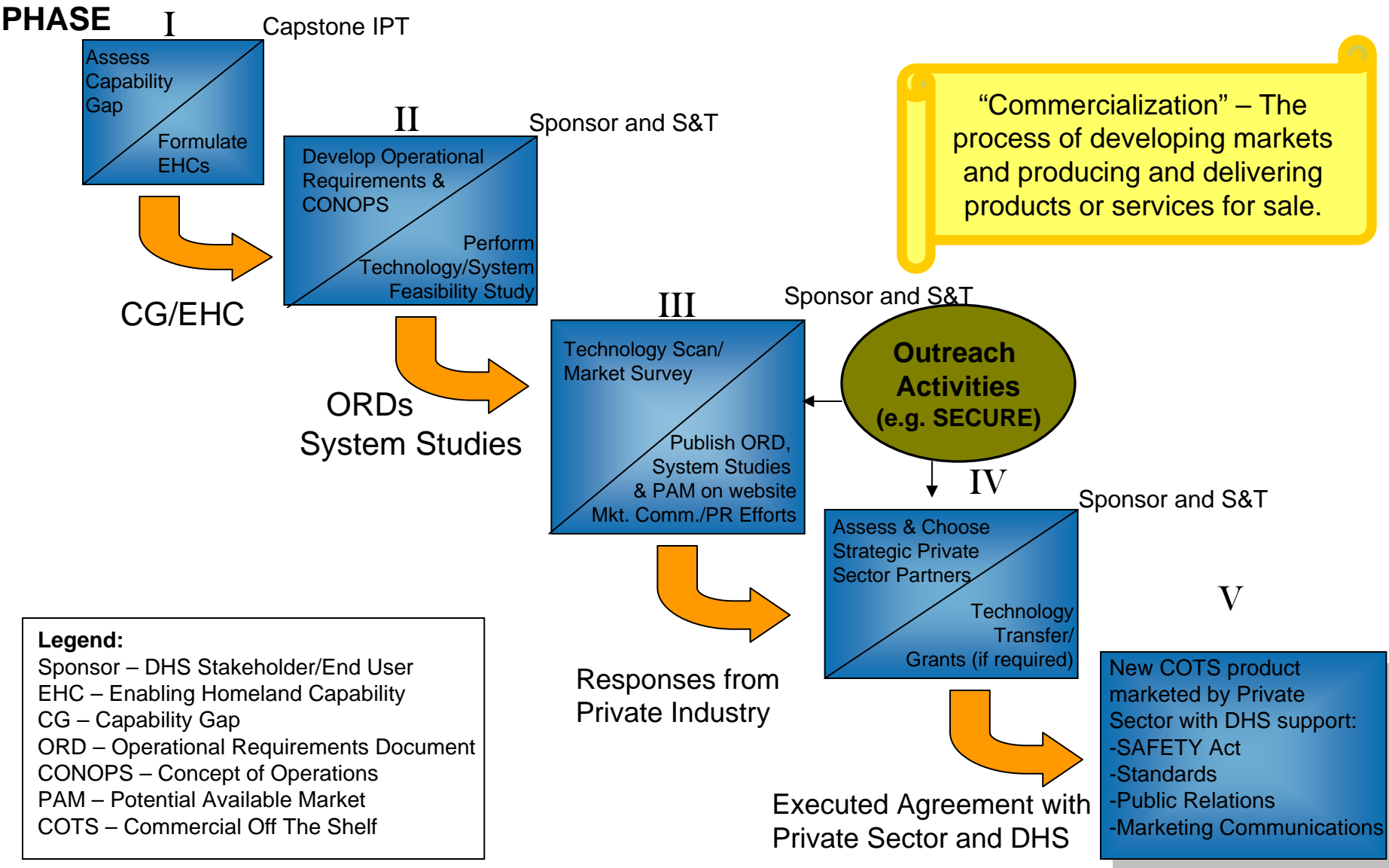
- **Primary criteria for partner selection is market penetration, agility, and performance/price ratio**
- **Product development is not funded by DHS**
- **Government involvement is limited to inherently governmental functions (e.g., Grants and Standards)**



**Homeland
Security**

Commercialization Process

“Commercialization” – The process of developing markets and producing and delivering products or services for sale.



Legend:
 Sponsor – DHS Stakeholder/End User
 EHC – Enabling Homeland Capability
 CG – Capability Gap
 ORD – Operational Requirements Document
 CONOPS – Concept of Operations
 PAM – Potential Available Market
 COTS – Commercial Off The Shelf

ORD: Operational Requirements Document

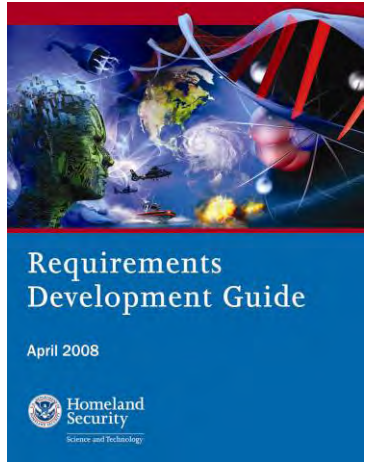
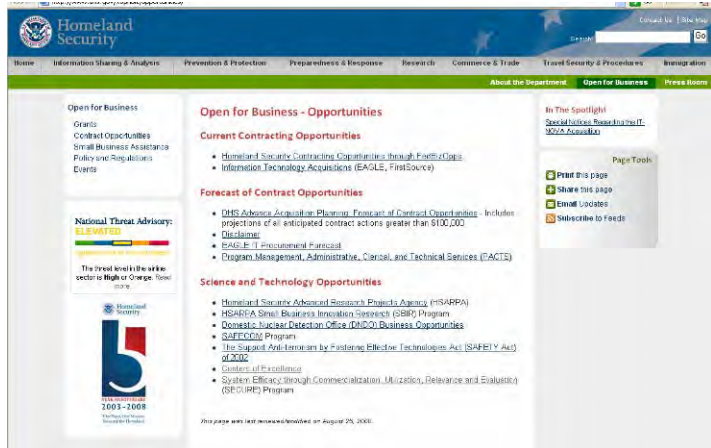
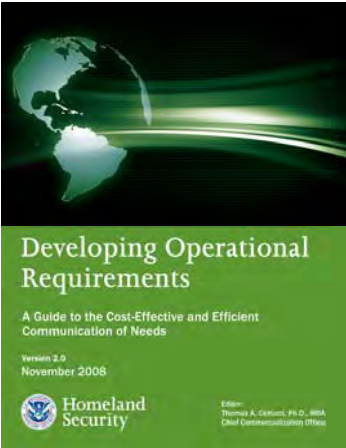
What: ORDs provide a clear definition and articulation of a given problem.

How: Training materials have been developed to assist drafting ORDs.

- *Developing Operational Requirements*, 194pp. Available online: http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf

When: For Use in Acquisition, Procurement, Commercialization and Outreach Programs –Any situation that dictates detailed requirements (e.g. RFQ, BAA, RFP, RFI, etc.)

Why: It's cost-effective and efficient for both DHS and all of its stakeholders.



Why SECURE Program

•Multi-Use

- Provides private sector, in an open and transparent way, with what they need most - - Business Opportunities
- Provides assurance to DHS, First Responders and private sector users (like CI/KR) that products/services perform as prescribed (and provides vehicle for First Responders, CI/KR owners and operators to voice their requirements)
- Augments the value of the SAFETY Act

•Saves Money

- Private Sector uses its own resources to develop products and services to the benefit of the taxpayer and the Federal Government

•Creates Jobs

- Detailed articulation of requirements coupled with funded large, potential available markets yield OPPORTUNITY that yields Job Creation (it's better to teach a person to fish than to give them a fish)
- Enables small firms with innovative technologies to partner with larger firms, VCs and angel investors because of the credibility of having government show detailed requirements with associated market potential (instead of just their own business plans).

•Efficient Use of Government Funds

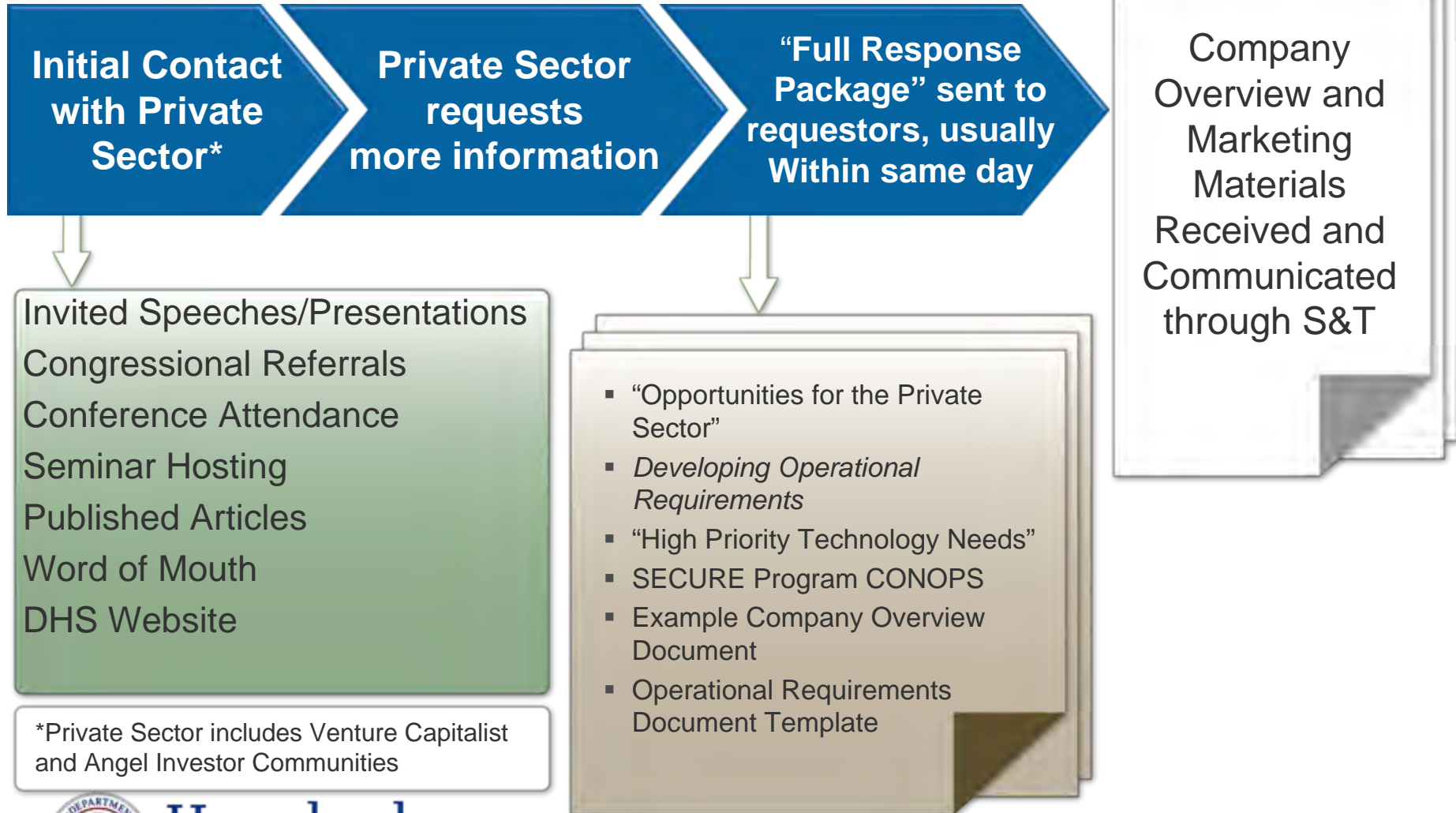
- Articulating detailed requirements saves time and money. It is better for Government to spend funds to procure products or services that are available for sale and rigorously tested compared to spending money and time to develop new solutions for ill-defined problems.

SECURE Program Benefit Analysis

“Win-Win-Win”

Taxpayers	Private Sector	Public Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Save significant time and money on market and business development activities	1. Improved understanding and communication of needs
2. Tax savings realized through Private Sector investment in DHS	2. Firms can genuinely contribute to the security of the Nation	2. Cost-effective and rapid product development process saves resources
3. Positive economic growth for American economy	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work	3. Monies can be allocated to perform greater number of essential tasks
4. Possible product “spin-offs” can aid other commercial markets	4. Significant business opportunities with sizeable DHS and DHS ancillary markets	4. End users receive products aligned to specific needs
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. Commercialization opportunities for small, medium and large business	5. End users can make informed purchasing decisions with tight budgets

Contact with the Private Sector



Commercialization Office - Return on Investment (ROI)

Assumptions for Conservative ROI Projections:

- *Return on Investment* – (Gain on Investment/Cost Savings – Cost of Investment) / Cost of Investment
- *Gain on Investment/Cost Savings* – conservative estimate of potential savings of nominally expended R&D dollars at S&T; in general, estimated savings is 75% of given/related FY09 enabling homeland capability (EHC), which is identified through Capstone IPT process
- *SECURE Program – Cost of Investment* – 20% of Commercialization Office personnel salary + (10% Other expenses such as OGC, OPA, CCD, etc.); divided by 20 operational requirements documents (ORDs) completed and publically released in given year
- *R&D Funds at DHS S&T* – R&D funds do not include labor or overhead (not fully burdened cost of managing program/projects/EHCs)

SECURE Program – ORD	Market Size	ROI
<u>Blast Resistant Autonomous Video Equipment (BRAVE) ORD</u> Requirements for a forensic camera deployed in public transportation vehicles to assist in incident cause analysis.	Over 1.5 million units	290
<u>National Emergency Response Interoperability Framework and Resilient Communication System of Systems ORD</u> Requirements for a system to provide interoperable communications on a national framework for remote use by first responders.	Over 2,000 units	525
<u>Interoperable Communications Switch ORD</u> Requirements for an interoperability switch-based communications system that provides networked communications between any number of agencies and personnel.	Over 230 units	525
<u>Crisis Decision-Support Software ORD</u> Requirements for a system with a user-centric approach matched with an expansive database of past decisions and a proven method to quickly reach critical decisions in high pressure environments for wide operational use.	Approx. 50,000 units	1023
<u>Blast Mitigation of Fuel Tank Explosions ORD</u> Requirements for an explosion suppression system to protect fuel containers. A “fuel container” ranges from fuel tanks found in vehicles, boats or trains to fuel storage tanks at airports, seaports and the neighborhood gas station.	Over 1 million units	727
<u>Integrated Intrusion Protection ORD</u> Requirements for an adaptable, scalable surveillance capability that provides automated, real-time protection for a wide range of operational scenarios.	Over 41,000 units	290
<u>Predictive Modeling for Counter-Improvised Explosive Devices (IED) ORD</u> Requirements for a system to predict the threat of an IED attack and further data fusion from law enforcement, intelligence partners and other sources to support the common operating picture.	Over 250,000 seats in US alone	870

Return on DHS Investment is LARGE when compared to Angel Investors (4x to 7x) and Venture Capitalists (5x to 20x)

Let's Make it Happen

Commercialization Office Major Activities

Potential Benefits

Requirements Development Initiative enables easy-to-use guidelines for articulating detailed operational requirements used throughout the Department to enhance internal and external communications for program/project development and execution, procurement and private sector outreach programs.

Net Impact:
Savings of >\$2.5 Billion annually in DHS resources

S&T Commercialization Process ensures the cost-effective and efficient development of products/services for DHS, First Responders, and Critical Infrastructure/Key Resources owners with the aid of the private sector's resources.

Net Impact:
When implemented across DHS, conservative savings in current and opportunity costs >\$10 Billion annually.

SECURE Program is an innovative public-private partnership in which DHS relays detailed operational requirements and a conservative estimate of potential available markets for a given need in exchange for the private sector to develop widely distributed product/service at their own expense.

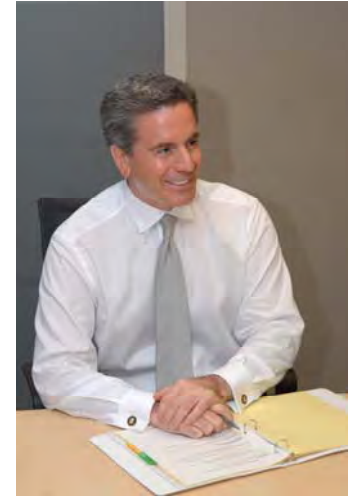
Net Impact:
To date, over \$261 Million has been conservatively invested in DHS projects for the SECURE Program pilot.

S&T Private Sector Outreach is a concerted effort to engage the private sector in understanding DHS detailed needs and establish a large repository of technologies/products/services aligned with DHS needs.

Net Impact:
Savings of >\$350 Million in S&T Budget and opportunity costs.

U.S. Department of Homeland Security: Science and Technology Directorate's Chief Commercialization Officer

Dr. Cellucci accepted a five-year appointment from the Department of Homeland Security in August 2007 as the Federal Government's first Chief Commercialization Officer (CCO). He is responsible for initiatives that identify, evaluate and commercialize technology for the specific goal of rapidly developing and deploying products and services that meet the specific operational requirements of the Department of Homeland Security's Operating Components and other DHS stakeholders such as First Responders and Critical Infrastructure/Key Resources owners and operators. Cellucci has also developed and continues to drive the implementation of DHS-S&T's outreach with the private sector to establish and foster mutually beneficial working relationships to facilitate cost-effective and efficient product/service development efforts. His efforts led to the establishment of the DHS-S&T Commercialization Office in October 2008. The Commercialization Office is responsible for four major activities; a requirements development initiative for all DHS stakeholders, the development and implementation of a commercialization process for DHS, development and execution of private sector partnership programs such as SECURE and leading the private sector outreach for the S&T directorate.



Since his appointment, he has published three comprehensive guides [*Requirements Development Guide* (April 2008), *Developing Operational Requirements* (May 2008), and *Developing Operational Requirements, Version 2* (November 2008)] dealing with the development of operational requirements, developed and implemented a commercialization model for the entire department and established the SECURE Program—an innovative public-private partnership to cost-effectively and efficiently develop products and services for DHS's Operating Components and other DHS stakeholders. In addition, he has written over 25 articles and a compilation of works [*Harnessing the Valuable Experiences and Resources of the Private Sector for the Public Good*, (February 2009)] geared toward the private sector to inform the public of new opportunities and ways to work with DHS. Cellucci has received recognition for his outreach efforts and engagement with the small and disadvantaged business communities who learn about potential business opportunities and avenues to provide DHS with critical technologies and products to help secure America. Cellucci is an accomplished entrepreneur, seasoned senior executive and Board member possessing extensive corporate and VC experience across a number of worldwide industries. Profitably growing high technology firms at the start-up, mid-range and large corporate level has been his trademark. He has authored or co-authored over 139 articles on Requirements development, Commercialization, Nanotechnology, Laser physics, Photonics, Environmental disturbance control, MEMS test and measurement, and Mistake-proofing enterprise software. He has also held the rank of Lecturer or Professor at institutions like Princeton University, University of Pennsylvania and Camden Community College. Cellucci also co-authored ANSI Standard Z136.5 "The Safe Use of Lasers in Educational Institutions". Dr. Cellucci is also a commissioned Admiral and Commander of a Squadron in Texas responsible for civil defense and has been a first responder for over twenty years. As a result of his consistent achievement in the commercialization of technologies, Cellucci has received numerous awards and citations from industry, government and business. In addition, he has significant experience interacting with high ranking members of the United States government—including the White House, US Senate and US House of Representatives—having provided executive briefs to three Presidents of the United States and ranking members of Congress. Cellucci represents DHS as the first Federal Government member on the U.S. Council on Competitiveness.

Cellucci earned a PhD in Physical Chemistry from the University of Pennsylvania, an MBA from Rutgers University and a BS in Chemistry from Fordham University. He has also attended and lectured at executive programs at the Harvard Business School, MIT Sloan School, Kellogg School and others. Dr. Cellucci is regarded as an authority in rapid time-to-market new product development and is regularly asked to serve as keynote speaker at both business and technical events.



Homeland Security



Commercialization: The First Responders' Best Friend

DHS reaches out to First Responders to address their needs

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security**

January 2009



**Homeland
Security**

Science and Technology

Commercialization: The First Responders' Best Friend

DHS reaches out to First Responders to address their needs

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

Commercialization, broadly described as “the development of markets and the production and delivery of products/services to meet the unsatisfied needs/wants of the markets,” represents a key process that the U.S. Department of Homeland Security can use to create effectively capabilities for the first responder community.

Commercialization allows DHS to develop and deliver products/services to the first responder community in a more cost-effective and efficient manner as compared to a traditional governmental Acquisition process; at the benefit of the first responder and, just as importantly, to the benefit of the American taxpayer. Through this commercialization process, DHS is fostering new partnerships with the private sector to participate in cooperative product/service development efforts aligned to DHS needs.

In a relatively short amount of time, DHS has developed and is now implementing a “commercialization mindset” in its approach to responding to the needs of its stakeholders. These stakeholders include DHS’s seven operating components (TSA, CBP, FEMA, ICE, USCIS, U.S. Secret Service and U.S. Coast Guard), the first responder community and the critical infrastructure/key resources (CIKR) owner/operators. The idea of utilizing a commercialization process at DHS is a much-needed and significant departure from the commonly employed Acquisition model because it has the potential to yield significant benefits in terms of reducing research and development costs, as well as realizing a much more rapid time-to-market for newly developed commercial products/services for DHS. Rather than have DHS pay for the development of custom “one-off” systems, which is frequently the case in military applications, it is apparent that DHS has much to offer the private sector in terms of potential available markets that can be addressed in a more “commercial” fashion with firms competing for sales in an open and free market system. Figure 1 shows the major differences between a “pure” Acquisition versus “pure” commercialization process, and our resultant DHS “hybrid” commercialization process.

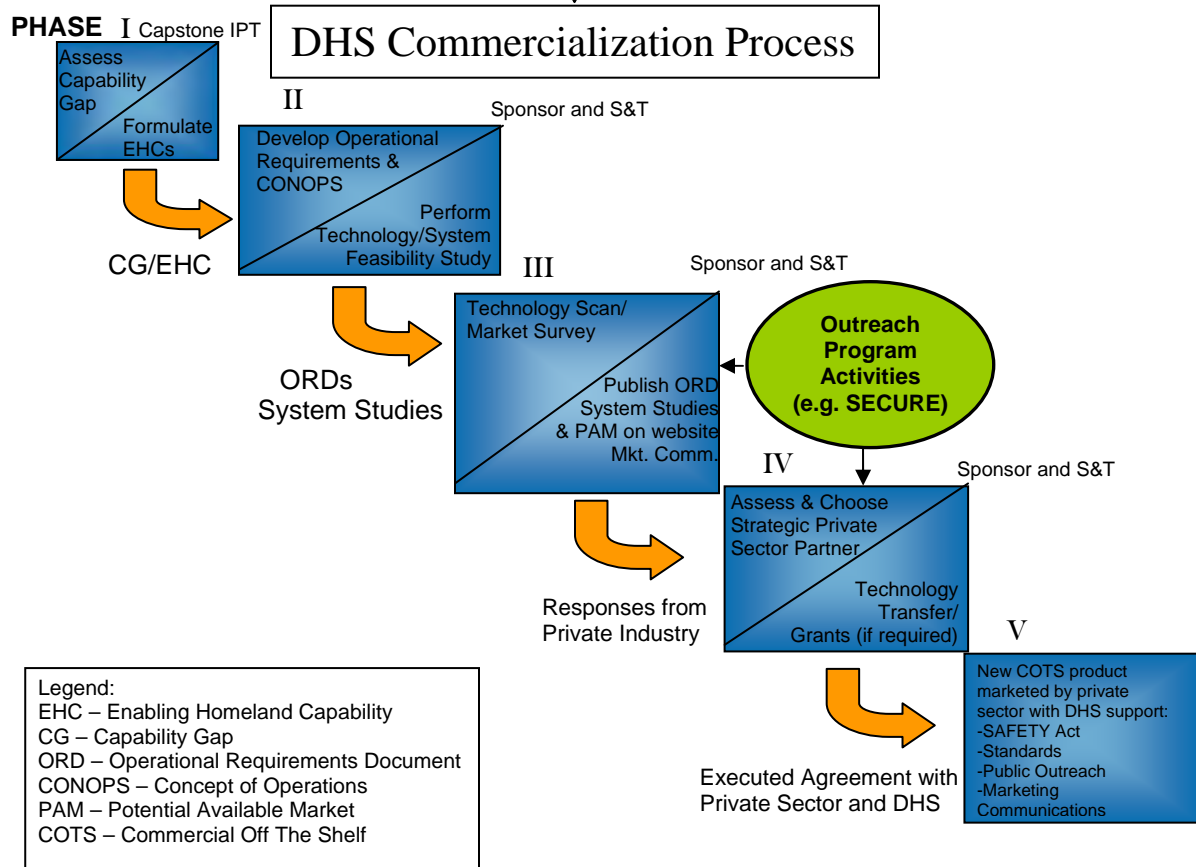
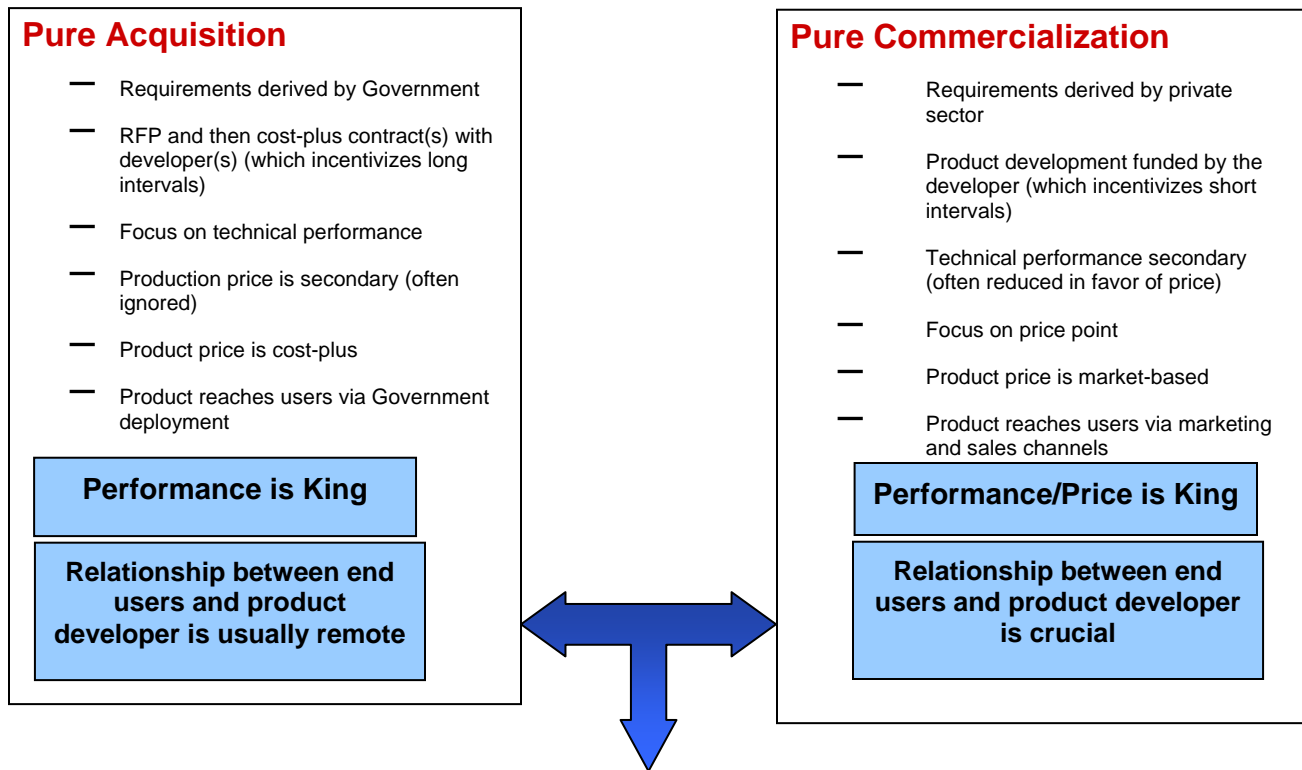


Figure 1 DHS’s commercialization process combines aspects of a “pure” Acquisition and Commercialization model resulting in the current “hybrid” commercialization model.

The SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program, outlined in Figure 2, is one such effort leveraging the DHS commercialization process to meet end-user needs. Briefly, the SECURE Program is based on the premise that the private sector has shown repeatedly that it is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and money to such activities if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two things from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s). This information can then be used by the private sector to generate a business case for their possible participation in the program.

SECURE Program

Overview of Concept of Operations



- **Application** – Seeking products/technologies aligned with posted DHS requirements
- **Selection** – Products/Services TRL-5 or above, scored with internal DHS metrics
- **Agreement** – One-page Cooperative Research and Development (CRADA)-like document that outlines milestones and exit criteria
- **Publication of Results** – Recognized Third-Party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal
Benefits:
 - ✓ Successful products/technologies share in the imprimatur of DHS
 - ✓ DHS operating components and first responders make informed decisions on products/services aligned to their stated requirements

Figure 2 A brief overview of the SECURE Program Concept of Operations. (See http://www.dhs.gov/xres/programs/gc_1211996620526.shtm)

While the development of highly specialized products is still relevant to the Department, DHS itself represents a substantial potential available market for widely distributed products; in many instances requiring thousands, if not millions of product or service units to address unsatisfied needs. Couple to this the fact that DHS has responsibility for an array of ancillary markets: namely, first responders and CIKR owner/operators, representing large potential available markets in their own right; it is evident that substantial business opportunities exist for the private sector. Figure 3 shows those groups of individuals classified as first responders according to Homeland Security Presidential Directive 8. While these groups represent a highly fragmented market, the

size of the market is nonetheless attractive enough that many companies seek to capture portions of it.



Figure 3 Homeland Security Presidential Directive (HSPD) - 8 classifies those individuals considered first responders in the United States. A conservative estimate shows that over 25.3 Million people work or volunteer as first responders. For a complete segmentation of the first responder market map, please refer to Appendix I of the Developing Operational Requirements book available online at http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf.

There is a new concentrated focus in understanding the requirements of members of the first responder community in an effort to close their mission-critical capability gaps. Given the fragmented nature of the first responder communities, DHS, through the Science and Technology Directorate (S&T), is formulating a crosscutting Capstone Integrated Product Team (IPT) to focus solely on the needs and requirements of the first responders. Figure 4 shows the general organization of a Capstone IPT along with the appropriate functions of each member. This First Responder Capstone IPT will reach out to the various first responder associations and organizations across the country to gain valuable insight into their needs and requirements and provide a forum for them to be discussed and addressed.

S&T Transition IPT Members and Function

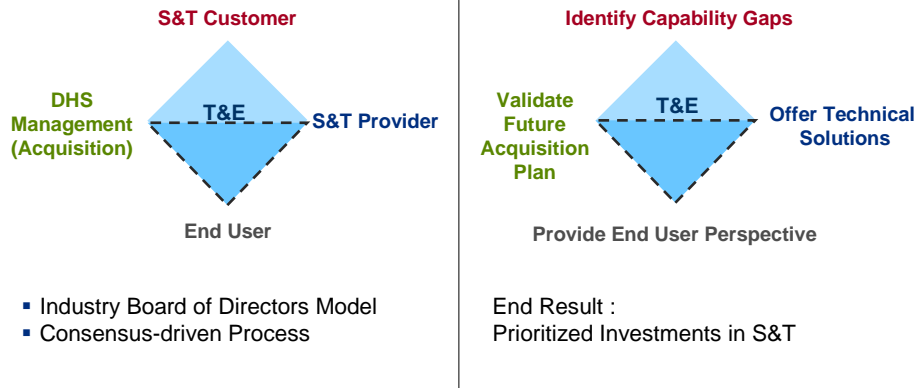


Figure 4 The First Responder Capstone IPT will bring together end-users, scientists and program managers to discuss mission-critical capability gaps and requirements.

The Capstone IPT process¹ ensures that quality, efficacious products are developed in close alignment with customer needs. Through a network of communication channels, Capstone IPTs bring together S&T division heads, management personnel and end-users (operating components, field agents and supporting first responders and/or CIKR owner/operators) involved in Research, Development, Testing and Evaluation (RDT&E). Working collaboratively, the First Responder IPT collects, evaluates and prioritizes requirements to enable new mission-critical capabilities.

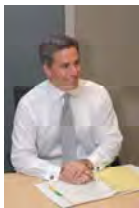
In providing critical information to the private sector in terms of the collection and articulation of detailed operational requirements and a conservative estimate of the potential available market, DHS has laid the foundation for cooperative product development with the private sector. These relationships drive the commercialization process and ensure that end-users such as first responders receive needed products/services in a timely manner at minimal costs to DHS. Given these relationships, it is relatively easy to make a case for commercialization at the Department (see Figure 5) as it results in “wins” for the American taxpayer, public and private sectors.

¹ Kikla, Richard V. and Cellucci, Thomas A. “Capstone IPTs: Even in Government the Customer Comes First,” April 2008.

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Figure 5 A benefit analysis of the SECURE Program shows a number of positive outcomes for Taxpayers as well as the public and private sectors.

In conclusion, a commercialization process is ideal to match the detailed requirements of the collective first responder community with product development efforts undertaken by the private sector who seek access to the large potential available markets represented by the first responders. Commercialization is not only an attractive method by which DHS can develop products/services for first responders – but it is also beneficial to both the public and private sectors and – most importantly – to the American taxpayers at large.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security’s first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





DHS: Leading the way to Help the Private Sector Help Itself

The Office of Infrastructure Protection offers a window into which the private sector can realize significant business opportunities

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Science and Technology, Commercialization Office
U.S. Department of Homeland Security**

February 2009



**Homeland
Security**

Science and Technology

DHS: Leading the way to Help the Private Sector Help Itself

The Office of Infrastructure Protection offers a window into which the private sector can realize significant business opportunities

Thomas A. Cellucci, Ph.D., MBA
 Chief Commercialization Officer
 Commercialization Office
 U.S. Department of Homeland Security

Commercialization, broadly described as “the development of markets and the production and delivery of products/services to meet the unsatisfied needs/wants of these markets,” represents a key process that the U.S. Department of Homeland Security (DHS) now uses to generate product/services for its numerous stakeholders in a cost-effective and efficient way. DHS’s primary users of technology-based products are its seven operating components. However, DHS is also a conduit to numerous other users. For example, the Office of Infrastructure Protection (OIP) coordinates 18 Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) organized under the National Infrastructure Protection Plan (NIPP). These SCCs represent various critical infrastructure/key resources (CI/KR) owners and operators found in the chemical industry to power companies, for example. See Table 1 for the list of SCCs. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would create a debilitating effect on our security, national economic security, public health or safety, or any combination of the above. Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

Responsible Federal Agency	Sector Coordinating Council
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Public Health and Healthcare
Department of Interior	National Monuments and Icons
Department of Treasury	Banking and Finance
Environmental Protection Agency	Water
DHS’s Office of Infrastructure Protection	Chemical Commercial Facilities Dams Emergency Services Nuclear Reactors, Materials, and Waste Critical Manufacturing
DHS’s Office of Cyber Security and Telecommunications	Information Technology Communications
DHS’s Transportation Security Administration	Postal and Shipping

DHS's Transportation Security Administration, United States Coast Guard	Transportation Systems
DHS's Immigration and Customs Enforcement, Federal Protective Service	Government Facilities

Table 1 – HSPD-7 establishes a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks.

Under Homeland Security Presidential Directive 7 (HSPD-7), Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies work with state and local governments and the private sector to accomplish this objective. The NIPP process provides clarity into the specific needs or requirements of the SCCs, which in turn generates information that yields rough estimates of the potential available markets (PAMs) for solutions that address a particular need.

The recently adopted, commercialization process allows DHS to develop and deliver products/services for the CI/KR community in a more cost-effective and efficient manner as compared to a traditional governmental Acquisition process; all at the benefit of the CI/KR owners and operators in the private sector and, just as importantly, to the benefit of the American taxpayer. Through this commercialization process, DHS is fostering new and innovative partnerships with the private sector to cooperatively develop products/services aligned to the needs of the expansive CI/KR market.

In a relatively short amount of time, DHS has developed, and is now implementing, a “commercialization mindset¹” in its approach to responding to the needs of its valued stakeholders. The idea of utilizing a commercialization process at DHS is a much-needed and significant departure from the commonly employed Acquisition model. Commercialization has the potential to yield significant benefits in terms of reducing federal R&D costs, enabling rapid time-to-market for newly developed commercial products/services for DHS and some of its other stakeholders like first responders and CI/KR owners/operators. Rather than have DHS pay for the development of custom “one-off” systems, which are frequently required in many military applications, it is apparent that DHS has much to offer the private sector in terms of its large potential available markets requiring widely distributed products. Figure 1 shows the major differences between a “pure” Acquisition versus a “pure” commercialization process, and our resultant DHS “hybrid” commercialization process. To put it simply, when widely-distributed products or services are required, commercialization should be utilized at the benefit of the taxpayer, DHS and the private sector.

¹ See, for example, *Developing Operational Requirements, Version 2, Product Realization Chart, DHS Implements a Commercialization Process* and other valuable resources online at http://www.dhs.gov/xres/programs/gc_1211996620526.shtm

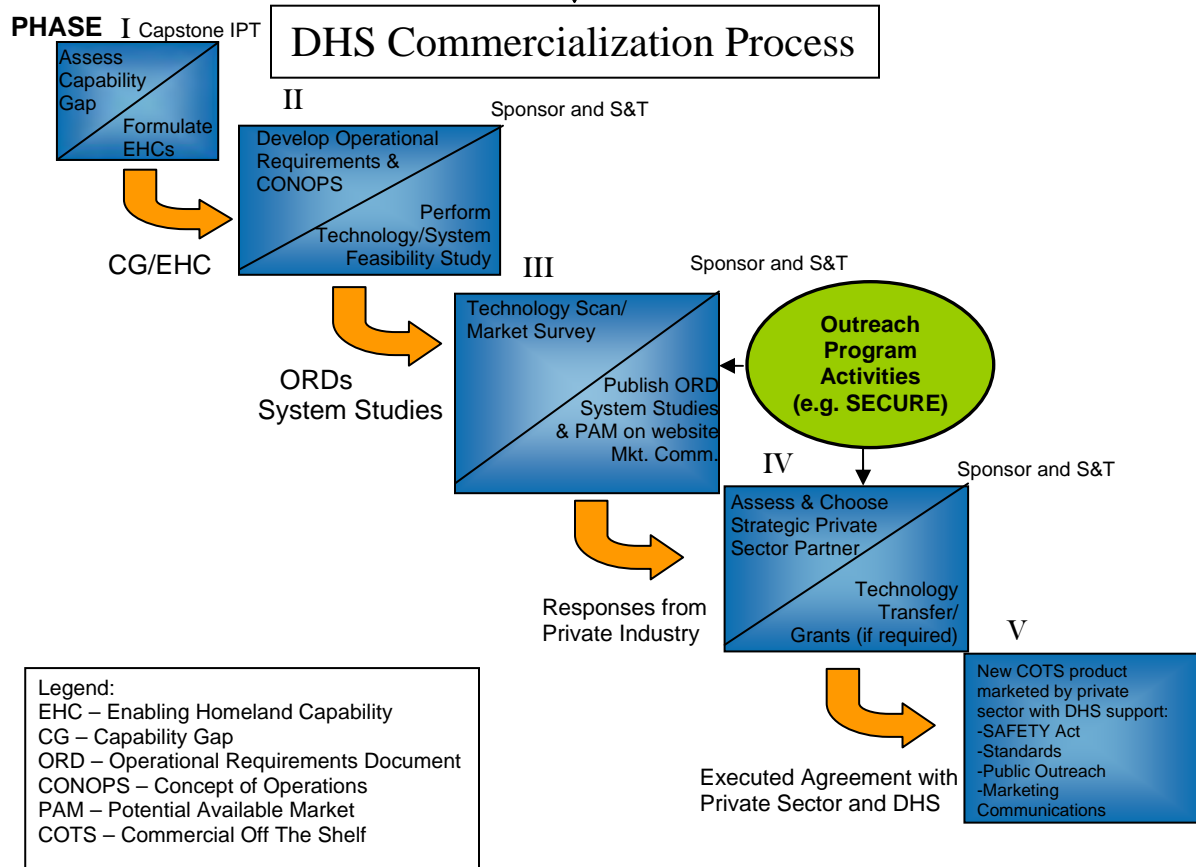
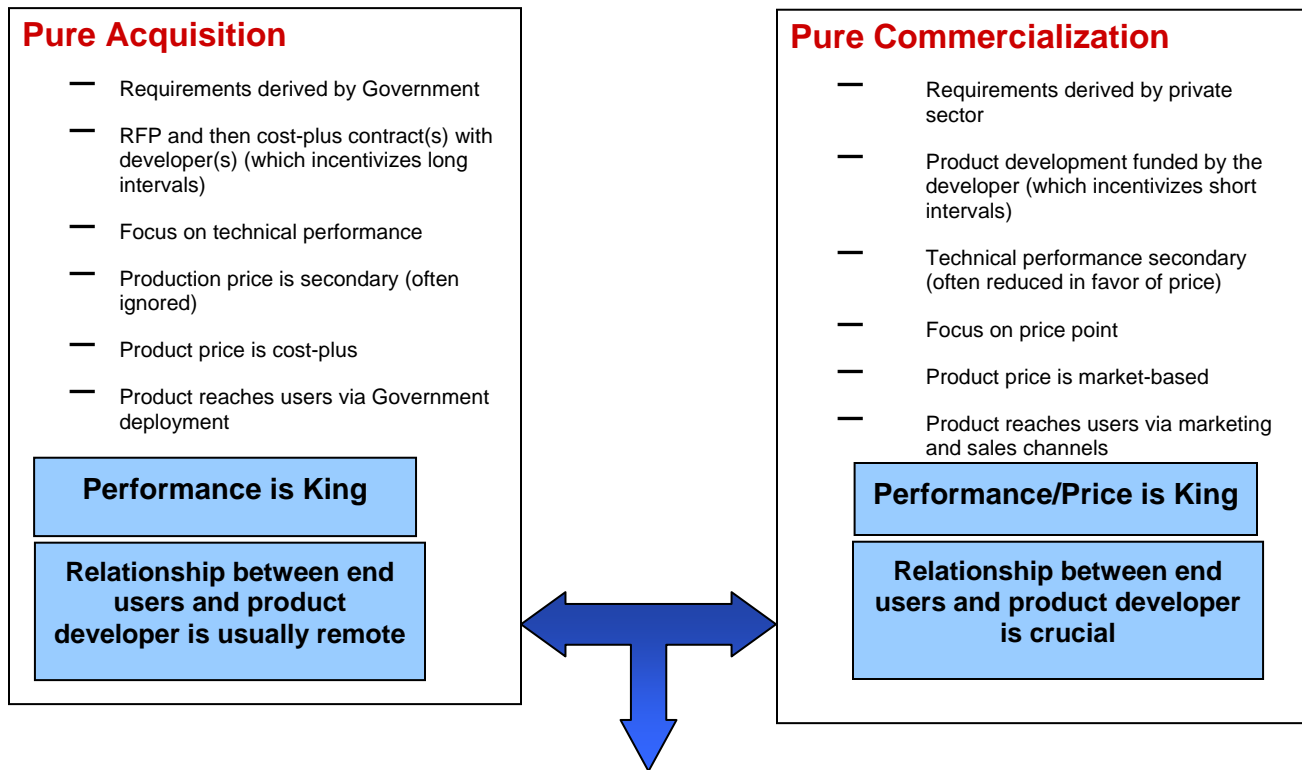
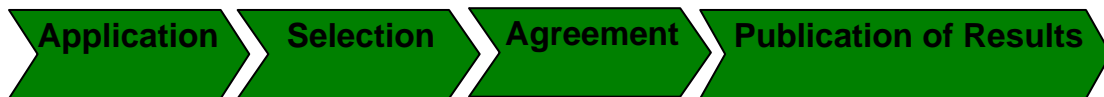


Figure 1 DHS’s commercialization process combines aspects of a “pure” Acquisition and commercialization model resulting in the current “hybrid” commercialization model.

The SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program, outlined in Figure 2, is an innovative public-private sector partnership effort leveraging the DHS commercialization process to meet end-user needs found at DHS, the first responder community and within the CI/KR market. Briefly, the SECURE Program is based on the premise that the private sector has shown repeatedly that it is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and money to such activities if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two pieces of information from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s) where a given product or service can be used. This information can then be verified by the private sector to generate a business case for their possible participation in the program.

SECURE Program

Overview of Concept of Operations



- **Application** – Seeking products/technologies aligned with posted DHS requirements
- **Selection** – Products/Services TRL-5 or above, scored with internal DHS metrics
- **Agreement** – One-page Cooperative Research and Development (CRADA)-like document that outlines milestones and exit criteria
- **Publication of Results** – Recognized Third-Party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal
Benefits:
 - ✓ Successful products/technologies share in the imprimatur of DHS
 - ✓ DHS operating components and first responders make informed decisions on products/services aligned to their stated requirements

Figure 2 A brief overview of the SECURE Program Concept of Operations. (See http://www.dhs.gov/xres/programs/gc_1211996620526.shtm)

While the development of highly specialized products is still relevant to the Department, DHS itself represents a substantial potential available market for widely distributed products; in many instances requiring thousands, if not millions of product or service units to address unsatisfied needs. Couple to this the fact that DHS has responsibility for an array of ancillary markets: namely, first responders and CI/KR owners/operators, representing large potential available markets in their own right; it is evident that substantial business opportunities exist for the private sector. The NIPP process brings greater vision into the needs of the 18 SCCs previously described, which

in turn generate the detailed operational requirements necessary for private sector efforts to develop potential solutions. See Figure 3 for a market potential template of the 18 sectors and their major sub-components/applications.

Critical Infrastructure Key Resources (CIKR)															
Agriculture and Food	Defense Industrial Base	Energy	Public Health and Healthcare	Natural Monuments and Icons	Banking and Finance	Water	Chemical	Commercial facilities	Emergency Services	Materials, Reactors and	Telecommunications	Critical Manufacturing	Retail and Shipping Services	Transportation	Information Technology
Food Retail \$. . Units	Defense Contractors \$. . Units	Coal mining operations \$. . Units	Public/University hospitals \$. . Units	Guided tour services \$. . Units	Credit lending institutions \$. . Units	Public utilities \$. . Units	Inorganic chemical production \$. . Units	Hotels \$. . Units	Fire Departments \$. . Units	Electric utilities \$. . Units	Telephone/Cellular services \$. . Units	Iron and Steel mills \$. . Units	United States Postal Service \$. . Units	AMTRAK \$. . Units	Hardware providers \$. . Units
Farm Equipment \$. . Units	Industry analysis \$. . Units	Coal power plants \$. . Units	Private/For Profit hospitals \$. . Units	Travel services \$. . Units	Commercial banking \$. . Units	Desalination plants \$. . Units	Organic industrial production \$. . Units	Shopping centers \$. . Units	Law enforcement agencies \$. . Units	Reactor and associated materials \$. . Units	Satellite data transmission \$. . Units	Aluminum production and processing \$. . Units	High volume document and parcel shipping \$. . Units	Commuter rail \$. . Units	IT Conglomerates \$. . Units
Meat/Poultry Processing \$. . Units	Think tanks/research institutions \$. . Units	Coal equipment manufacturers \$. . Units	Clinics \$. . Units	Lodging/Hotel \$. . Units	Private equity \$. . Units	Treatment plants \$. . Units	Ceramics \$. . Units	Stadiums and sport arenas \$. . Units	Search and rescue teams \$. . Units	University and educational institutions \$. . Units	Broadcasting entities \$. . Units	Nonferrous metal production and processing \$. . Units	Container shipping services \$. . Units	Intracity rail services \$. . Units	Semiconductor production \$. . Units
Food Processing \$. . Units	University partnership programs \$. . Units	Hydroelectric \$. . Units	Private medical practices \$. . Units	Guest services/tourist hospitality \$. . Units	Consumer banking \$. . Units	Equipment manufacturers \$. . Units	Petrochemicals \$. . Units	Schools \$. . Units	Ambulance companies \$. . Units	Control systems \$. . Units	Broadcast equipment manufacturing \$. . Units	Engine, Turbine and Power transmission \$. . Units	Commercial airline \$. . Units	Commercial airfare \$. . Units	Electronics manufacture \$. . Units
Dairy Processing \$. . Units	National laboratories \$. . Units	Dam operations \$. . Units	Medical laboratories \$. . Units	People moving services \$. . Units	Building societies/Private banks \$. . Units	Pipe and water control device manufacturers \$. . Units	Agrochemicals \$. . Units	Commercial office buildings \$. . Units	Mountain/Cave/ Mine rescue teams \$. . Units	Nuclear safety systems \$. . Units	Radio equipment manufacturing \$. . Units	Marine shipping \$. . Units	Private air services \$. . Units	IT services \$. . Units	
Dairy Farms \$. . Units		Wind power \$. . Units	Pharmaceutical \$. . Units	Quoting equipment makers \$. . Units	Merchant banks \$. . Units		Polymers \$. . Units	Museums \$. . Units	Other technical rescue teams \$. . Units	Waste disposal services \$. . Units	Intelnet equipment manufacturing \$. . Units	Trucking industry \$. . Units	Subway hardware \$. . Units	IT services \$. . Units	
Ranching \$. . Units		Solar power \$. . Units	Health insurance \$. . Units	Private security \$. . Units	Global financial services firms \$. . Units		Elastomer production \$. . Units	Zoos and Aquariums \$. . Units	Bomb disposal units \$. . Units	Uranium processors \$. . Units	High speed data transmission \$. . Units	Airborne shipping \$. . Units	Cruise lines \$. . Units	IT services \$. . Units	
Organic Farming/Sustainable Agriculture \$. . Units		Public utilities companies \$. . Units	Medical material providers \$. . Units	Community development institutions \$. . Units	Community banks \$. . Units		Oleochemicals \$. . Units	Public Libraries \$. . Units	Blood/Organ transplant supply \$. . Units	Protective garment manufacturers \$. . Units	Internet service providers \$. . Units	Motor Vehicle manufacturing \$. . Units	Subway systems \$. . Units	IT services \$. . Units	
Traditional Planting \$. . Units		Oil companies \$. . Units	Medical equipment manufacturers \$. . Units	Community banks \$. . Units	Savings and Loans \$. . Units		Explosives \$. . Units	Amusement parks \$. . Units	Amateur radio emergency comms \$. . Units	Print media \$. . Units	Railroad rolling stock \$. . Units	Aviation product & parts manufacturing \$. . Units	Long-haul maritime shipping \$. . Units	IT services \$. . Units	
Commercial Fishing \$. . Units			Medical technology manufacturers \$. . Units	Community banks \$. . Units	Credit unions \$. . Units		Fragrance production \$. . Units		Public utility protection providers \$. . Units	Internet technology providers \$. . Units	Other Transportation equipment \$. . Units	Distribution services \$. . Units	Trucking \$. . Units	IT services \$. . Units	
			Biotechnology \$. . Units	Insurance companies \$. . Units	Insurance brokerages \$. . Units		Chemical wholesale \$. . Units		Emergency Road Services \$. . Units			Railroad rolling stock \$. . Units	Bus services \$. . Units	IT services \$. . Units	
				Reinsurance companies \$. . Units	Stock brokerages \$. . Units		Exotic chemicals \$. . Units		Emergency Social services \$. . Units			Railroad rolling stock \$. . Units	Freight rail services \$. . Units	IT services \$. . Units	
				Stock brokerages \$. . Units	Capital market banks \$. . Units				Community emergency response teams \$. . Units			Railroad rolling stock \$. . Units	Automobile travel \$. . Units	IT services \$. . Units	
				Angel investment \$. . Units	Angel investment \$. . Units				Disaster relief \$. . Units			Roads, Highways, bridges and tunnels \$. . Units	Automobile travel \$. . Units	IT services \$. . Units	
				Venture capital \$. . Units	Venture capital \$. . Units				Family relief teams \$. . Units				Automobile travel \$. . Units	IT services \$. . Units	
									Poison Control units \$. . Units					IT services \$. . Units	
									Animal control teams \$. . Units					IT services \$. . Units	
									Wildlife services \$. . Units					IT services \$. . Units	



Figure 3 - Market Potential Template for the CI/KR Market

Given the fragmented nature of the CI/KR communities, DHS, through the Science and Technology Directorate (S&T), created a crosscutting Capstone Integrated Product Team (IPT) to focus solely on the critical infrastructure protection needs and requirements of the CI/KR communities. Figure 4 shows the general organization of a Capstone IPT along with the appropriate functions of each member. Our Infrastructure Protection IPT² works closely with the Office of Infrastructure Protection to reach out to the various CI/KR owners and operators across the country to gain valuable insight into their needs and requirements and provide a forum for them to be addressed.

² Kikla, Richard V. and Cellucci, Thomas A. "Capstone IPTs: Even in Government the Customer Comes First," April 2008.

S&T Transition IPT Members and Function

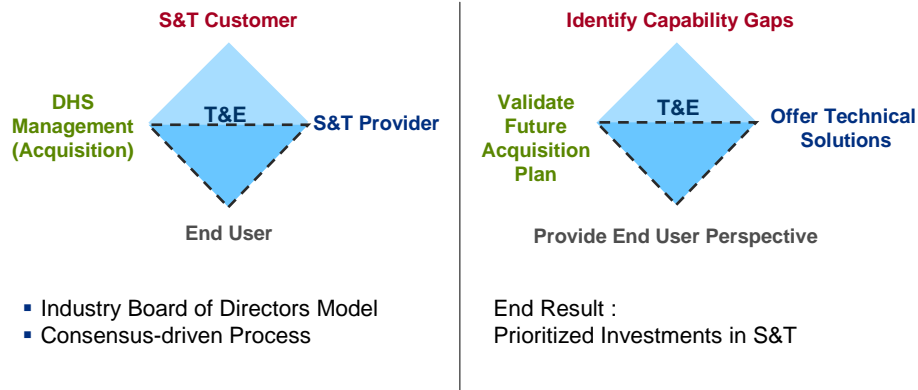


Figure 4 The Infrastructure Protection Capstone IPT will bring together end-users, scientists and program managers to discuss mission-critical capability gaps and requirements.

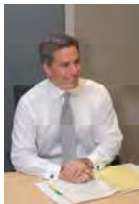
The Capstone IPT process ensures that quality, efficacious products and services are developed in close alignment with customer needs. Through a network of communication channels, Capstone IPTs bring together S&T division heads, management personnel and end-users (operating components, field agents and supporting first responders and/or CIKR owner/operators) involved in Research, Development, Testing and Evaluation (RDT&E). Working collaboratively, the Infrastructure Protection IPT collects, evaluates and prioritizes requirements to enable new mission-critical capabilities.

In providing critical information to the private sector in terms of the collection and articulation of detailed operational requirements and a conservative estimate of the potential available market, DHS has laid the foundation for cooperative product development with the private sector. These relationships drive the commercialization process and ensure that end-users such as CI/KR owners and operators receive needed products/services in a timely manner at minimal costs to DHS. Given these relationships, it is relatively easy to make a case for commercialization at the Department (see Figure 5) as it results in “wins” for the American taxpayer, public and private sectors.

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products/services	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Figure 5 A benefit analysis of the SECURE Program shows a number of positive outcomes for taxpayers as well as the public and private sectors.

In conclusion, our commercialization process is ideal in matching the detailed requirements of the collective CI/KR community with product development efforts undertaken by the private sector who seek access to the large potential available markets. Commercialization is not only an attractive method by which DHS can develop products/services for CI/KR owners and operators – but it is also beneficial to both the public and private sectors and – most importantly – to the American taxpayers at large.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security’s first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology

firms in the private sector.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





DHS Implements Commercialization Process

DHS' new commercialization process demonstrates that cost-effective and efficient development of products and services to protect our nation and its resources is possible – all at the benefit of the taxpayer.

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security**

August 2008



**Homeland
Security**

Science and Technology

DHS Implements Commercialization Process

DHS' new commercialization process demonstrates that cost-effective and efficient development of products and services to protect our nation and its resources is possible – all at the benefit of the taxpayer.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

The U.S. Department of Homeland Security (DHS) possesses an “Acquisition Mindset,” as do so many government agencies. While the Acquisition model has been utilized effectively in developing custom, one-off products such as aircraft carriers, it is not particularly germane to a majority of the needs at DHS as well as the first responders (a DHS ancillary market). The timely design, development and deployment of lower priced, widely distributed products for both DHS operating components (FEMA, TSA, USCIS, CBP, USSS, ICE and U.S. Coast Guard) and the first responder communities represents a critical step in protecting our nation. Recognizing this fact, the Department recently started implementing a “Commercialization Mindset” in order to leverage the vast capabilities and resources of the private sector through an innovative “win-win” private-public partnership called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program.

DHS experienced several challenges merging twenty-two disparate organizations into a cohesive organization with a unified mission and culture. Those familiar with M&A activities realize that while integration of organizations poses difficulties, it also represents opportunities to infuse new processes and values into the newly created organization. Through both “top-down” and “bottom-up” approaches, DHS has been successful in developing, socializing and now implementing an innovative commercialization framework that has started to gain traction throughout the agency. The creation of a “Commercialization Mindset” has caught the attention of DHS managers and employees and has been embraced by senior management because of its significant benefits to the Department’s internal and external activities.

Why is there a need for a commercialization process? DHS requirements, in most instances, are characterized by the need for widely distributed COTS (Commercial-Off-The-Shelf) products. Oftentimes, the need is for thousands, if not millions, of products for DHS’ seven operating components and the fragmented, yet substantial first responder market. Figure 1 shows the major differences between a “pure” Acquisition versus “pure” commercialization processes, along with the recently developed and implemented DHS “hybrid” commercialization process.

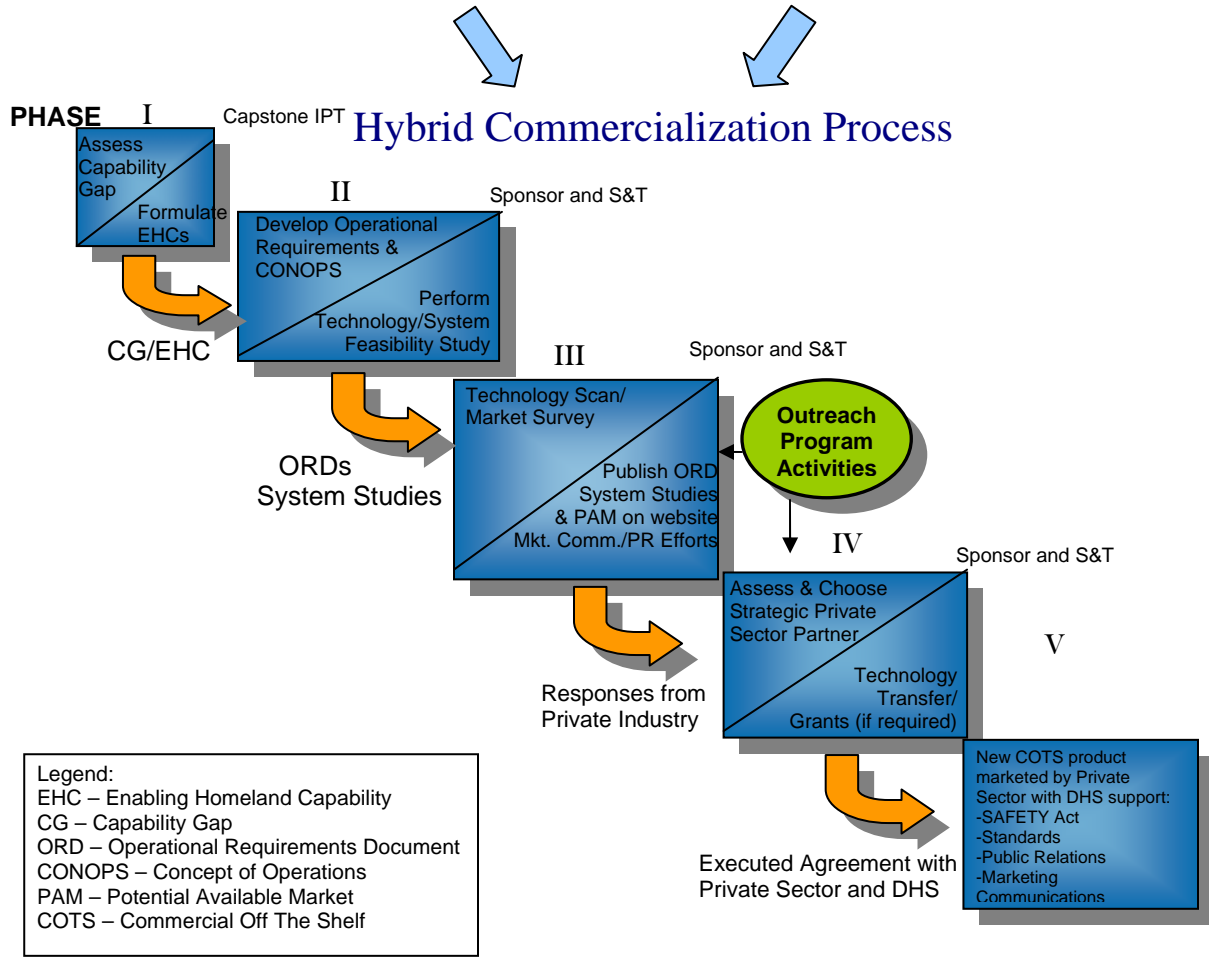
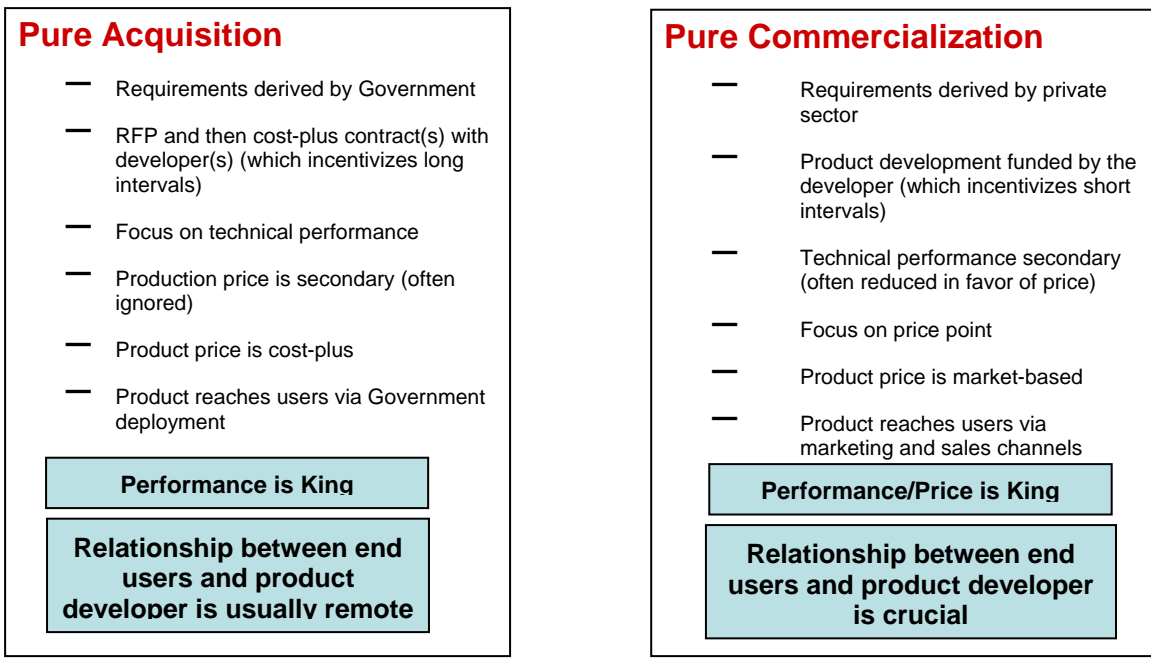
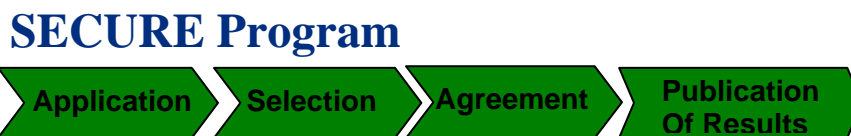


Figure 1: Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system development and the resultant hybrid model implemented by DHS.

Figure 2 delineates the overall description of DHS’ new commercialization model and its first private sector outreach program called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program to develop products and services in a private-public “win-win” partnership described in detail at www.dhs.gov/xres/programs/gc_1211996620526.shtm. Briefly, the SECURE Program is based on the simple premise that the private sector is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and resources to such activities, if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two pieces of critical information from DHS: 1. detailed operational requirement(s), and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in the program.

A New Model for Commercialization...

- Develop Operational Requirements Documents (ORDs)
- Assess addressable market(s)
- Publish ORD and market assessment on public DHS web portal, solicit interest from potential partners in a way that is open to small, medium and large businesses
- Execute no-cost (CRADA-like) agreement with multiple private sector entities and transfer technology and/or IP(if necessary)
- Develop supporting grants and standards as necessary
- Assess T&E findings after product is developed to assure DHS and ancillary markets that product meet its published specifications
- New Commercial-Off-The-Shelf (COTS) product marketed by private sector with DHS support



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized third-party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal to provide confidence to potential customers at DHS and its ancillary markets that product(s) meet or exceed their published specifications in reference to their actual performance.

Figure 2: Step-by-step guide to the commercialization process developed and adopted by DHS with a brief summary of the popular SECURE Program.

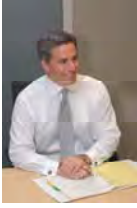
To augment the commercialization process, DHS has undertaken the task of developing an easy-to-use comprehensive guide to assist in developing operational requirements. This guide now enables DHS personnel to articulate, in detail, a given system’s requirements and communicate those needs to both internal and external audiences. This effort addresses a long standing need for DHS to fully articulate its requirements.

Early response from groups within DHS, the private sector, and first responders about this guide and programs like SECURE has been very favorable¹. The Department plans to regularly update its website with Operational Requirements Documents (ORDs) to continually expand this innovative private-public partnership. In addition, as evidenced in Figure 3, the taxpayers, private sector and public sector view programs like this as “win-win-win.”

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Figure 3: The SECURE Program is viewed positively by DHS stakeholders. The success of the program lies in the fact that all participants receive significant benefits.

In conclusion, DHS’ newly created and implemented commercialization process offers long-awaited benefits to the rapid execution of cost-effective and efficient development of products and services to protect our nation and its resources.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector.

¹ See Cellucci, T. "Opportunities for the Private Sector," 2008, 43pp. [Available online: http://www.dhs.gov/xres/programs/gc_1211996620526.shtm].

² Margetta, R. "S&T Official Working to Move Product Development Out of DHS, Into Private Sector," Congressional Quarterly Homeland Security. June 27, 2008.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





Bridging the “Communications Gap” between the Public and Private Sector – Making it Easier to do Business with DHS

DHS’ new commercialization outreach efforts center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department.

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security**

October 2008



**Homeland
Security**

Science and Technology

Bridging the “Communications Gap” between the Public and Private Sector – Making it Easier to do Business with DHS

DHS’ new commercialization outreach efforts center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

If you think about it, there are numerous examples in our professional and private lives where the lack of communication or unclear terminology has created misunderstandings, problems and myriad other issues. As in any worthwhile pursuit, effective communication is critical in the cost-effective and efficient interactions between various parties seeking a mutually beneficial partnership. The U.S. Department of Homeland Security (DHS) is putting into practice the necessary rigor to improve communication that will allow the public and private sectors to work jointly to meet the unsatisfied needs of the DHS in order to protect the Nation.

To this end, the DHS Commercialization Office has developed a number of processes, programs and tools to facilitate the clear articulation of DHS needs (See Figure 1). In that same spirit of working together with the private sector, we recently developed a “Product Realization Chart” (see <https://dhsonline.dhs.gov/portal/jhtml/dc/sf.jhtml?doid=116836>) which is a useful guide to relate concepts and correlate terminology used by both the public and private sector to clearly delineate how science, technology development and product development (terms used in the private sector) are related to basic research, innovation and transition using a Technology Readiness Level (TRL) “backbone” (terms used in the public sector).

Further examination of the Product Realization Chart shows that this resource also provides a stage-gated approach for cost-effective and efficient product development to provide a “discussion framework” useful in private-public sector discussions as well as a template for utilization to develop and communicate agreements. The chart describes the objectives, deliverables and the type of management review necessary to develop and deliver technologies/products/services that meet the specific requirements of the DHS’ operating components (U.S. Coast Guard, FEMA, TSA, CBP, USCIS, U.S. Secret Service and ICE) and its end users such as first responders.

Stage One: Needs Assessment

Needs assessment is the critical first stage of product realization (accomplished via acquisition or commercialization processes) that enables DHS to identify capability gaps and investigate new product/technology/service capabilities. By understanding the specific and detailed requirements of its customers, the DHS Science & Technology Directorate (DHS S&T) conducts market research and technology scans to find and

assess technology-based solutions that could potentially be developed, matured and delivered to DHS end users.

Commercialization programs, processes and tools...

- 1) "Developing Operational Requirements" Guide
- 2) "DHS Implements Commercialization Process" Article
- 3) "Partnership Program Benefits Taxpayers as well as Private and Public Sectors" Article
- 4) SECURE Program and website
- 5) DHS online
- 6) Invited talks to trade conventions, reaching small, medium and large businesses. Efforts also extend to meet with minority, disadvantaged and HUB Zone groups on a regular basis.

Figure 1: Outreach efforts to inform the public on "How to do Business with DHS" is receiving positive feedback from the private sector and media. See the following website for additional information: <https://dhsonline.dhs.gov/portal/jhtml/community.jhtml?index=15&community=S%26T&id=2041380003>

Please note that management reviews for both the public and private sector are required to ensure that exit criteria and deliverables are met when discussing public-private programs like the SECURE Program.

The remainder of the chart shows the various key objectives and deliverables for each major phase of product realization. Entrance at any point of the chart is possible and certainly, the overall objective of many projects currently underway at DHS is to obtain widely distributed products or services (where commercialization is key). DHS also sometimes has unique "custom-like" requirements with lower unit-volume potential (normally using the Acquisition model as shown in Figure 2). It also should be noted that in a basic research program, it may certainly not be possible to generate an ORD, as the objective may be the "exploring uncharted territory" rather than the development of products or services for sale to a particular market. For this reason, a dark box is drawn around Stage 1 to indicate that the Product Realization Chart is a multiple-use chart, rather than a concrete process because it simply offers a framework to visualize several processes, some of which (developing custom or widely distributed products/services) require a Needs Assessment.

Stage Two: Science

At the beginning of the second stage, basic principles are observed and reported, and scientific research begins to be translated into applied research and development (R&D). At this stage, a program sponsor and end user/customer have been identified and the mission needs statement, feasibility study and program management vision have been developed.

Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. In the case of developing products/services, operational requirements analysis has been conducted and operational requirements are applied to functional

requirements. A risk management plan has been developed, a program cost analysis has been completed and a preliminary security assessment has been conducted.

As the technology concept and/or application is formulated, active R&D is initiated that results in an analytical and experimental critical function and/or characteristic proof of concept. This includes analytical studies to physically validate the analytical predictions of separate elements of the technology. A Systems Engineering Management Plan (SEMP), Program Management Plan (PMP) and proof of concept plan are key deliverables and serve as exit criteria for the next stage of product realization.

During the second stage, the private sector normally produces a complete product plan during commercialization that addresses marketing opportunities, financial considerations, design concept and many additional analyses. Sales/Marketing team performs a SWOT (strengths, weaknesses, opportunities, and threats), a scenario analysis and a sales forecast estimate. Research assembles the key IP disclosure submissions. Quality Assurance (QA) generates all safety/standards compliance items, calibration requirements and other quality control specifications.

Management reviews for both the public and private sector are required (in partnership projects or programs) to ensure that exit criteria and deliverables are met.

Stage Three: Technology Development

The third stage of product realization ensues when basic technological components are integrated to establish that they will work together, which is a relatively “low fidelity” analysis when compared with the eventual system. The proof of concept report and functional requirements document have been finalized. The SEMP, Test and Evaluation Master Plan (TEMP), quality assurance plan and other deliverables are revised and updated on a continuous basis.

The basic technological components are then integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. The fidelity of the breadboard technology increases significantly in this case. The Operational Requirements Document (ORD) and CONOPS are better developed. The technology scan and market survey are ongoing during the third stage, and an analysis of alternatives is provided.

Once the component is validated in a relevant environment, the system/subsystem model or prototype is demonstrated in a relevant environment. After successful T&E in a simulated operational environment, a preliminary Technology Transition Agreement (TTA) or a Technology Commercialization Agreement (TCA) is executed as applicable. A program manager is identified and an interoperability assessment is performed.

During this stage, the private sector uses its product plan to conduct a beta design review, produce a detailed supplier list and supplier benchmark, begin writing the user’s manual, develop a service strategy, confirm the risk analysis and review engineering change orders. Manufacturing creates a preliminary manufacturing plan and works with Marketing/Sales to finalize product packaging. Quality Assurance defines regulatory

requirements, prepares a preliminary quality plan and procedure for first prototype testing and designs the inspection tooling.

Management reviews for both the public and private sector are required to ensure that exit criteria and deliverables are met.

Acquisition versus Commercialization

Once a representative model or prototype system, which beyond TRL 5, is tested in a relevant environment, the product realization process splits into two paths that are extraordinarily different as evidenced in Figure 2: Acquisition and Commercialization. Acquisition occurs when a government contractor executes design, development and production, driven by DHS requirements, using DHS funding and under contract to DHS. In this case, the product is then deployed to captive users and the product unit price is determined by cost-based pricing. The contractor's customer is DHS and not the end-user community.

Commercialization, on the other hand, is a private-sector driven activity enterprise that executes design, development and production, driven by market requirements, using private funding and perhaps assisted by DHS technology licenses, standards and grants. The product is then sold as commercial-of-the-shelf (COTS) directly to end users and the product unit price is determined by market-based pricing. The vendor's major customer is the end-user community (e.g. first responders) as well as various private sector markets.

Why is there a need for commercialization? As previously mentioned, DHS requirements, in most instances are characterized by the need for widely distributed COTS products. Oftentimes, the need is for thousands, if not millions of products for DHS' seven operating components and the fragmented, yet substantial first responder end-user market. Figure 2 shows the major differences between a "pure" Acquisition versus "pure" commercialization processes, along with the recently developed and implemented DHS "hybrid" commercialization process.

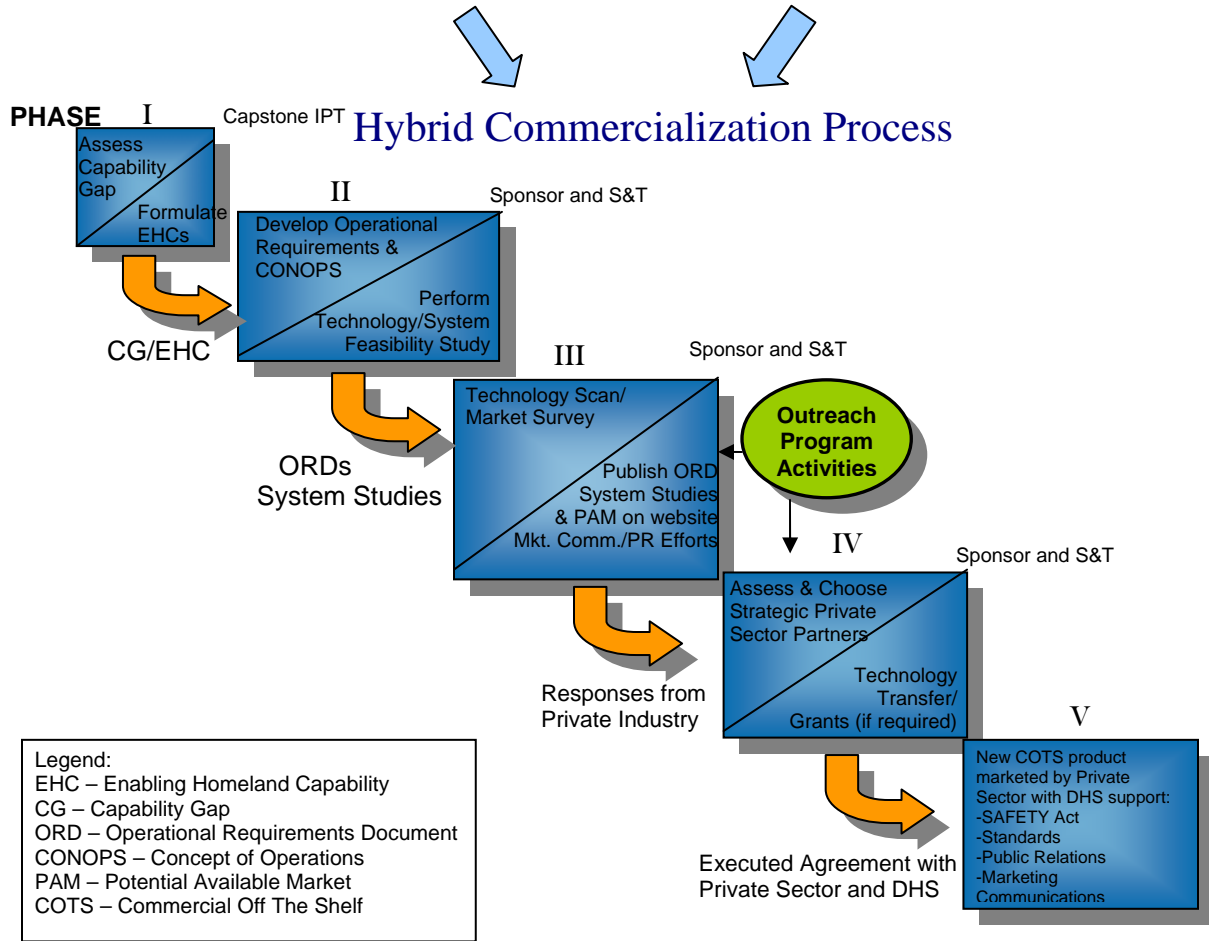
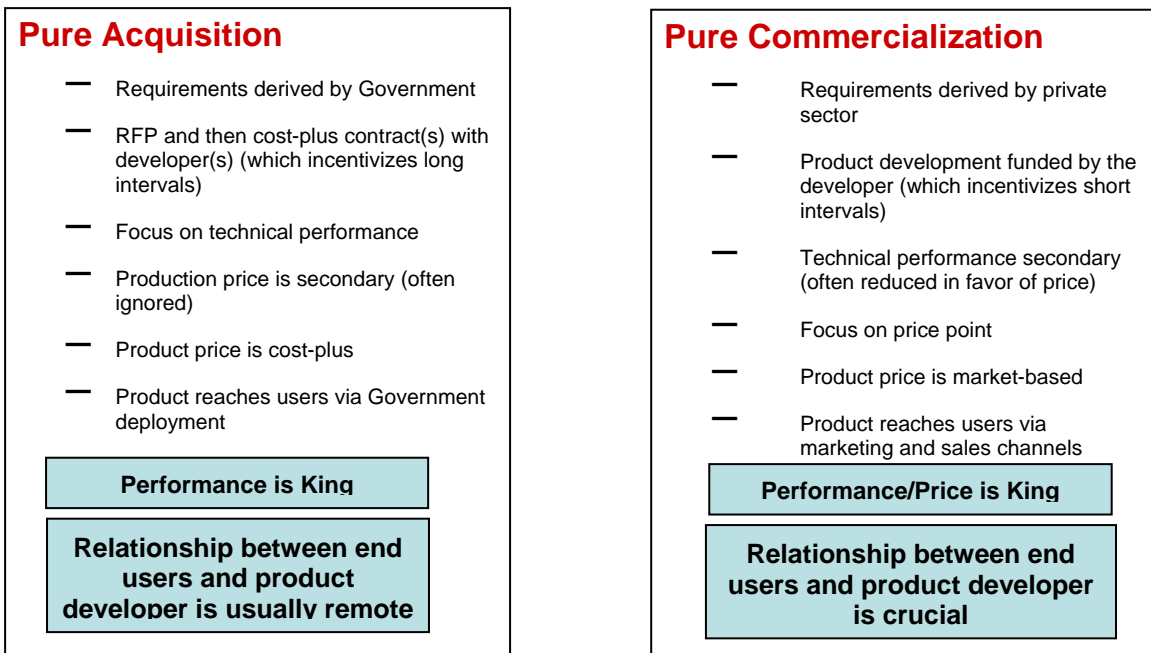


Figure 2: Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system development and the resultant hybrid model implemented by DHS.

Figure 3 delineates the overall description of DHS' new commercialization model and its first private sector outreach program called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program to develop products and services in a private-public "win-win" partnership, recently approved in June 2008 by DHS and described in detail at www.dhs.gov/xres/programs/gc_1211996620526.shtm. Briefly, the SECURE Program is based on the premise that the private sector has shown that it is willing and able to use its own money, resources, expertise and commercialization experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and money to such activities if and when an attractive business case can be made related to large revenue/profit opportunities that certainly exist at DHS and its ancillary markets to participate in the advancement of DHS commercialization efforts. The private sector requires two things from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s). Once this information is posted to the SECURE Program website, small, medium and large companies are open to generate their own business cases and pursue possible participation in the program.

A New Model for Commercialization...

- Develop Operational Requirements Documents (ORDs)
- Assess addressable market(s)
- Publish ORD and market assessment on public DHS web portal, solicit interest from potential partners in a way that is open to small, medium and large businesses
- Execute no-cost (CRADA-like) agreement with multiple private sector entities and transfer technology and/or IP(if necessary)
- Develop supporting grants and standards as necessary
- Assess T&E findings after product is developed to assure DHS and ancillary markets that product meet its published specifications
- New Commercial-Off-The-Shelf (COTS) product marketed by private sector with DHS support

SECURE Program



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized third-party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal to provide confidence to potential customers at DHS and its ancillary markets that product(s) meet or exceed their published specifications in reference to their actual performance.

Figure 3: Step-by-step guide to the commercialization process developed and adopted by DHS with a brief summary of the popular SECURE Program.

In order to provide DHS operating components, the first responder community and other end-users with products that meet their specific requirements, the SECURE program provides a vehicle by which private sector entities can offer products and/or conduct product development geared specifically toward meeting those needs. Private sector entities currently possessing a technology/product/system rated at a Technology Readiness Level TRL-5 (i.e. applied or advanced R&D) or above that potentially closes a defined DHS capability gap by addressing detailed operational requirements supplied by DHS-S&T on the SECURE Program website will have the opportunity enter into a CRADA-like agreement to continue development of their technology/product/system to TRL-9 (i.e. fully field deployable product) at their expense. The CRADA-like agreement also provides private sector entities with the assurance that DHS-S&T will verify their recognized independent third-party test(s) of a given technology/product/system. A Cooperative Research and Development Agreement (CRADA) is a written agreement between a private company and a government agency to work together on a project¹.

Stage Four: Product Development

After DHS determines whether the Acquisition or the Commercialization process is appropriate, the fourth stage commences and the system prototype is demonstrated in an operational environment. S&T and the end user/customer have begun to develop a final transition plan and updates have been made to the operational and/or functional requirements document. Interoperability has been demonstrated and Management Directives (MD) have been reviewed to assure compliance. An operations and maintenance manual has been completed and a security manual has been developed.

Since the technology has been proven to work in its final form and under expected conditions, TRL 8 represents the end of true system development. Technology components are therefore form, fit, and function compatible with an operational system. The operational test report has been completed and a Limited User Test (LUT) Plan has been developed. A training plan has also been developed and implemented.

The actual system is then proven through successful mission operations and the end user fully demonstrates the technology in the CONOPS. All critical documentation has been completed and planning is underway for the integration of the next generation technology into the existing program components.

During the last stage, the private sector focuses on the manufacturing plan and the development effort includes the final design reviews, product prototypes along with documented product test results and other product development deliverables. Sales/Marketing update the marketing plan, the sales and distribution plan, and all sales materials. Manufacturing develops assembly and manufacturing procedures, designs and fabricates manufacturing tooling. Quality Assurances updates the Test Q/A plan and creates the quality plan. They also develop testing procedures, create test and fixture

designs, perform reliability testing on the prototype and design and test the shipping container.

The goal of the private sector during the final stage is to demonstrate product manufacturing according to quality assurance standards while remaining within cost/schedule targets. The development effort concludes with a customer-adopted defect-free product, implemented engineering change orders and a final user's manual. Applications engineering and technical engineering support are then implemented. Sales/Marketing also provides sales training, creates a promotional plan and coordinates literature advertising and public relations. Manufacturing establishes the final manufacturing/assembly routines and procedures, the final manufacturing tooling, and the manufacturing document release and acceptance, then undertakes an analysis for future product cost reduction. Quality Assurance does the final QA and test pooling, prepares the final QA/test procedures, and compiles the manufacturing yield data.

Management reviews for both the public and private sector are required to ensure that the final exit criteria and deliverables are met. Since the actual system has been proven through successful mission operations, the product is then deployed to captive users or sold as COTS directly to end users.

Conclusion

The Commercialization Office has developed a number of processes, programs and tools to clearly articulate the needs of DHS. Outreach efforts are also critical and center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department. Therefore, we have developed a "Product Realization Chart" that serves as a useful guide to relate and correlate terminology used by both the public and private sector in order to develop and deliver required technologies/products that meet the specific operational requirements of the Department of Homeland Security's operating components and its end users such as first responders.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector.

ⁱFor more information on CRADAs, please visit:

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+15USC3710a and
<http://www.usgs.gov/tech-transfer/what-crada.html>.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





Making it Easier to Work with DHS: The Critical Role of Detailed Operational Requirements

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security

September 2008



**Homeland
Security**

Science and Technology

Making it Easier to Work with DHS: The Critical Role of Detailed Operational Requirements

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

In today's dynamic homeland security environment, delivering cost-effective products and services that meet well thought-out detailed requirements is a critical objective for the U.S. Department of Homeland Security (DHS). DHS is composed of many organizational elements with an overriding goal: to enable, support and expedite the mission-critical objectives of DHS' seven operating components – Transportation Security Administration (TSA); U.S. Customs and Border Protection (CBP); U.S. Secret Service, (USSS); U.S. Citizenship and Immigration Service (USCIS); U.S. Immigration and Customs Enforcement (ICE); Federal Emergency Management Agency (FEMA); and the U.S. Coast Guard (USCG). These seven operating components work closely with, support and are supported by a large network of first responders at the state, local and tribal levels. DHS must coordinate, drive and prioritize the detailed needs of this diverse group of operating components and supporting elements, whose missions address a wide variety of terrorist and natural threats to our homeland, in order to maximize the effective use of DHS' resources. Ever changing threat dynamics often require new, innovative-technology based solutions in order to prevent or mitigate the potential effects of current and future dangers. The DHS Science and Technology Directorate (DHS-S&T), works diligently to understand, document and offer solutions to current and anticipated threats faced by our "customers" (DHS operating components and field agents) and our "customers' customers" (first responders and the eighteen infrastructure industrial sectors such as banking, chemicals and communications, etc.).

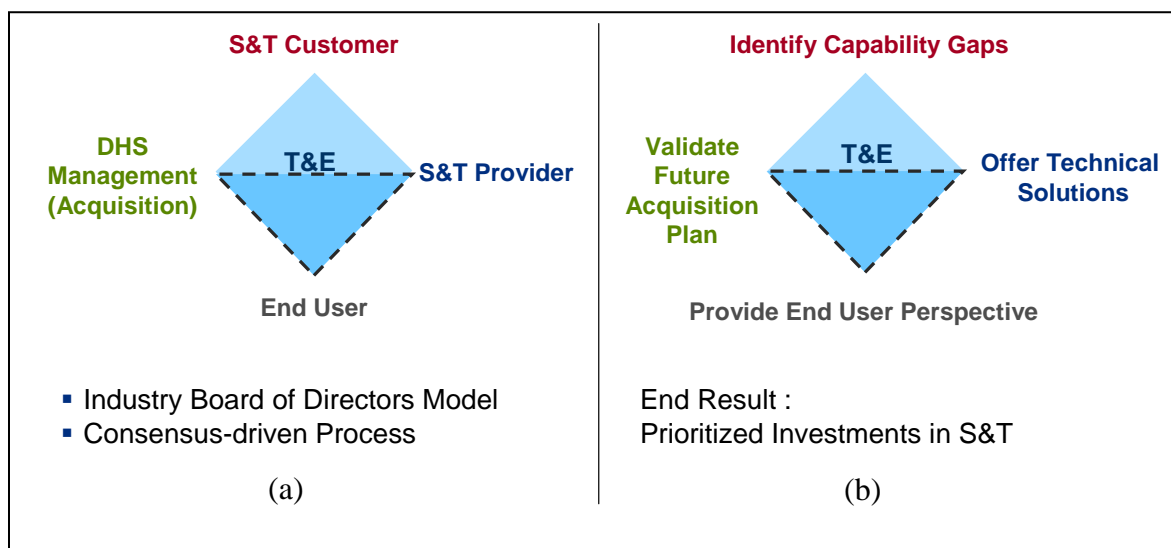
Capstone IPTs and Capability Gaps

DHS-S&T, through the Capstone Integrated Product Team (IPT) process¹, ensures that quality, efficacious products are developed in close alignment with customer needs. The Capstone IPT process is the framework that determines that developed capabilities meet operational needs, analyzes gaps in strategic needs and capabilities, determines operational requirements, and develops programs and projects to close capability gaps and expand mission competencies. This process is a DHS customer-led forum through which the identification of functional capability gaps and the prioritization of these gaps across the Department are formalized. The IPTs oversee the research and development efforts of DHS-S&T and enable the proper allocation of resources to the highest priority needs established by the DHS operating components and first responders.

Capstone IPTs bring together S&T division heads, acquisition partners and end-users (Operating Components, field agents and supporting First Responders – customers of DHS) involved in the Research, Development, Testing and Evaluation (RDT&E) and acquisition activities. Working together, the IPT identifies, evaluates and prioritizes the necessary requirements to complete missions successfully. IPTs also assess the technological and system readiness of products that will ultimately be deployed into the

field. Figure 1 shows the organization of a Capstone IPT. The formation of the IPT at an early stage allows key stakeholders to identify and address critical capability gaps. Each Capstone IPT has a DHS operating component chair or co-chairs. The chair/co-chair, representing the end-users of the delivered Enabling Homeland Capabilities (EHCs), or suite of technologies needed to close a capability gap, engage throughout the process to identify, define and prioritize current and future requirements and ensure that planned technology and/or product transitions and acquisition programs, commercialization efforts and standards development are optimally suited to their operational requirements. Operating components, field agents, first responders and other non-captive end-users with an interest in the core functional areas of an IPT are welcome to participate and contribute throughout the Capstone IPT process.

Figure 1 (a) This diagram shows the structure of the Capstone IPT model with (b) the models' output



functions carried out by each IPT member.

The Capstone IPTs are structured to focus on functional, department level requirements, articulated as capability gaps, and deal with programmatic and technology issues within the six S&T divisions. Capstone IPTs have been created across twelve major Homeland Security core functional areas: Information Sharing/Management, Cyber Security, People Screening, Border Security, Chemical/Biological Defense, Maritime Security, Counter-Improvised Explosive Devices, Transportation Security, Incident Management, Interoperability, Cargo Security and Infrastructure Protection. Each Capstone IPT is chaired by senior leadership from a DHS operating component with needs that correspond to a specific functional area. All DHS operating components with an interest in a particular Capstone IPT are invited to send a representative to participate as an IPT member. See Figure 2 for the captive members for each IPT.

DHS Requirements/Capability Capstone IPTs

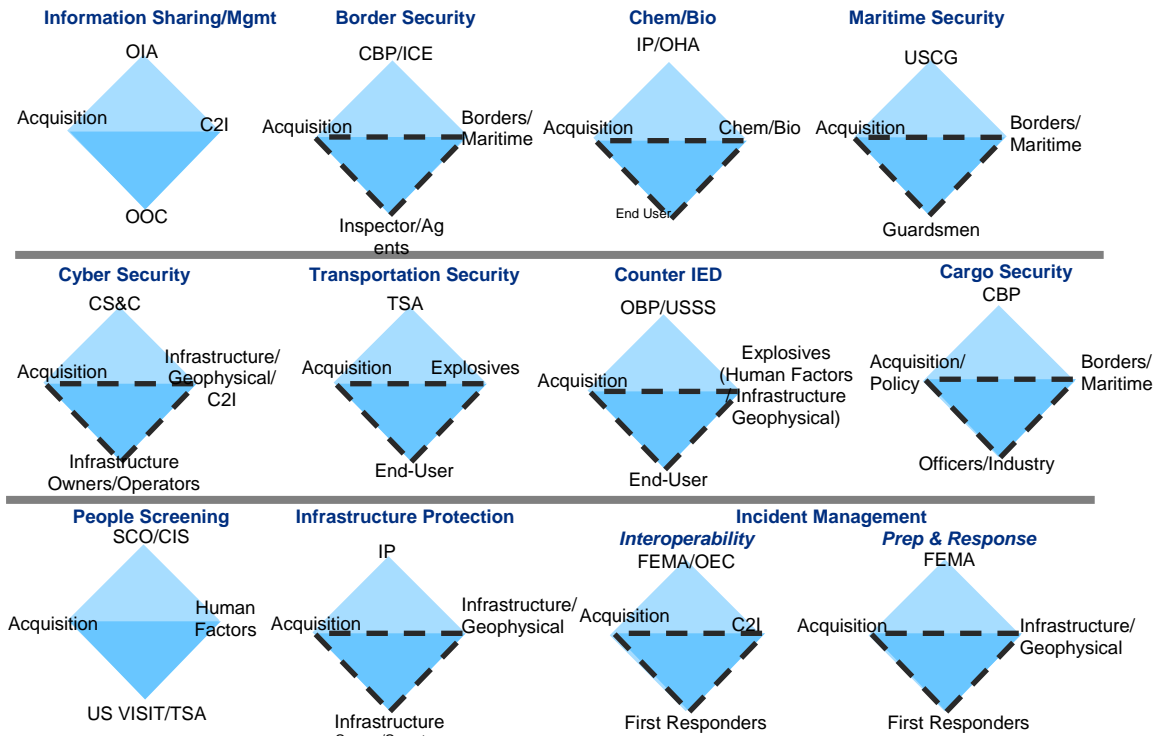


Figure 2. This diagram shows the twelve Capstone IPTs, the DHS operating component, DHS end-user(s), the S&T Division technical provider, and, when applicable, the Acquisition conducted by DHS management.

Technology development is aligned functionally, rather than by operating component “stove pipes,” to allow technologies to be used in support of multiple operating components within DHS. This broad focus aids in reducing the duplication of efforts among various operating components of DHS. In order to achieve greater insight into the facets that comprise each Capstone IPT, Project-IPTs are created to manage specific project areas within a functional area. For example, Border Officer Tools and Safety, and Container Security are Project-IPTs for the Border Security and Cargo Security Capstone IPTs, respectively. Project-IPTs consist of several subject matter experts who are responsible for clarifying the capability gaps derived from the Capstone IPTs and for developing detailed operational requirements with the operating components for the systems that will comprise the EHCs. The Project-IPTs work closely with DHS customers, through an Operational Requirements Document (ORD), to define clearly the specific requirements that must be met in order for a technological solution to address a given problem. Integration of these products into systems forms the EHCs for use by the customers. All DHS agencies are responsible for integrating and fielding the technology deliverables into operational systems scheduled for delivery to their operating component.

Beyond Capability Gaps...

Capstone IPTs generate several outputs that guide the development and fielding of products, services and systems for the operating components. The primary role of the IPTs is to conduct strategic needs analysis to determine and prioritize the capability gaps that exist within a particular functional area. Capability gaps are broad descriptions of

department level identified mission needs that are not met given current products and/or standards. Capability gaps catalog opportunities for enhanced mission effectiveness or address deficiencies in national capability.

The Capstone IPT process enables our divisions within DHS-S&T to interact regularly with their customer(s) to determine capability gaps. These capability gaps, in many ways, are just the beginning. From a product development standpoint, a capability gap is one of the initial steps in the requirements hierarchy scheme. Additional detailed requirements must be developed to enable the development of a technology or product. In our outreach efforts with the Private Sector, DHS-S&T realizes that we must work with our customers to produce a detailed set of requirements in order to communicate with other operating components and frequently to the private sector, which has the ability to develop products aligned to stated requirements.

Commercialization Model Drives the Need for Detailed Requirements

The U.S. Department of Homeland Security is forging a new paradigm with far-reaching positive consequences for DHS' customers, private sector partners, and U.S. taxpayers through the rapid, cost-effective and efficient development and deployment of products and services to protect the Homeland of the United States. As a recently formed U.S. Federal Government Department (March 6, 2003), DHS is "creating a culture" where public-private sector partnerships, beneficial to both sectors and taxpayers alike, expedite the development of products and services to protect the nation. Recently announced commercialization initiatives like the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program are truly groundbreaking and innovative approaches to foster a mutually beneficial relationship between the public and private sectors by creating an open and freely competitive program accessible by small, medium and large firms to provide potential solutions to DHS requirements. These efforts are a natural extension of the Capstone IPT process.

DHS possesses an "Acquisition Mindset," as do so many government agencies. While the Acquisition model has been, and continues to be, utilized effectively in developing custom, one-off products such as aircraft carriers, it is not particularly germane to a majority of the needs at DHS as well as the first responders (a DHS ancillary market). The timely design, development and deployment of lower priced, widely distributed products for both DHS operating components and the first responder communities represents a critical step in protecting our nation. Recognizing this fact, the Department recently started implementing a "Commercialization Mindset" in order to leverage the vast capabilities and resources of the private sector through an innovative "win-win" private-public partnership called the SECURE Program stressing the need for detailed requirements.

Why is there a need for a commercialization process? DHS requirements, in most instances, are characterized by the need for widely distributed COTS (Commercial-Off-The-Shelf) products. Oftentimes, the need is for thousands, if not millions, of products for DHS' seven operating components and the fragmented, yet substantial first responder market. Figure 3 shows the major differences between a "pure" Acquisition versus "pure" commercialization processes, along with the recently developed and implemented DHS "hybrid" commercialization process.

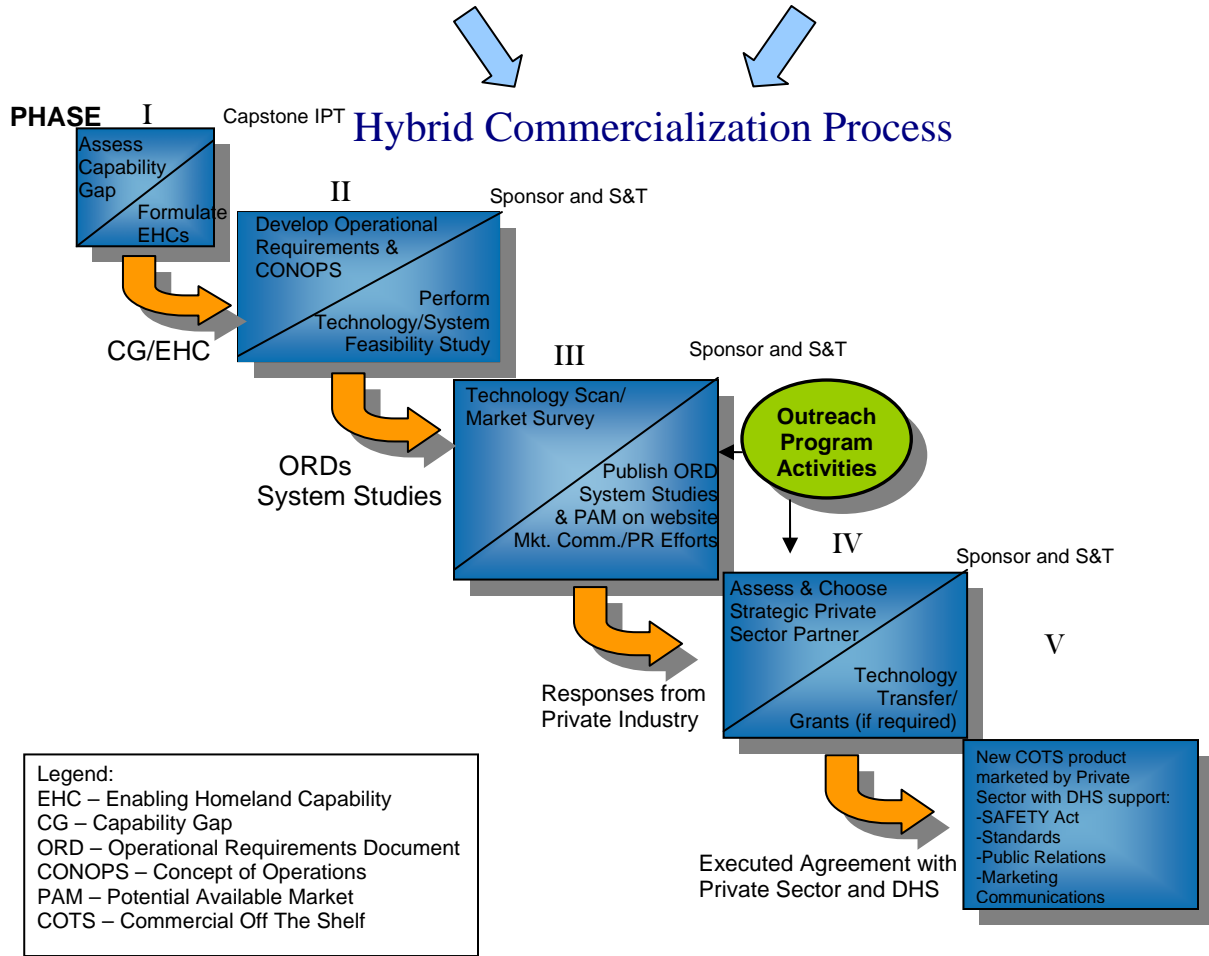
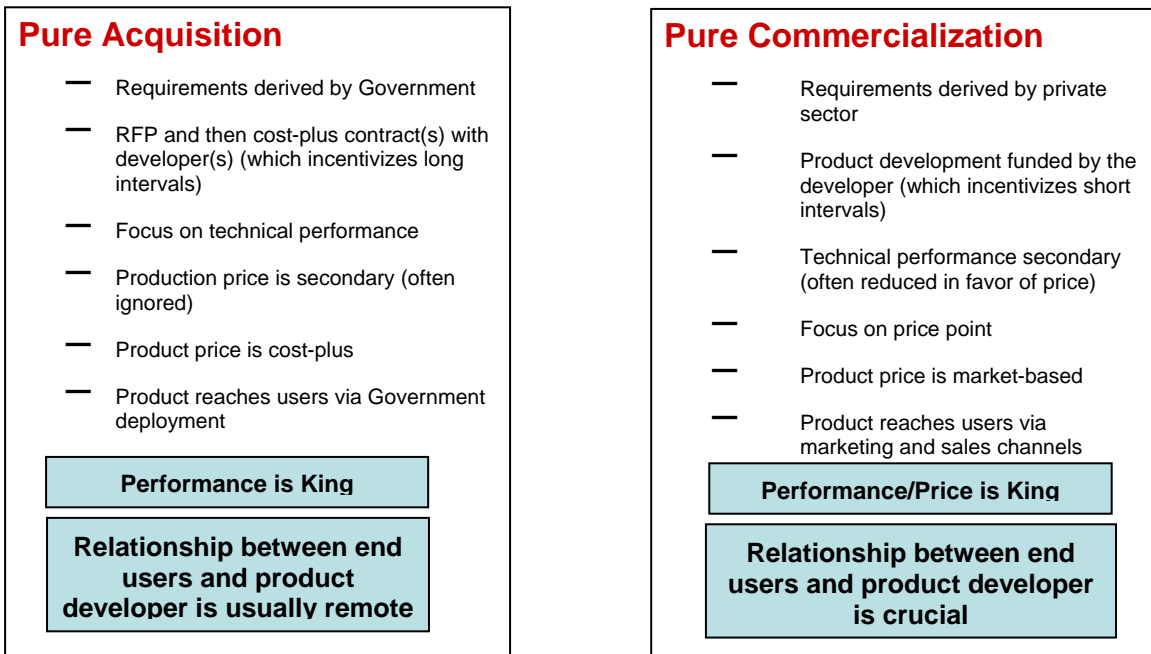


Figure 3: Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system development and the resultant hybrid model implemented by DHS.

Figure 4 delineates the overall description of DHS’ new commercialization model and its first private sector outreach program called the SECURE Program to develop products and services in a private-public “win-win” partnership described in detail at www.dhs.gov/xres/programs/gc_1211996620526.shtm. The SECURE Program is based on the simple premise that the private sector is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and resources to such activities, if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two pieces of critical information from DHS: 1. detailed operational requirement(s), and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in the program.

A New Model for Commercialization...

- Develop Operational Requirements Documents (ORDs)
- Assess addressable market(s)
- Publish ORD and market assessment on public DHS web portal, solicit interest from potential partners in a way that is open to small, medium and large businesses
- Execute no-cost (CRADA-like) agreement with multiple private sector entities and transfer technology and/or IP(if necessary)
- Develop supporting grants and standards as necessary
- Assess T&E findings after product is developed to assure DHS and ancillary markets that product meet its published specifications
- New Commercial-Off-The-Shelf (COTS) product marketed by private sector with DHS support

SECURE Program



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized third-party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal to provide confidence to potential customers at DHS and its ancillary markets that product(s) meet or exceed their published specifications in reference to their actual performance.

Figure 4: Step-by-step guide to the commercialization process developed and adopted by DHS with a brief summary of the popular SECURE Program.

To augment the commercialization process, DHS has undertaken the task of developing an easy-to-use comprehensive guide to assist in developing operational requirements. This guide now enables DHS personnel to articulate, in detail, a given system’s requirements and communicate those needs to both internal and external audiences. This effort addresses a long-standing need for DHS to fully articulate its requirements. Figure 5 clearly shows how an ORD takes a capability gap to “much higher resolution,” a

necessary required if the private sector is to aid DHS in its goal of expediting the development and deployment of cost-effective and efficient widely distributed products.

Requirements Hierarchy (TSA example)

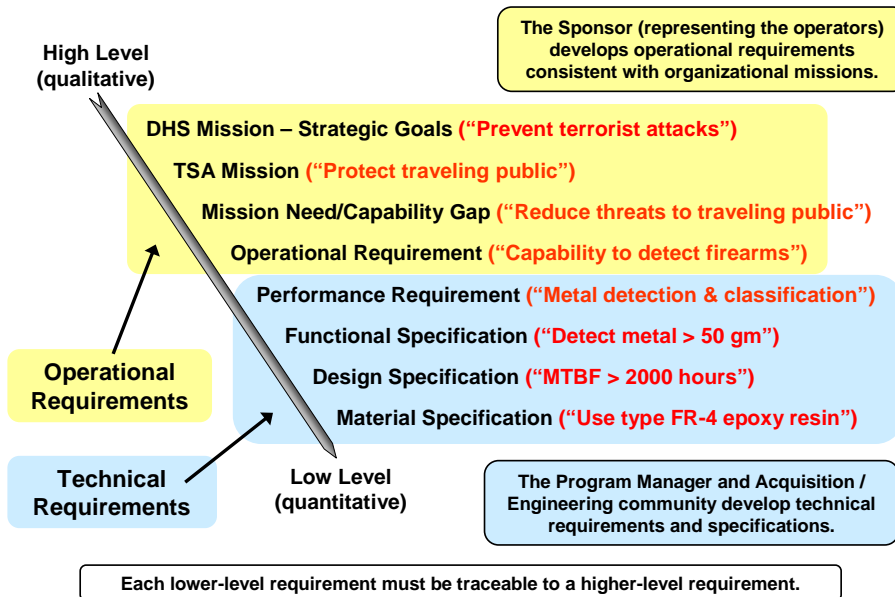


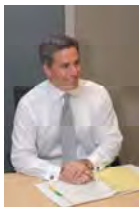
Figure 5. This requirements hierarchy shows the evolution of requirements from a high-level macro set of operational requirements to a low-level micro set of technical requirements. Note that each lower level requirement stems directly from its higher requirement so that all requirements are traceable to the overall DHS Mission.

Early response from groups within DHS, the private sector, and first responders about this guide and programs like SECURE has been very favorable². The Department plans to regularly update its website with Operational Requirements Documents (ORDs) to continually expand this innovative private-public partnership. In addition, as evidenced in Figure 6, the taxpayers, private sector and public sector view programs like this as “win-win-win.”

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Figure 6: The SECURE Program is viewed positively by DHS stakeholders. The success of the program lies in the fact that all participants receive significant benefits.

In conclusion, DHS’ newly created and implemented commercialization process offers long-awaited benefits to the rapid execution of cost-effective and efficient development of products and services to protect our nation and its resources.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security’s first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector.

¹ Kikla, Richard V. and Cellucci, Thomas A. “Capstone IPTs: Even in Government the Customer Comes First,” April, 2008.

² Margetta, R. “S&T Official Working to Move Product Development Out of DHS, Into Private Sector,” Congressional Quarterly Homeland Security. June 27, 2008.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





DHS Global Outreach Efforts: Looking for the Best Technology and Products -- Period.

DHS to leverage international partnerships to find the best technologies and products from around the globe for Homeland Security applications.

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security**

November 2008



**Homeland
Security**

Science and Technology

DHS Global Outreach Efforts: Looking for the Best Technology and Products -- Period.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

The recent establishment of the Commercialization Office at the U.S. Department of Homeland Security (DHS) Directorate of Science and Technology (S&T) has already made a significant impact to ensure that the Department and its members understand the value of commercialization to satisfying the needs of the Department. Commercialization efforts have shown the benefits that the private sector can bring in the efforts to work in a partnership with the Department to leverage the private sector's skills, experience, resources and interest in creating widely distributed products to achieve the goal of developing and deploying high performance products, systems and services critical to the objectives of DHS's seven operating components (TSA, FEMA, Coast Guard, Secret Service, ICE, CBP and USCIS) and first responders. Furthermore, the Department has made a concerted effort to reach out globally to become aware of, assess and work with technologies and products from around the globe because we understand that no one region has complete dominance in technology and product development. In so many ways, science, technology and product development transcend politics and geography. To this end, we have a keen interest in learning about all novel technologies and solutions that are available to meet our requirements.

The Department has recently undertaken the critical step of "socializing" a "commercialization mindset" throughout DHS and the first responder communities. Why is there a need for a commercialization process? DHS requirements, in most instances, are characterized by the need for widely distributed COTS (Commercial-Off-The-Shelf) products. Oftentimes, there is a need for thousands, if not millions, of products for DHS's seven operating components and the fragmented, yet substantial first responder market. Figure 1 shows the major differences between a "pure" Acquisition versus "pure" commercialization processes, along with the recently developed and implemented DHS "hybrid" commercialization process.

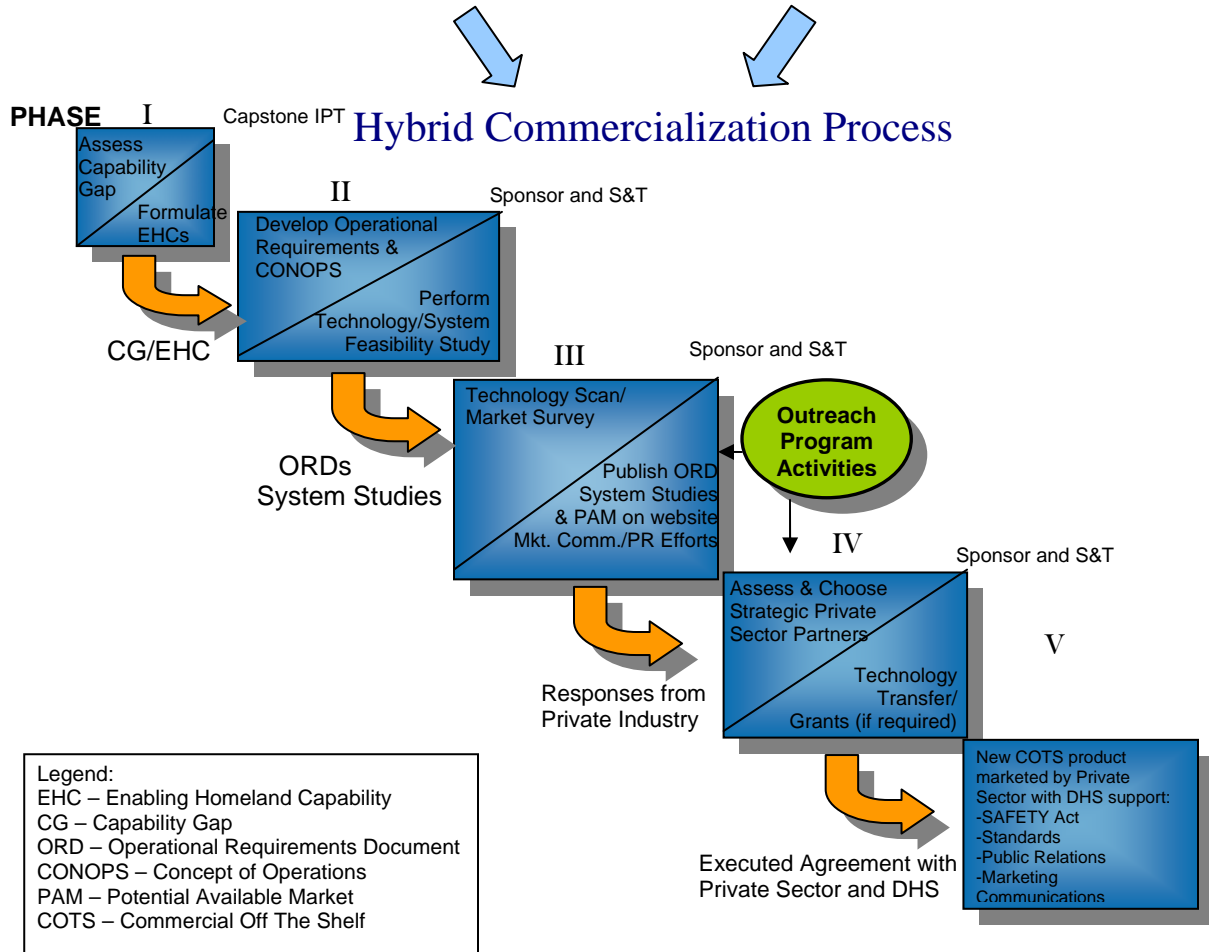
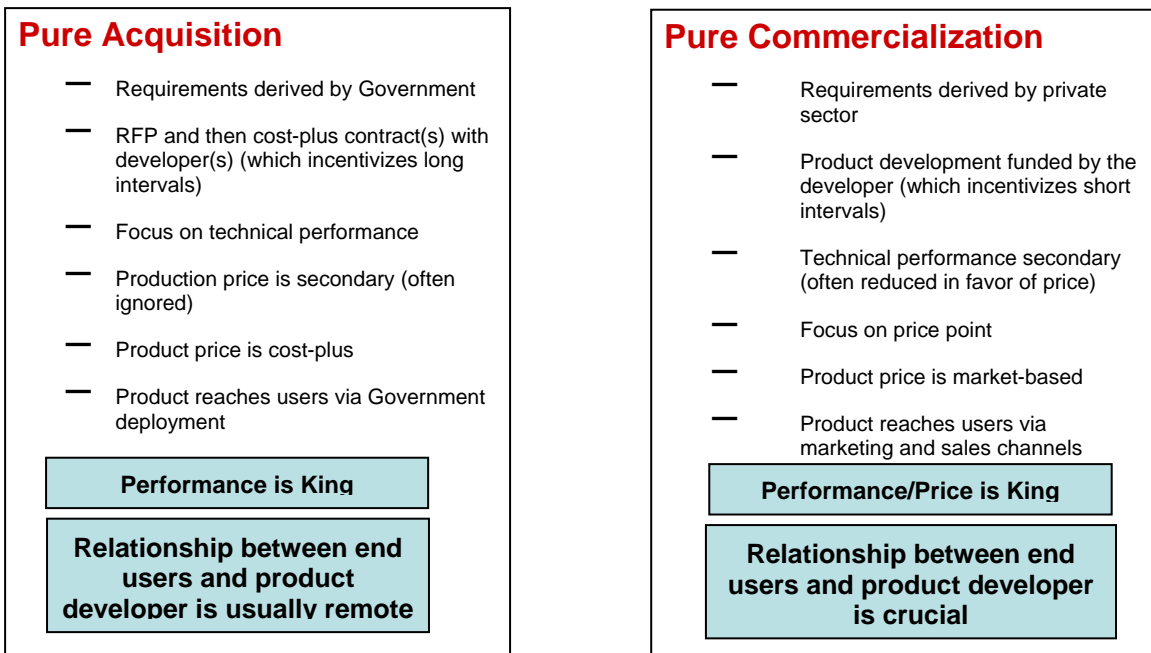


Figure 1: Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system development and the resultant hybrid model implemented by DHS.

Figure 2 delineates the overall description of DHS’s new commercialization model and its first private sector outreach program called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program. The goal of these efforts is to engage private sector companies, from any country, to develop products and services in a private-public “win-win” partnership and described in detail at www.dhs.gov/xres/programs/gc_1211996620526.shtm. Briefly, the SECURE Program is based on the premise that the private sector has shown that it is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and money to such activities if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two things from DHS: 1. detailed operational requirements and 2. a conservative estimate of the potential available market(s). This critical information can then be used to generate a business case for possible private sector participation in the program.

A New Model for Commercialization...

- Develop Operational Requirements Documents (ORDs)
- Assess addressable market(s)
- Publish ORD and market assessment on public DHS web portal, solicit interest from potential partners in a way that is open to small, medium and large businesses
- Execute no-cost (CRADA) agreement with multiple private sector entities and transfer technology and/or IP(if necessary)
- Develop supporting grants and standards as necessary
- Assess T&E findings after product is developed to assure DHS and ancillary markets that product meet its published specifications
- New Commercial-Off-The-Shelf (COTS) product marketed by private sector with DHS support

SECURE Program



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – Abbreviated CRADA document that outlines milestones and exit criteria
- Publication of Results – Recognized third-party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal to provide confidence to potential customers at DHS and its ancillary markets that product(s) meet or exceed their published specifications in reference to their actual performance.

Figure 2: Step-by-step guide to the commercialization process developed and adopted by DHS with a brief summary of the popular SECURE Program.

To augment the commercialization process, DHS has undertaken the task of developing an easy-to-use comprehensive guide to assist in developing operational requirements. This guide now enables DHS personnel to articulate, in detail, a given system’s requirements and communicate those needs to both internal and external audiences. This effort addresses a long standing need for DHS to fully articulate its requirements. A copy of this guide, entitled “Developing Operational Requirements,” has been made publicly available at the previously mentioned website.

Early responses from groups within DHS and in the private sector related to this guide and programs like SECURE have been very favorable¹. The Department plans to regularly update its website with Operational Requirements Documents (ORDs) to continually expand this innovative private-public partnership. In addition, as evidenced in Figure 3, the taxpayers, private sector and public sector view programs like this as “win-win-win.”

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

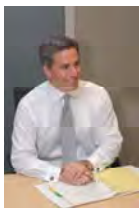
Figure 3: The SECURE Program is viewed positively by DHS stakeholders. The success of the program lies in the fact that all participants receive significant benefits.

It should also be mentioned that we are often asked about the “Buy American Act” and how that could be an issue for a non-American based firm. Simply stated, the Buy American Act is intended to provide a preference for supplies and construction materials that are of domestic (U.S.) origin. The Act does not affect the provision of services. Generally, when the Act applies, the preference takes the form of a pricing advantage in evaluation of offers. Because the negotiation of various treaties and trade agreements, however, supplies, services, and construction of non-domestic origin may be treated as though they are of domestic (U.S.) origin.

Some examples are: (a) For nations who are participants in the World Trade Organization Government Procurement Agreement, U.S. domestic treatment will be given to supplies and services valued at \$193,000 or more and construction valued at \$7.407 million or more; and (b) For NAFTA signatories, supplies of Canadian origin valued at \$25,000 or more and supplies of Mexican origin and services of Canadian and Mexican origin valued at \$64,786 or more, and construction of both nations valued at \$8.422 million or more receive domestic (U.S.) treatment.

In addition, the U.S. has negotiated other Free Trade Agreements (for example, with Australia, Singapore, Chile, and certain Caribbean nations) and a separate agreement with Israel that may use these or other values. The message is that, depending upon the value of the procurement, goods of non-domestic (U.S.) origin may well receive domestic treatment and not be subject to the Buy American Act preference. As you can see, the concept is simple, but the participating nations and dollar values differ. For your specific situation, it is suggested that you consult Part 25 of the Federal Acquisition Regulation, which is at Title 48 of the U.S. Code of Federal Regulations.

As one can observe, there are a plethora of opportunities for global businesses with DHS available to those who possess unique technologies and products. For more information please visit and read the background materials on the SECURE Program at the program’s website: http://www.dhs.gov/xres/programs/gc_1211996620526.shtm



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security’s first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector.

¹ See Cellucci, T. “Opportunities for the Private Sector,” 2008, 43pp. [Available online: http://www.dhs.gov/xres/programs/gc_1211996620526.shtm].

² Margetta, R. “S&T Official Working to Move Product Development Out of DHS, Into Private Sector,” Congressional Quarterly Homeland Security. June 27, 2008.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





Conservative Estimates of Potential Available Market(s)

SECURE Program provides a conservative estimate of the potential available market (PAM) for a given product, technology or service.

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security**

December 2008



**Homeland
Security**

Science and Technology

Conservative Estimates of Potential Available Market(s)

SECURE Program provides a conservative estimate of the potential available market (PAM) for a given product, technology or service.

Thomas A. Cellucci, Ph.D., MBA
 Chief Commercialization Officer
 Commercialization Office
 U.S. Department of Homeland Security

While volumes have been written¹ on effective market sizing and segmentation, the SECURE Program provides a conservative estimate of the potential available market (PAM) for a given system (product or service) which needs to be verified through independent research by a potential commercialization partner.

The DHS commercialization process relies on providing two key pieces of information to potential solution providers in order for them to devote their valuable time, money and resources to develop products and services for use by DHS operating components, first responder communities, critical infrastructure and key resources (CIKR) owner/operators and other stakeholders: 1) a clear and detailed delineation and explanation of the operational requirements, and 2) a conservative estimate of the potential available market for a potential commercialization partner to offer potential solution(s). We have forged the development of Operational Requirements Documents (ORDs) through the publication of several books, training materials and articles to address the first half of this equation, and the following pages of a comprehensive market potential template address the latter.

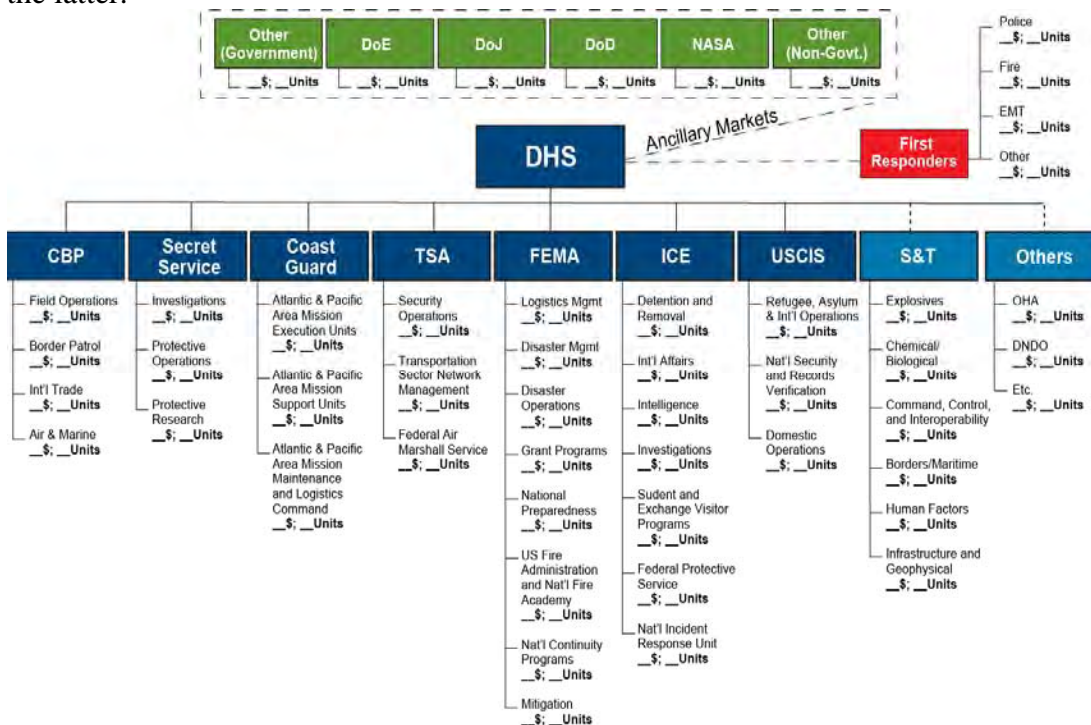
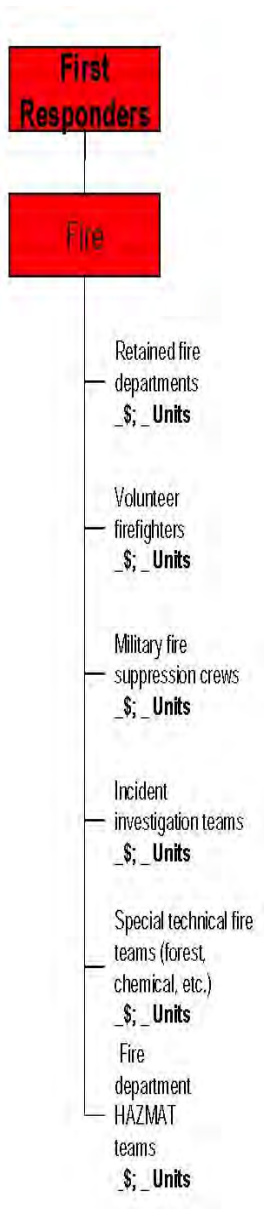


Figure 1 The market potential template maps out many potential available markets to which DHS has direct control and responsibility or acts as a conduit.

It is important to understand not only the detailed operational requirements necessary to provide DHS stakeholders with mission-critical capabilities, but also understand the volume of potential users of these solutions. DHS itself can represent a substantial potential available market; in many instances requiring hundreds, if not thousands of product or service units to address unsatisfied needs. Couple to this the fact that DHS has responsibility for so many ancillary markets (e.g. first responders, critical infrastructure and key resources, etc.) representing large potential available markets, it is evident that substantial business opportunities exist for the private sector as these large pools of potential customers and users represent the “lifeblood” for businesses (see Figure 1). We outline the top level of key players in the public and private sectors. In turn, each “branch” of the template has been further segmented to hone in on detailed opportunities.



For example, in Figure 2 we’re interested in demonstrating the number and scope of various fire fighting sub-segments or applications within the fire fighting market segment. While these groups confront the same basic threat, each sub-segment represents and responds to specific threat profiles requiring different tactics. Similarly, another part of this market revolves around special technical fire teams, which encounter very unique challenges that most fire departments are not expected or ill-equipped to confront, such as widespread forest fires. HAZMAT-capable fire teams may deal with material disposal, incident investigators might not require the same heavy-duty tools that fire crews need, and military fire suppression crews frequently have to battle an inferno that is driven by special propellants (i.e. jet fuel).

The wide variety of requirements within the fire protection and suppression market shows the keen observer just how potentially large this market may be for a given product or service, or demonstrates potential new unsatisfied needs/wants. In addition, rather than limiting a solution provider to offering a given solution to a very specific sub-segment of a given market, this comprehensive template demonstrates the wide variety of market users of a requirements-driven fire fighting solution *platform* that can be potentially tailored to meet the individual and unique needs among the various fire fighting sub-segments. Instead of limiting the solution provider, we hope that our market analysis encourages innovative thinking on the part of the private sector to market a valuable solution because a given need may be shared across both public and private sector communities.

Figure 2 – The chart maps various fire fighting segments.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector.

1. See for example:

- a. Myers, James H. Segmentation & Positioning for Strategic Marketing Decisions. Ohio: South-Western Educational Pub, 1996.
- b. Meer, David, and Daniel Yankelovich. Rediscovering Market Segmentation. Boston: Harvard Business Review, 2006.
- c. Mcquarrie, Edward F. The Market Research Toolbox: A Concise Guide for Beginners. Thousand Oaks: Sage Publications, Inc, 2005

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





Innovative New Partnership Program creates “Wins” for Taxpayers and the Private & Public Sectors

SECURE Program provides the Speed-of-Execution, Cost-Effectiveness, and Efficiency necessary to develop products and services for Homeland Security.

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security**

September 2008



**Homeland
Security**

Science and Technology

Innovative New Partnership Program creates “Wins” for Taxpayers and the Private & Public Sectors

SECURE Program provides the Speed-of-Execution, Cost-Effectiveness and Efficiency necessary to develop products and services for Homeland Security.

Thomas A. Cellucci, Ph.D., MBA
 Chief Commercialization Officer
 U.S. Department of Homeland Security

Experienced leaders know that the best types of relationships are those where each participant receives genuine benefit. This simple fact is the basis for a recently announced initiative at the U.S. Department of Homeland Security (DHS) called the SECURE Program. SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) is part of an overall effort at the Department to create a “Commercialization Mindset” by recognizing that while DHS has a limited budget, it does have something much more valuable – a large potential available market comprised of the seven DHS operating components (TSA, CBP, FEMA, ICE, USCIS, USSS and U.S. Coast Guard) and other large ancillary markets such as diverse and substantial first responder markets.

Briefly, the SECURE Program is based on the premise that the private sector has shown that it is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS. They will devote time and money to such activities if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two things from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in a program or project.

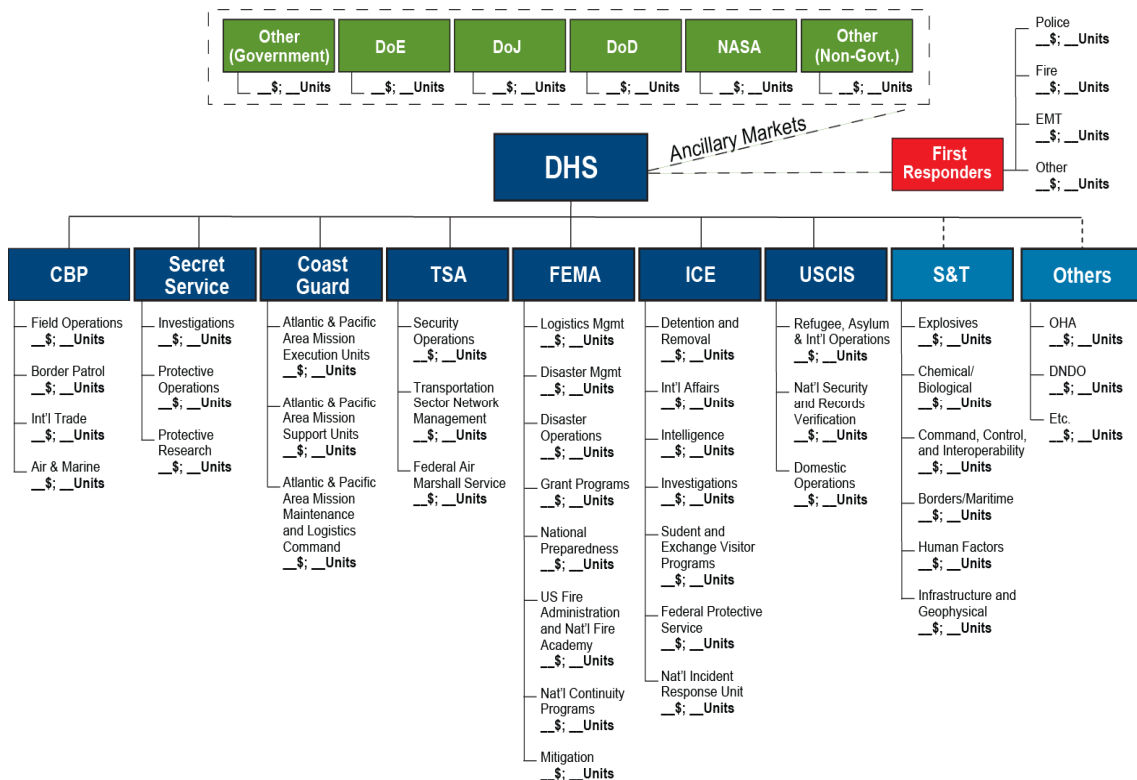


Figure 1: This Market Potential Template is used to estimate the given size of a particular market that DHS has identified as an area requiring new products or services.

This Market Potential Template is used to demonstrate how large (in both dollar and unit volume) a given market is for a particular product or service. Coupled with an Operational Requirements Document (ORD), the private sector receives ample information from DHS to generate a business case for developing a product or service sought after by DHS for its operating components or first responders, whose combined ranks are significant, as delineated in Figure 2.



Figure 2: Homeland Security Presidential Directive Number 8 (HSPD-8) conservatively classifies over 25.3 million individuals as First Responders in the United States alone.

In return for providing this critical information and saving the private sector considerable time and money related to market and business development activities, DHS expects the private sector to offer solutions – utilizing the free market system with open and fair competition – to meet published requirements. Simply stated, the private sector receives significant business opportunities, DHS and its supported entities receive products and services developed at faster execution rates at the private sector’s cost to the benefit of the American taxpayer. See Figure 3 for an overview of the SECURE Program.

SECURE Program

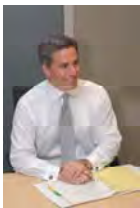
Concept of Operations



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized Third-Party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal
Benefits:
 - ✓ Successful products/technologies share in the imprimatur of DHS
 - ✓ DHS operating components and first responders make informed decisions on products/services aligned to their stated requirements
 - ✓ DHS spends less on programs → Taxpayers win

Figure 3: Brief overview of the SECURE Program' Concept-of-Operations

To learn more about the SECURE Program and other opportunities for the private sector, please visit http://www.dhs.gov/xres/programs/gc_1211996620526.shtm or contact the Commercialization Office at SandT_Commercialization@hq.dhs.gov.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





Commercialization: It's not Business as Usual at the Department of Homeland Security

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security

April 2008



**Homeland
Security**

Science and Technology

Commercialization: It's not business as usual at USDHS
*Robert R. Hooks and Thomas A. Cellucci, U.S. Department of Homeland Security:
Science and Technology Directorate, Washington D.C. 20528*

Introduction:

The U.S. Department of Homeland Security (DHS) is comprised of many organizational elements with a single purpose: to enable, support and expedite the mission critical objectives of DHS' seven operating components – Transportation Security Administration (TSA), U.S. Customs and Border Patrol (CBP), U.S. Secret Service, (USSS), U.S. Citizenship and Immigration Service (USCIS), U.S. Immigration and Customs Enforcement (ICE), Federal Emergency Management Agency (FEMA), and the U.S. Coast Guard (USCG).

In these unprecedented times, there is an immediate need for DHS to provide these operating components with the products and services they require, using efficient and cost-effective product development methods. DHS is working proactively to attract the private sector to develop, produce, test and evaluate products that meet the requirements of DHS operating components and first responders.

Why would the private sector be inclined to develop products at their own expense? This initiative's high probability for success lies in the following principles and guidelines:

1. DHS operating components determine clearly-defined capability gaps and operational requirements that can be addressed effectively with Commercial-Off-The-Shelf (COTS) items.
2. The private sector wants access to large potential available markets (PAMs) that comprise the DHS operating components and ancillary markets as it enables a presumably strong business opportunity.
3. Taxpayer cost savings will be realized by the "win-win" private-public sector partnership. Figures 2 and 3 respectively outline a market potential template and private sector outreach process of the critical elements to attract the private sector's interest in partnering with DHS.

"Win-Win" Strategic Partnerships

One often-overlooked vehicle to cost-effectively and efficiently commercialize technology is the formation of a win-win strategic partnership. The relationship between the public and the private sectors can be mutually beneficial in many ways, as each has something of value that the other desires. DHS has substantial potential available markets and direct access to the operating requirement of its large "customer base" as well as detailed information on the unmet needs and wants of ancillary market customers found in state, local and tribal communities.

Requirements development is one of the cornerstones of the commercialization process. DHS' Science & Technology Directorate (S&T) develops clear, detailed operational requirements documents (ORDs) and intends to publish them on what would be a public web portal accessible by the private sector entities who believe they have the ability to meet those published requirements. Further benefits that DHS has to offer

private sector entities come in the form of grants and Small Business Innovative Research (SBIR) programs.

Conversely, the private sector has skills, expertise, capital, established sales channels and the integrated marketing programs necessary to produce and distribute technically advanced products. The private sector appreciates a conservative estimate of the potential available markets within DHS operating component and/or ancillary markets, as well as clear, detailed operational requirements. With these two items in hand, the private sector can verify supplied estimates and generate business cases to determine if it is feasible to conduct research and development to develop and distribute products or services. This relationship enables substantial benefits given the ever-changing nature of the needs of established and potential new security applications. The private sector will need to continue its innovation as DHS adjusts to address new, emerging threats.

Synchronization:

The execution of a radically different methodology to develop, produce and distribute new products for use by DHS operating components does not come without its challenges. For many years, the U.S. government was indoctrinated and accustomed to the acquisition process of commissioning a custom-made product or service to perform a specific objective. The government would oversee the creation of the requirements, concept and technology development, system capability development, testing and evaluation, and production and deployment – paying for each step of the process. The concept of transferring responsibility of many of the steps in the process to the private sector ultimately removes control by the government. Not only is this a new way of thinking about developing and procuring products, it necessitates clear and precise communications between the public and private sectors.

In its new commercialization model, S&T acts as a facilitator between its customers, DHS' operating components and ancillary markets, and the private sector entities potentially developing products. S&T must work with its valued customers in the creation of ORDs as well as conduct market surveys and technology scans to ensure that needed technical capabilities and/or products exist within firms accessible for distribution of these ORDs. Oftentimes, private sector entities have products in development that are closely aligned with current homeland security capability gaps. In these situations, it is important to determine the exact level of development for the product.

As previously stated, clear and precise communications are paramount. To that end, the lexicon of product development was different in the public versus private sectors (see figure 4). Notice that DHS utilizes Basic Research, Innovation, and Transition nomenclature with Technology Readiness Levels as a “backbone” language, while the private sector utilizes Science, Technology Development, and then Product Development as the phases of developing a product from a concept. In order to ensure effective communications, the Technology Readiness Levels (TRL) model is used to standardize communication for all parties involved (see Figure 5). With the TRL system in use, all parties are able to assess quickly the development stage of a given product and determine an anticipated timeline for product deployment.

Open and Fair Competition leads to Cooperative New Product Development:

Once DHS has fulfilled its obligation to create realistic ORDs, conducts technology scans and market surveys to ensure that capabilities exist, the department would then post pertinent requirement information on the proposed publicly available, open access website. This web portal would be the vehicle by which private sector entities can engage DHS to find capability gaps for which solutions exist or can be produced quickly and efficiently. Given this information, private sector entities could to develop or enhance a given product or service in cooperation with S&T to enable or improve upon currently fielded DHS solutions. Close alignment with the detailed requirements are critical in this process.

In theory, in order for a company to be considered by S&T for cooperative development, it should be able to:

1. Demonstrate they possess technology at TRL-5 (i.e. applied or advanced R&D) or above and possess the resources to invest in the commercialization of its technology to TRL-9 (i.e. fully field deployable product);
2. Propose a technology development effort that has clear and substantial alignment with published S&T requirements; and

A simple, straightforward and binding agreement could then be executed whereby the private sector entity will detail milestones with dates to develop its technology to a TRL-9 state (if not already at that level). Once the private sector entity has successfully achieved TRL-9, it will perform independent third-party testing and evaluation (T&E) on the product to ensure it meets all required previously agreed-upon specifications. S&T then would review and evaluate the accuracy of the third-party T&E and publish its factual findings on the proposed Web site. The free market system should yield several companies producing similar products as is often seen in commercial markets. DHS customers and ancillary markets stand to benefit from this system.

Measurable Results:

The ultimate goal of any commercialization initiative is to produce products that are better, faster and less expensive compared to what is currently on the market. S&T hopes to leverage the private sector's endless pursuit of this idea and marry it with the vast demands created by an organization whose mission is to protect a nation. S&T has a critical role acting as the facilitator between sets of markets and a willing and able private sector looking for large, stable markets to purchase and use advanced technologies. A program like this should result in a demonstrable increase in the quality and quantity of technologies, products and services to assist not only DHS in carrying out its mission objectives, but customers engaged in many other related security applications. It is indeed expected that taxpayers will observe a significant and demonstrative increase in the amount of private sector funding used for the timely development of new and reliable products to help thwart the threat of terrorism.

Conclusion:

The U.S. Department of Homeland Security Science & Technology Directorate is forging a new paradigm that can have far-reaching positive consequences for its customers, private sector partners, and U.S. taxpayers through the rapid, cost-effective and efficient development and deployment of products and services to protect the United

States. The relatively recent formation of DHS (its fifth anniversary was on March 1, 2008) is advantageous in many ways, particularly in that it enables flexible and forward thinking in its long-term goals and processes. Our commercialization initiatives are a groundbreaking and innovative approach to foster a mutually beneficial relationship between the public and private sectors, both of whom stand to benefit greatly from this new partnership created in open and free competition. The future of this initiative looks bright; we have already experienced an overwhelmingly positive response to the initial private sector outreach. S&T will continue to monitor and measure the benefit this program stands to provide.

Acknowledgements:

The authors would like to express their sincere appreciation for all of the valuable assistance by Mr. Mark P. Protacio in the preparation of the materials used in this paper.



Robert R. Hooks is the Director of Transition at the U.S. Department of Homeland Security’s Science and Technology Directorate (DHS S&T) in Washington, D.C. and recently accepted the position of Deputy Assistant Secretary of Weapons of Mass Destruction and BioDefense of the DHS Office of Health Affairs in Washington, D.C.



Thomas A. Cellucci, Ph.D., MBA is currently the Science & Technology Directorate’s first Chief Commercialization Officer in Washington, D.C. He has spent the vast majority of his career as a senior executive and board member in high technology firms in the private sector.

FIGURES

Fig. 1: Capstone IPT Process

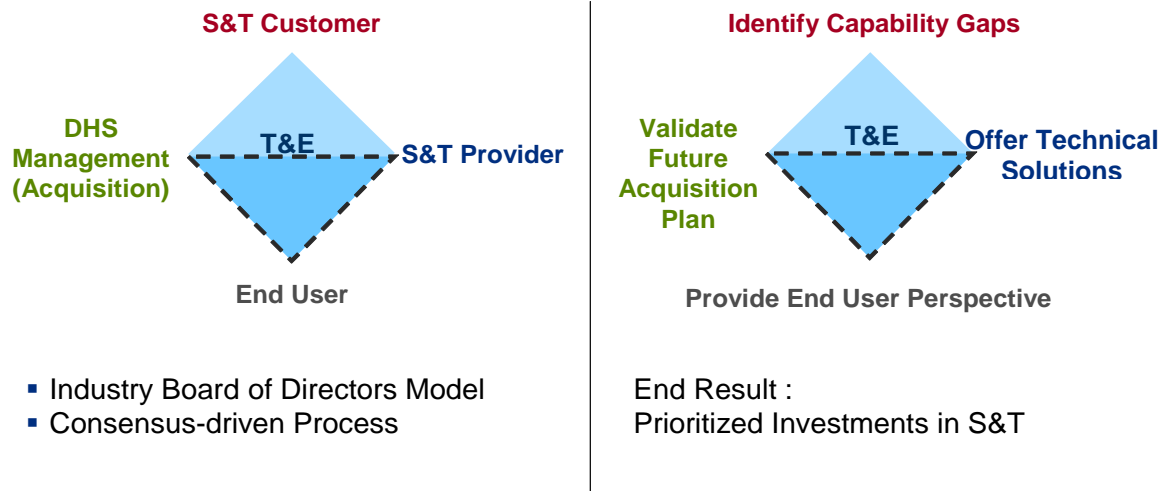


Fig.1 – This graphical representation shows the Capstone IPT (Integrated Product Team) process implemented at S&T that enables all stakeholders to participate actively in identifying and discussing the *Capability Gaps* germane to a specific functional area, such as people screening. S&T works with its customers, pertinent end-users and DHS organizational entities to delineate operational requirements to start a process to close identified capability gaps.

Fig. 2: Market Potential Template

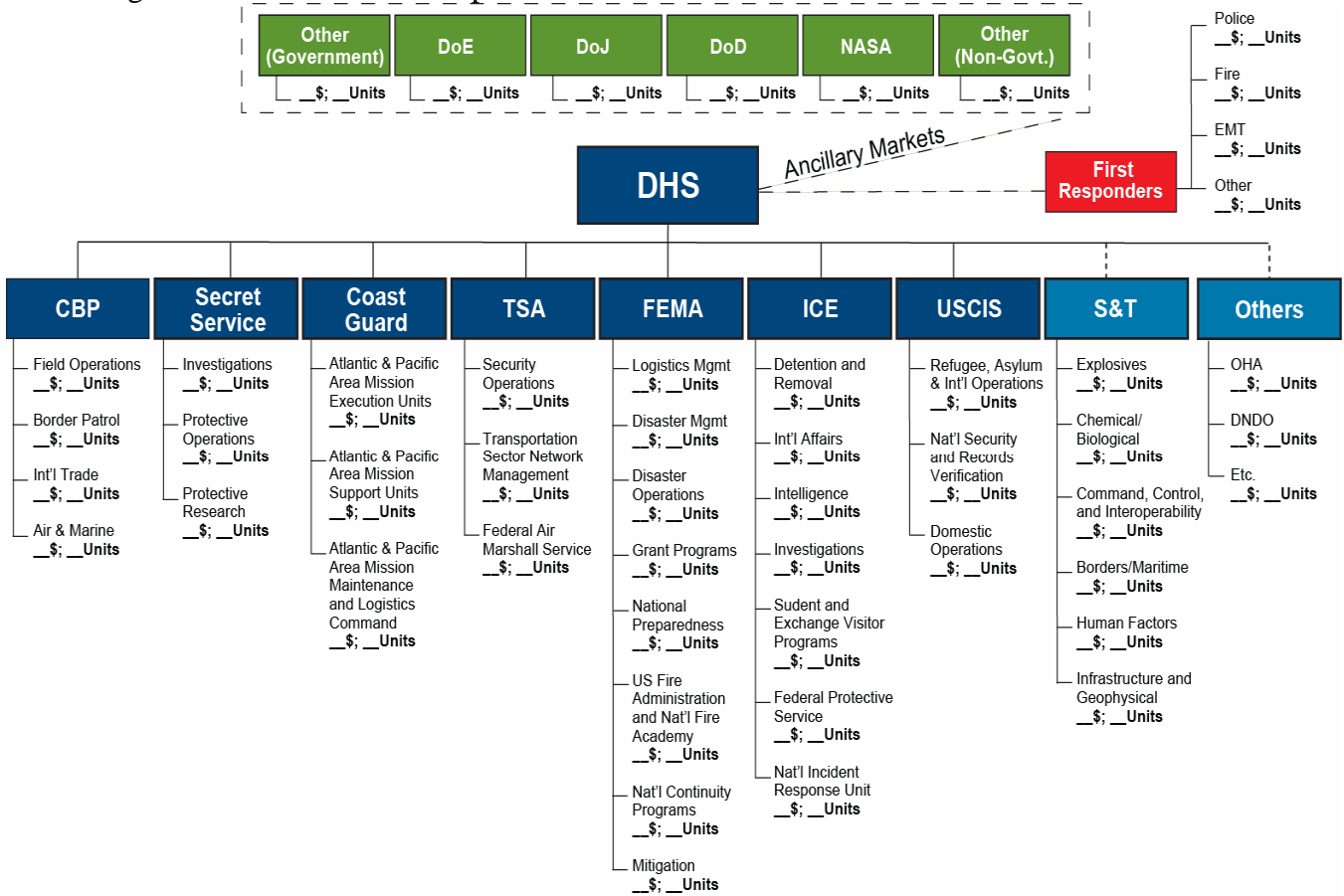
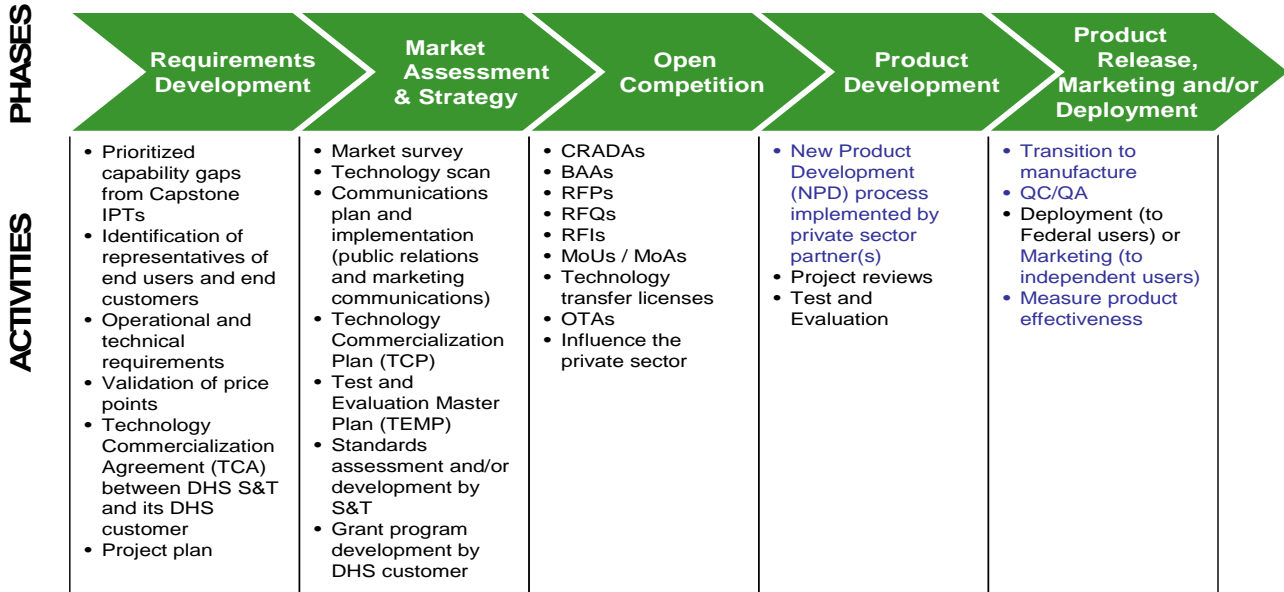


Fig. 2 – This graphic shows a market potential template used to conservatively estimate the DHS market segment by operating components, as well as demonstrate how DHS is a conduit to other large ancillary markets.

Fig. 3 Private Sector Outreach Process

Private Sector Outreach Process

Requirements Identification through Product Release



Legend: Black text = Government activities
 Blue Text = Private-sector activities

Fig.3 – The Private Sector Outreach Process outlines the steps and procedures undertaken to develop and deploy a product or service from capability gap identification to product deployment.

Fig. 4: Lexicon differences

Correlation: DHS and Private Sector

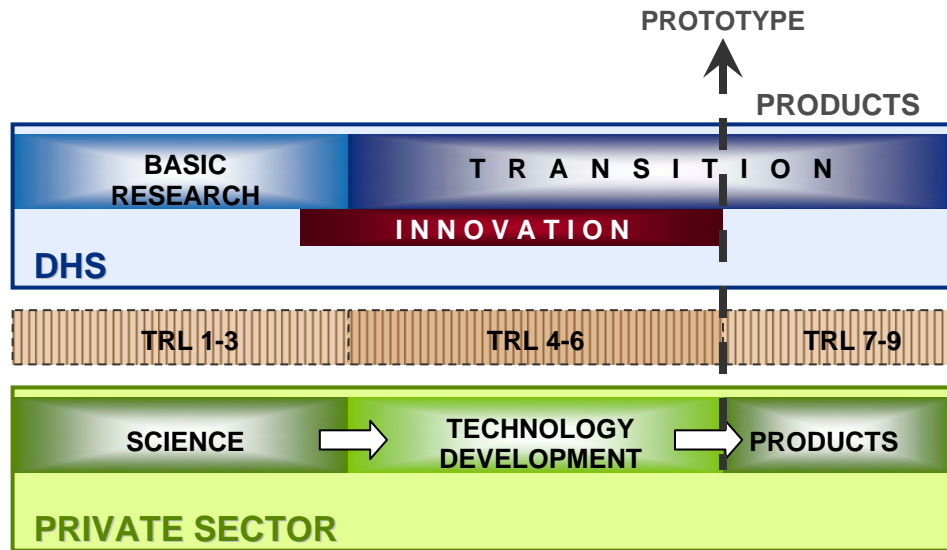


Fig. 4: This chart shows the correlation between the various nomenclatures to delineate differing levels of product development. The Technology Readiness Levels (TRL) serves as a standardized lexicon for enhanced communications.

Fig. 5: Technology Readiness Levels

TRLs are NASA-generated and Used Extensively by DoD

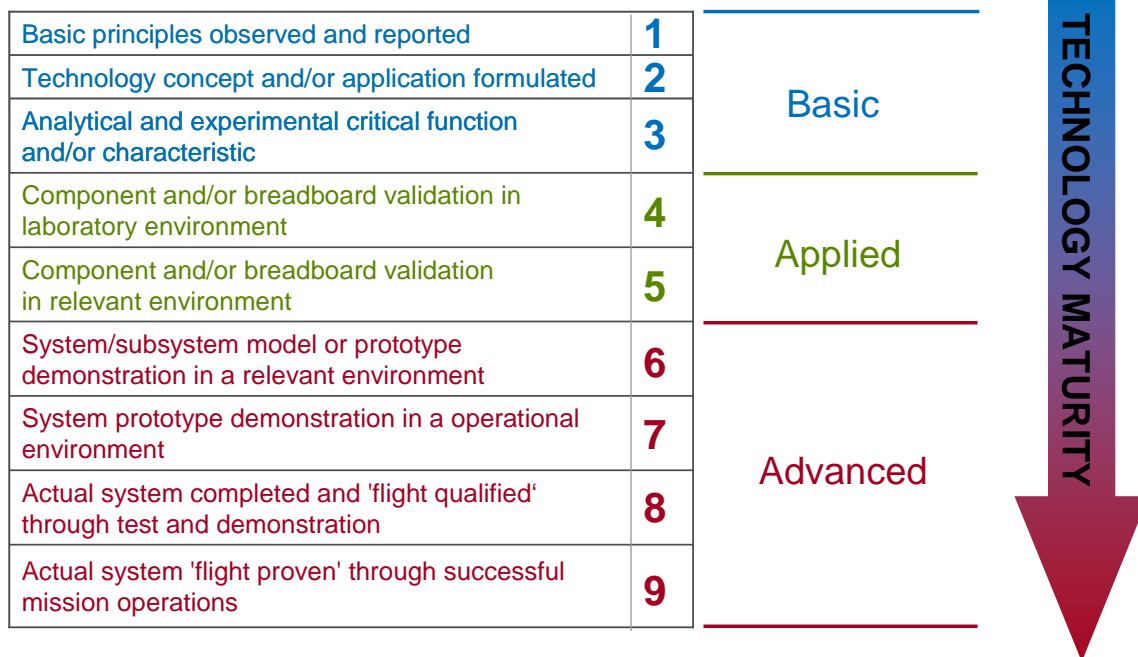


Fig. 5 – TRLs are used to assign a numerical value to a corresponding stage in a technology’s development and maturity. This system of standardization is useful to communicate effectively between entities that may have used varying technology-maturity lexicons.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reaches out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





Innovative Commercialization Process delivers Cost-Effective and Efficient Product Development at DHS with Unparalleled Speed-of-Execution

**The SECURE Program produces a “Win” for Taxpayers and the Private
and Public Sectors.**

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security**

November 2008



**Homeland
Security**

Science and Technology

Innovative Commercialization Process delivers Cost-Effective and Efficient
Product Development at DHS with Unparalleled Speed-of-Execution
SECURE Program produces a “Win” for Taxpayers and the Private & Public Sectors

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security

It is well known that the U.S. Department of Homeland Security (DHS) has faced several challenges attempting to amalgamate 22 disparate organizations into a cohesive organization with a unified mission and culture in its short five-year existence. Those familiar with merger and acquisition activities realize that while integration of organizations poses difficulties, it also represents opportunities to infuse new processes and values into the newly created organization. Through both a “bottom-up” and “top-down” approach, DHS has been successful in developing, socializing and now implementing an innovative commercialization framework within DHS that has started to gain traction with the seven DHS operating components (TSA, FEMA, CBP, ICE, USCIS, USSS and U.S. Coast Guard) and other organizational elements of DHS. The creation of a “Commercialization Mindset” has caught the attention of DHS managers and employees and has been embraced by senior management because of its apparent and significant benefits for the Department’s internal and external activities.

Why is there a need for a commercialization process? DHS requirements, in most instances, are characterized by the need for widely distributed COTS (Commercial-Off-The-Shelf) products. Oftentimes, the need is for thousands, if not millions, of products for DHS’ seven operating components and the fragmented, yet substantial first responder market. Figure 1 shows the major differences between a “pure” Acquisition versus “pure” commercialization processes, along with the recently developed and implemented DHS “hybrid” commercialization process.

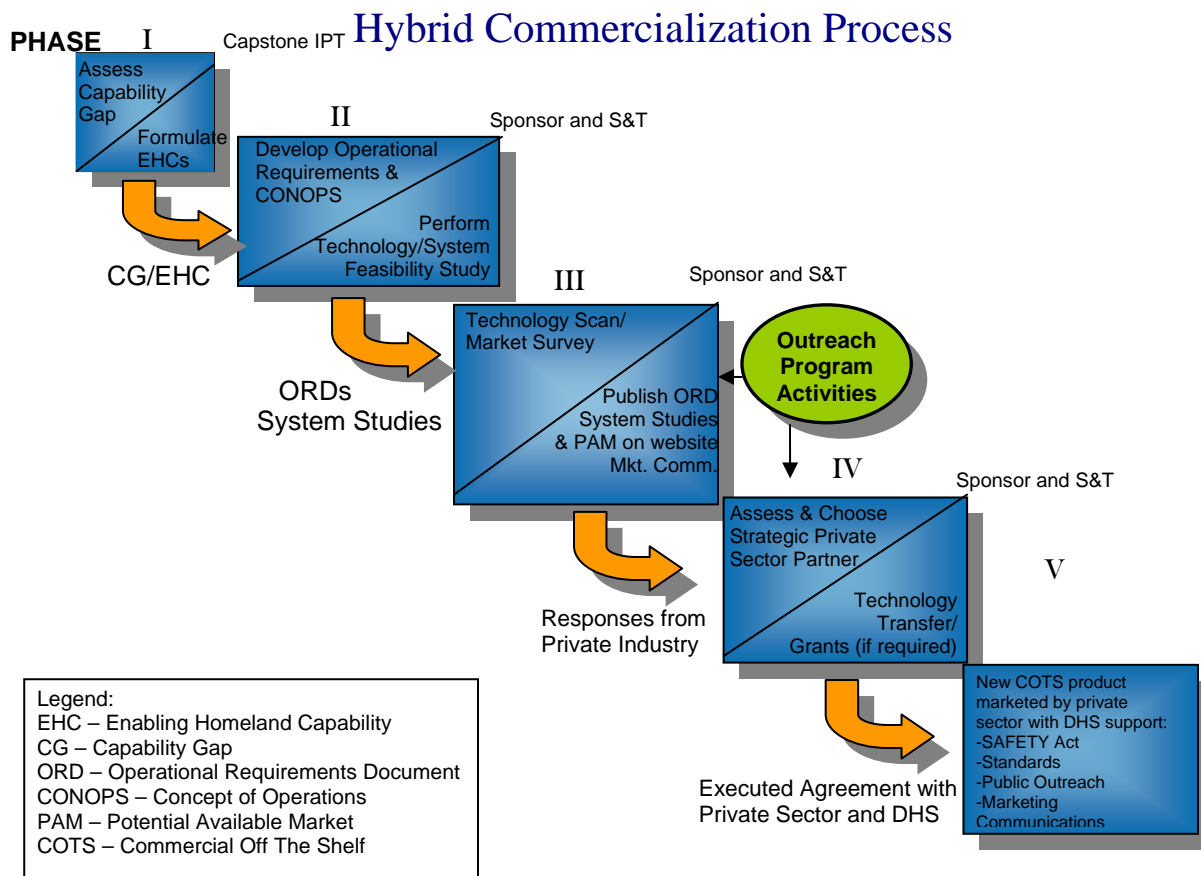
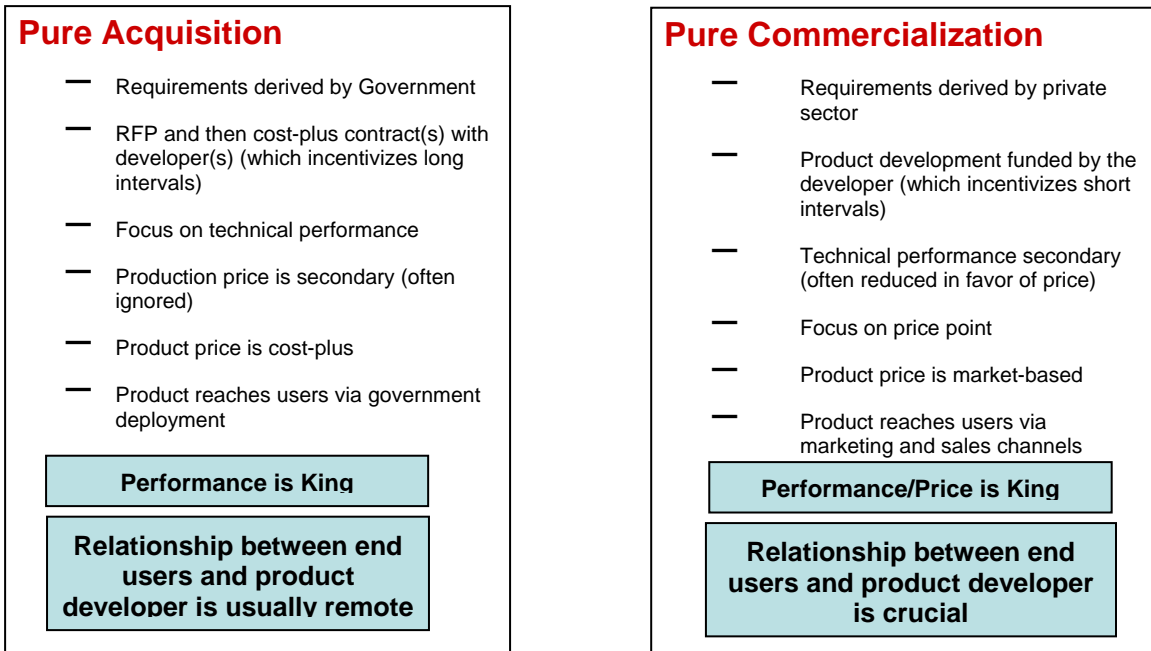


Figure 1: Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system development and the resultant hybrid model implemented by DHS.

Figure 2 delineates the overall description of DHS’ new commercialization model and its first private sector outreach program called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program to develop products and services in a private-public “win-win” partnership, recently approved in June 2008 by DHS and described in detail at www.dhs.gov/xres/programs/gc_1211996620526.shtm. Briefly, the SECURE Program is based on the premise that the private sector has shown that it is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and money to such activities if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two things from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in the program¹.

A New Model for Commercialization...

- Develop Operational Requirements Documents (ORDs)
- Assess addressable market(s)
- Publish ORD and market assessment on public DHS web portal, solicit interest from potential partners in a way that is open to small, medium and large businesses
- Execute no-cost (CRADA-like) agreement with multiple private sector entities and transfer technology and/or IP(if necessary)
- Develop supporting grants and standards as necessary
- Assess T&E findings after product is developed to assure DHS and ancillary markets that product meet its published specifications
- New commercial-off-the-shelf (COTS) product marketed by private sector with DHS support

SECURE Program



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized third-party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS Web portal to provide confidence to potential customers at DHS and its ancillary markets that product(s) meet or exceed their published specifications.

Figure 2: Step-by-step guide to the commercialization process developed and adopted by DHS with a brief summary of the SECURE Program.

To augment the commercialization process, DHS has undertaken the task of developing an easy-to-use comprehensive guide to assist in developing operational requirements. This guide now enables DHS personnel to articulate, in detail, a given system’s requirements and communicate those needs to both internal and external audiences. This effort addresses a long standing need for DHS to fully articulate its requirements.

Early response from groups within DHS and in the private sector related to this guide and programs like SECURE has been very favorable². The Department plans to regularly update its website with Operational Requirements Documents (ORDs) to continually expand this innovative private-public partnership. In addition, as evidenced in Figure 3, the taxpayers, private sector and public sector view programs like this as “win-win-win.”

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Figure 3: The SECURE Program is viewed positively by DHS stakeholders. The success of the program lies in the fact that all participants receive significant benefits.

In conclusion, DHS’ newly developed and recently implemented commercialization process offers long-awaited benefits to the rapid execution of cost-effective and efficient development of products and services to protect our nation and its resources.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector.

¹ See Cellucci, T. "Opportunities for the Private Sector," 2008, 43pp. [Available online: http://www.dhs.gov/xres/programs/gc_1211996620526.shtm].

² Margetta, R. "S&T Official Working to Move Product Development Out of DHS, Into Private Sector," Congressional Quarterly Homeland Security. June 27, 2008.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





Speed-of-Execution in Government?

You bet.

DHS' recently announced and piloted SECURE Program has the potential to significantly increase product development cycles by establishing an innovative "win-win" private-public sector partnership.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security

October 2008



**Homeland
Security**

Science and Technology

Speed-of-Execution in Government? You Bet.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security

Those who have responsibility for a private company realize that execution alone is not sufficient for success – rather, it is the speed-of-execution that dictates sustainable success, as markets and technologies evolve more quickly than ever. One normally does not associate speed-of-execution with the public sector – in fact, quite the opposite. But consider the following questions: Where would speed-of-execution be more important than in an area such as homeland security? What could be done to increase the speed-of-execution related to the development of products and services to protect our nation?

These vexing questions were the basis of the conception of a program to expedite the delivery or transition of products and services to the U.S. Department of Homeland Security’s operating components (FEMA, TSA, CBP, ICE, USCIS, USSS and U.S. Coast Guard) and ancillary DHS markets such as the first responder communities.

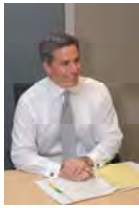
A recently announced and piloted program has the potential to significantly increase product development cycles by establishing an innovative “win-win” private-public sector partnership. This new initiative at DHS is called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program. It is part of an overall effort to create a “Commercialization Mindset” by recognizing that while DHS does not have a large budget (such as the Department of Defense, for example), it has something much more valuable. The seven DHS operating components and the fragmented, yet substantial first responder (police, fire, emergency medical, etc.) communities offer large potential available markets.

This Market Potential Template (See Figure 1) is used to demonstrate how large (in both dollar and unit volume) a given market is for a particular product or service. Coupled with an Operational Requirements Document (ORD), the private sector receives ample information from DHS to generate a business case for developing a product or service sought after by DHS for its operating components or the more than 25 million first responders across the nation. (See Figure 2).

In return for providing this critical information and saving the private sector considerable time and money related to market and business development activities, DHS expects the private sector to offer solutions – utilizing the free market system with open and fair competition – to meet published requirements. Simply stated, the private sector receives significant business opportunities, DHS and its supported entities receive products and services developed at faster execution rates at the private sector’s cost to the benefit of the American taxpayer. See Figure 3 for an overview of the SECURE Program.

To learn more about the SECURE Program and other opportunities for the private sector, please visit http://www.dhs.gov/xres/programs/gc_1211996620526.shtm or contact the

Commercialization Office at SandT_Commercialization@hq.dhs.gov.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector.

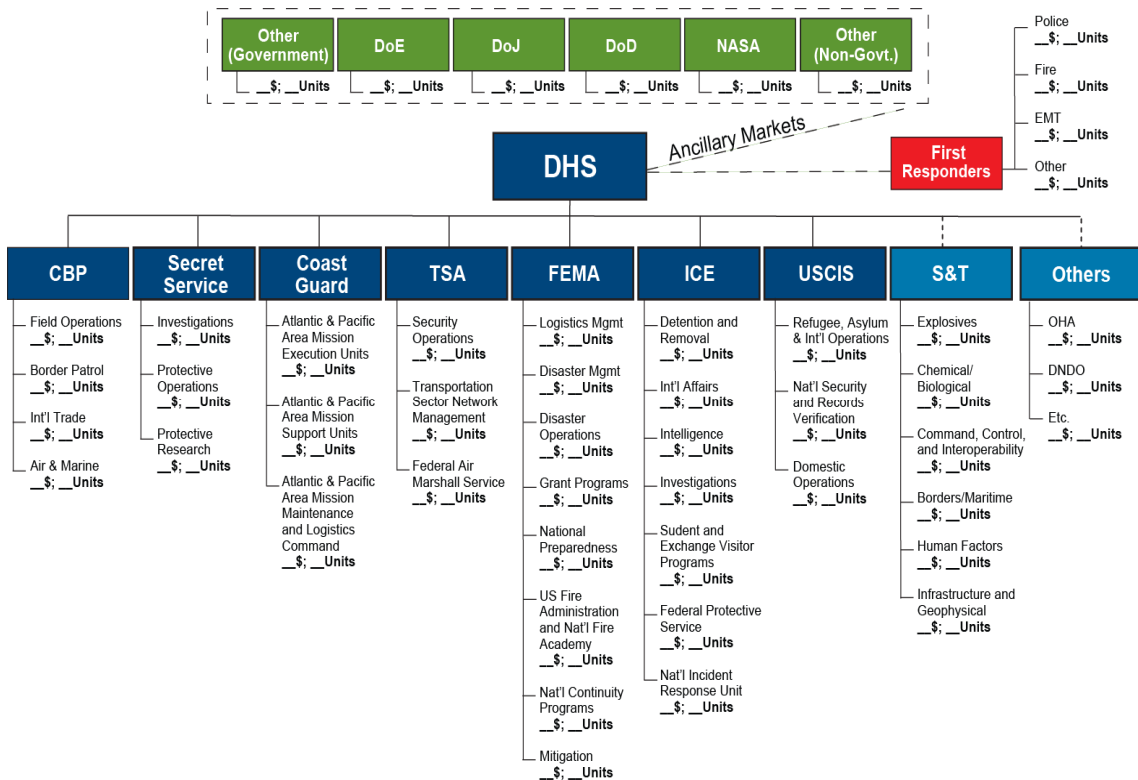


Figure 1: This Market Potential Template is used to estimate the given size of a particular market that DHS has identified as an area requiring new products or services.



Figure 2: Homeland Security Presidential Directive Number 8 (HSPD-8) conservatively classifies over 25.3 million individuals as First Responders in the United States alone.

SECURE Program Concept of Operations



- Application – Seeking products/technologies aligned with posted DHS requirements
 - Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
 - Agreement – One-page CRADA-like document that outlines milestones and exit criteria
 - Publication of Results – Recognized Third-Party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal
- Benefits:

- ✓ Successful products/technologies share in the imprimatur of DHS
- ✓ DHS operating components and first responders make informed decisions on products/services aligned to their stated requirements
- ✓ DHS spends less on programs → Taxpayers win.

Figure 3: Brief overview of the SECURE Program' Concept-of-Operations

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





DHS Makes Transition from Acquisition to Commercialization

DHS' newly developed and recently implemented commercialization process offers long-awaited benefits for the rapid execution of cost-effective and efficient development of products and services to protect our nation and its resources.

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security**

August 2008



**Homeland
Security**

Science and Technology

DHS Makes Transition from Acquisition to Commercialization

Key to Cost Effective and Efficient Product Development Allows All Stakeholders to Win

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security

It is undeniable that the U.S. Department of Homeland Security (DHS) – like many government agencies – possesses a deeply ingrained “Acquisition Mindset.” While the Acquisition model has been utilized effectively in developing custom, one-off products such as aircraft carriers, it is not particularly germane to the vast majority of needs at DHS – namely, the development of lower priced, widely distributed products for both DHS operating components (TSA, FEMA, CBP, ICE, USCIS, USSS and U.S. Coast Guard) and ancillary markets such as the first responder communities. Recognizing this fact, the Department recently developed and started implementing a “Commercialization Mindset” in order to leverage the vast capabilities and resources of the private sector through innovative “win-win” private-public partnerships.

DHS has faced several challenges attempting to amalgamate 22 disparate organizations into a cohesive organization with a unified mission and culture. Those familiar with merger and acquisition activities realize that while integration of organizations poses difficulties, it also represents opportunities to infuse new processes and values into the newly created organization. Through both a “bottom-up” and “top-down” approach, DHS has been successful in developing, socializing and now implementing an innovative commercialization framework that has started to gain traction throughout the agency. The creation of a “Commercialization Mindset” has caught the attention of DHS managers and employees and has been embraced by senior management because of its apparent and significant benefits to the Department’s internal and external activities.

Why is there a need for a commercialization process? DHS requirements, in most instances, are characterized by the need for widely distributed COTS (Commercial-Off-The-Shelf) products. Oftentimes, the need is for thousands, if not millions, of products for DHS’ seven operating components and the fragmented, yet substantial first responder market. Figure 1 shows the major differences between a “pure” Acquisition versus “pure” commercialization processes, along with the recently developed and implemented DHS “hybrid” commercialization process.

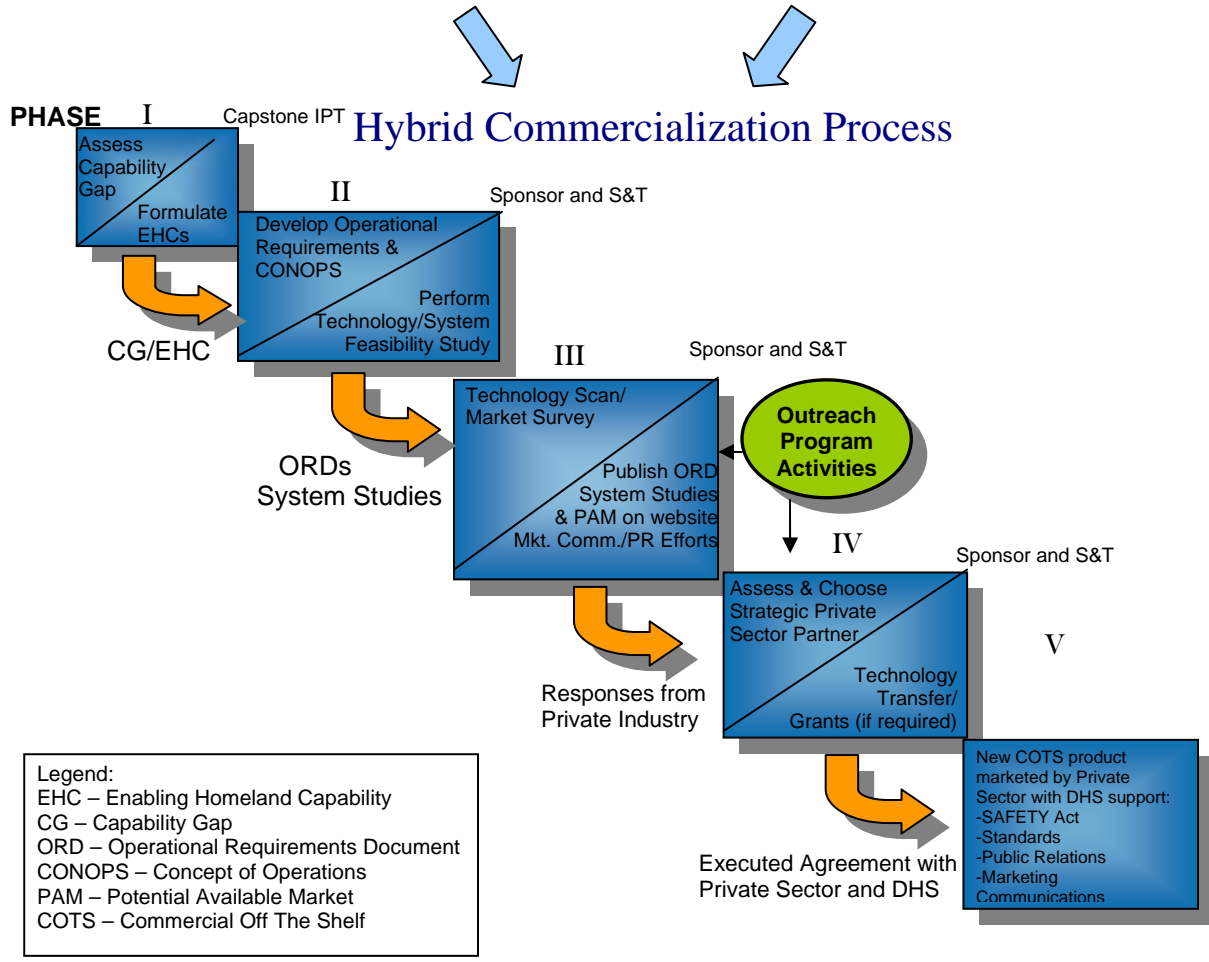
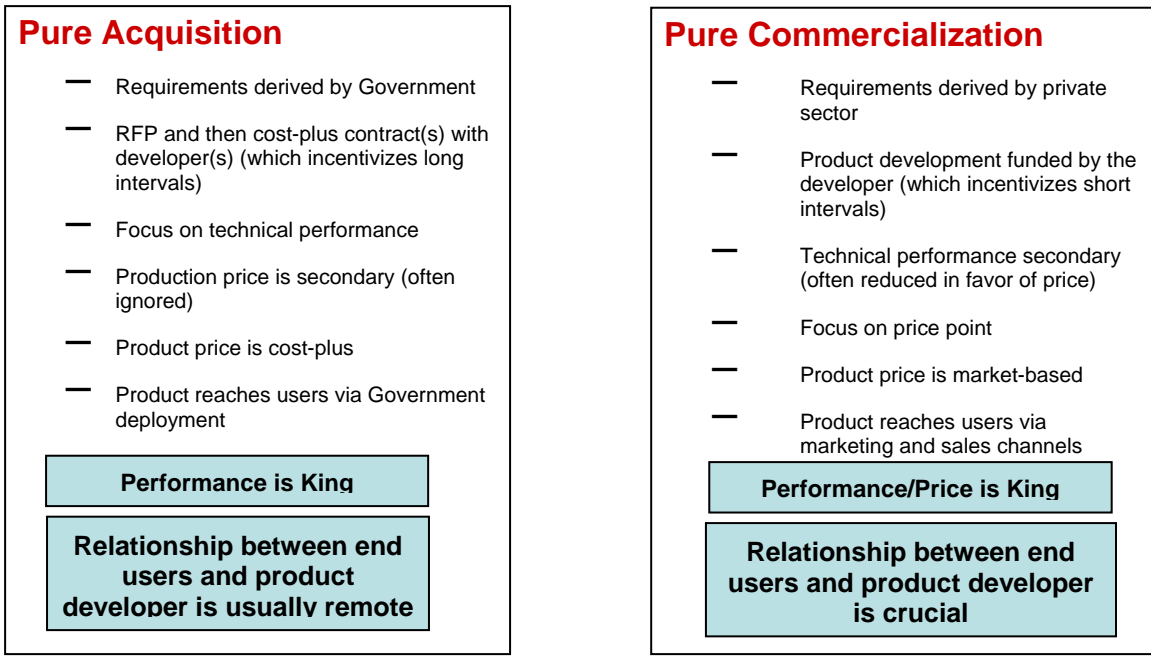


Figure 1: Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system development and the resultant hybrid model implemented by DHS.

Figure 2 delineates the overall description of DHS’ new commercialization model and its first private sector outreach program called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program to develop products and services in a private-public “win-win” partnership, recently approved in June 2008 by DHS and described in detail at www.dhs.gov/xres/programs/gc_1211996620526.shtm. Briefly, the SECURE Program is based on the premise that the private sector has shown that it is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and money to such activities if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two things from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in the program.

A New Model for Commercialization...

- Develop Operational Requirements Documents (ORDs)
- Assess addressable market(s)
- Publish ORD and market assessment on public DHS web portal, solicit interest from potential partners in a way that is open to small, medium and large businesses
- Execute no-cost (CRADA-like) agreement with multiple private sector entities and transfer technology and/or IP(if necessary)
- Develop supporting grants and standards as necessary
- Assess T&E findings after product is developed to assure DHS and ancillary markets that product meet its published specifications
- New Commercial-Off-The-Shelf (COTS) product marketed by private sector with DHS support

SECURE Program



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized third-party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal to provide confidence to potential customers at DHS and its ancillary markets that product(s) meet or exceed their published specifications in reference to their actual performance.

Figure 2: Step-by-step guide to the commercialization process developed and adopted by DHS with a brief summary of the popular SECURE Program.

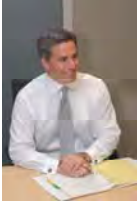
To augment the commercialization process, DHS has undertaken the task of developing an easy-to-use comprehensive guide to assist in developing operational requirements. This guide now enables DHS personnel to articulate, in detail, a given system’s requirements and communicate those needs to both internal and external audiences. This effort addresses a long standing need for DHS to fully articulate its requirements.

Early response from groups within DHS and in the private sector related to this guide and programs like SECURE has been very favorable¹. The Department plans to regularly update its website with Operational Requirements Documents (ORDs) to continually expand this innovative private-public partnership. In addition, as evidenced in Figure 3, the taxpayers, private sector and public sector view programs like this as “win-win-win.”

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Figure 3: The SECURE Program is viewed positively by DHS stakeholders. The success of the program lies in the fact that all participants receive significant benefits.

In conclusion, DHS’ newly developed and recently implemented commercialization process offers long-awaited benefits to the rapid execution of cost-effective and efficient development of products and services to protect our nation and its resources.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector.

¹ See Cellucci, T. "Opportunities for the Private Sector," 2008, 43pp. [Available online: http://www.dhs.gov/xres/programs/gc_1211996620526.shtm].

² Margetta, R. "S&T Official Working to Move Product Development Out of DHS, Into Private Sector," Congressional Quarterly Homeland Security. June 27, 2008.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





The Capstone IPTs and Beyond...

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security
Science & Technology Directorate

Richard V. Kikla
Director Of Transition
U.S. Department of Homeland Security
Science & Technology Directorate

December 2009



**Homeland
Security**

Science and Technology

The Capstone IPT and Beyond...

Richard V. Kikla and Thomas A. Cellucci of the Science and Technology Directorate, U.S. Department of Homeland Security, Washington, D.C.

Advances in science and technology continue to spur the development of new and innovative products focused on the homeland security market. As this market place expands, it becomes increasingly important for homeland security personnel to assist in guiding product development to match their various needs. Delivering these customer-driven products and technologies is a primary objective for the U.S. Department of Homeland Security (DHS). Among the challenges facing DHS is how to gather and refine the needs and requirements of its various stakeholders, who represent a wide variety of mission spaces and operating environments, in a cost-effective and efficient manner.

The Department was created from the Homeland Security Act of 2002 and became an organization of twenty-two disparate entities combined with a common vision: to enable, support and expedite the mission-critical objectives of DHS' seven operating components – Transportation Security Administration (TSA); U.S. Customs and Border Protection (CBP); U.S. Secret Service, (USSS); U.S. Citizenship and Immigration Service (USCIS); U.S. Immigration and Customs Enforcement (ICE); Federal Emergency Management Agency (FEMA); and the U.S. Coast Guard (USCG). The seven operating components work closely with, support and are supported by a large network of first responders at the state, local and tribal levels. In addition, key collaboration takes place with the eighteen sectors of America's critical infrastructure/key resources (CIKR) that comprise the backbone of the nation's economy.

DHS manages this diverse group of operating components and supporting elements whose missions address a wide variety of terrorist and natural threats to our homeland. Ever changing threat dynamics often require new, innovative technology based solutions in order to prevent or mitigate the potential effects of current and future dangers. The DHS Science and Technology Directorate (DHS S&T) works to understand, document and offer solutions to current and anticipated threats faced by these stakeholders; our "customers" (DHS operating components and field agents) and our "customers' customers" (first responders and CIKR owners and operators). DHS S&T, through the Capstone Integrated Product Team (IPT) process, ensures that quality, efficacious products are developed in close alignment with detailed customer needs. The Capstone IPT process represents the requirements-driven, output-oriented portion of DHS' technology development investments geared toward providing DHS stakeholders with the necessary tools to protect America's most valuable assets – its people.

Capstone Integrated Product Teams

The Capstone Integrated Product Teams are chartered to ensure that technologies and products are engineered and integrated into systems aligned to the needs of DHS customers. Consistent with the Homeland Security act of 2002, Capstone IPTs establish a lean and agile world-class S&T management team that delivers the technological

advantage necessary to ensure DHS agency mission success. The Capstone IPT process is the framework used to determine whether developed capabilities meet operational needs, analyzes gaps in strategic needs and capabilities, develops operational requirements, and develops programs and projects to close capability gaps and expand mission competencies. This process is a customer-led forum through which the identification of functional capability gaps and the prioritization of these gaps across the Department are formalized. The Capstone IPTs manage the research and development efforts of DHS S&T and enable the proper allocation of resources to the highest priority needs established by the DHS operating components.

Chaired by the DHS S&T customer, Capstone IPTs bring together DHS S&T division heads, acquisition partners and end-users (operating components, field agents and supporting first responders – customers of DHS) involved in the research, development, testing and evaluation (RDT&E) and acquisition activities. Working together, the Capstone IPT members identify, evaluate and prioritize the operational requirements necessary to complete missions successfully. Based on information gained from Capstone IPT meetings, DHS S&T providers assess the technological and system development of products that will ultimately be deployed into the field. Figure 1 shows the organization of a Capstone IPT. The formalization of efforts through the Capstone IPT at an early stage allows key stakeholders to identify and address critical capability gaps.

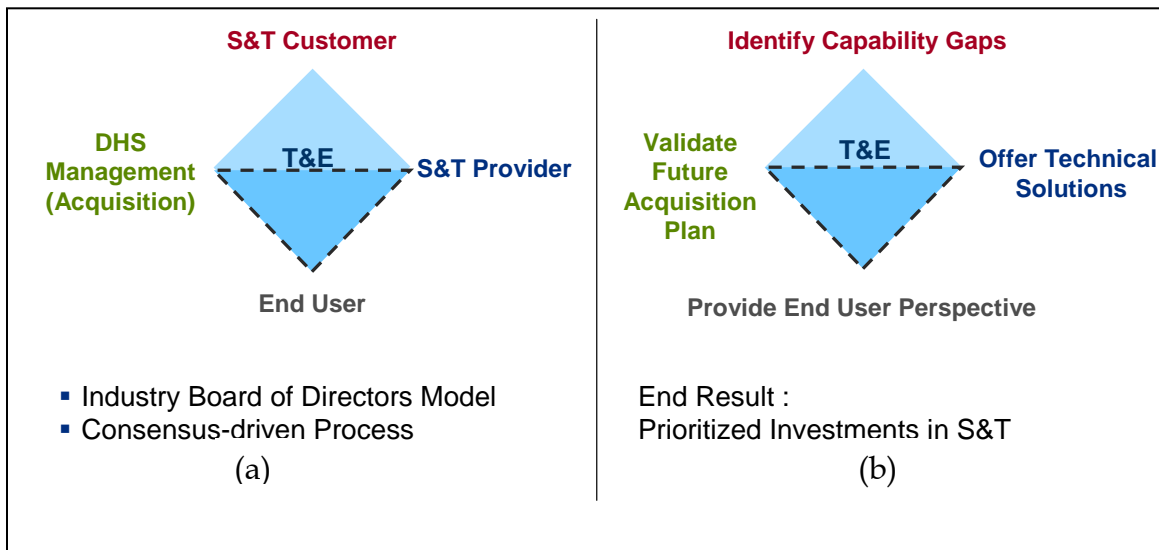


Figure 1: (a) This diagram shows the structure of the Capstone IPT model with (b) the models' output functions carried out by each IPT member.

The Capstone IPTs are structured to focus on functional, department level requirements and deal with programmatic and technology issues within the six DHS S&T divisions: Explosives (EXD), Chemical/Biological (CBD), Command Control and Interoperability (C2I), Borders and Maritime Security (BMD), Human Factors (HFD) and Infrastructure and Geophysical (IGD). Capstone IPTs have been created across thirteen major homeland security core functional areas: Information Sharing/Management, Cyber Security, People Screening, Border Security, Chemical/Biological Defense, Maritime

Security, Counter-Improvised Explosive Devices, Transportation Security, Incident Management, Interoperability, Cargo Security, Infrastructure Protection, and First Responders.

Each Capstone IPT is chaired or co-chaired by senior leadership from a DHS operating component with corresponding needs within a specific functional area. The chair/co-chair, representing the end-users of a delivered capability, engage throughout the process to identify, define and prioritize current and future requirements and ensure that planned technology and/or product transitions and acquisition programs, commercialization efforts and standards development are optimally suited to their operational requirements. Operating components, field agents, first responders and other non-captive end-users with an interest in the core functional areas of a Capstone IPT are welcome to participate and contribute throughout the Capstone IPT process. See Figure 2 for the captive members for each IPT.

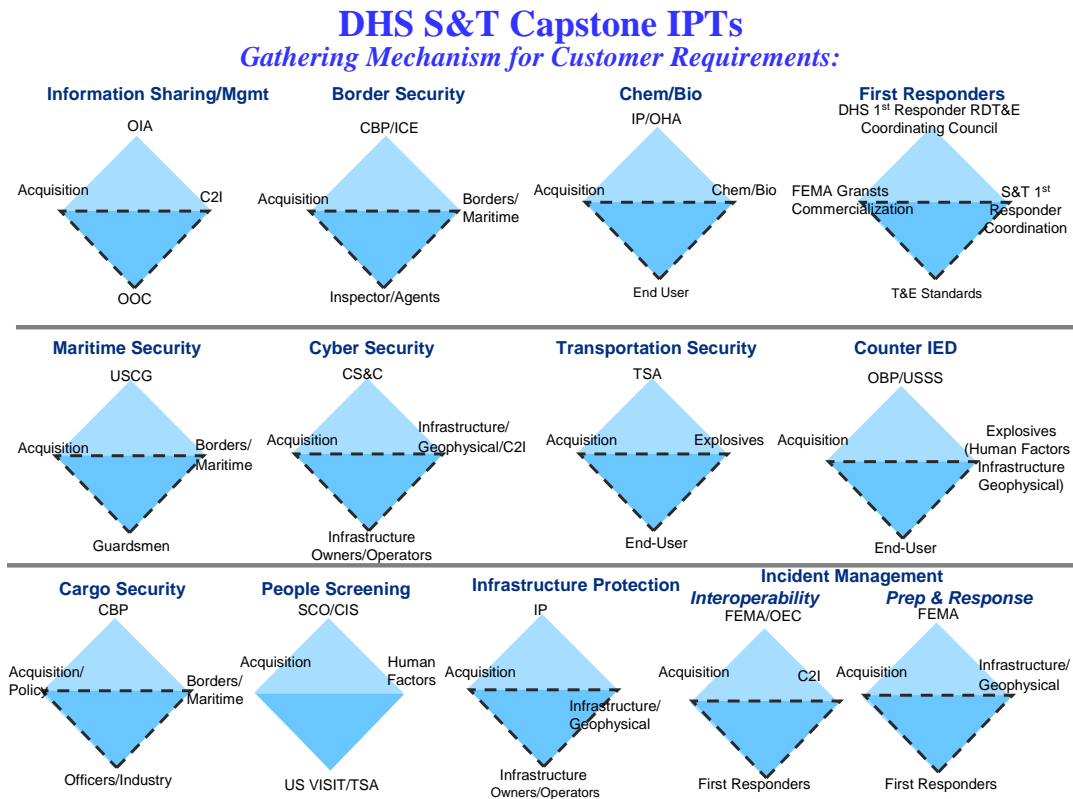


Figure 2: This diagram shows the thirteen Capstone IPTs, the DHS operating component, DHS end-user(s), the S&T Division technical provider, and, when applicable, the Acquisition conducted by DHS management.

Capstone IPTs purposefully cover very broad core functional areas. This broad focus aids in reducing the duplication of efforts geared toward various operating components of DHS. It is often the case that a given capability gap is experienced by numerous operating components and stakeholders simultaneously. Technology development is functionally aligned to allow technologies to be used in support of multiple operating components and customer sets within DHS. The effective

management and communication of capability gaps ensures that similar efforts are either combined or developed in concert so that required capabilities are provided to as many stakeholders sharing similar capability gaps, reducing overall technology development costs and accelerating the time-to-market for certain capabilities.

First Responder Capstone IPT

The First Responder Capstone IPT, the newest Capstone IPT, was established in FY 2009. This Capstone IPT coordinates the identification and prioritization of the capability gaps and detailed operational requirements of federal, state, local, tribal and territorial first responders in keeping with DHS S&T's "customer drive, customer focus" process. The First Responder Capstone IPT was organized to provide a more direct line of communication for first responders to share their unique requirements and needs with DHS S&T. Given the variety and scope of first responder duties, the IPT was formed to address the requirements of these first responder groups in order to respond to all hazards and threats, including preparation for catastrophic natural and man-made crises. Identified technology solutions will be designed, tested and assessed for effectiveness and reliability before they are produced for the first responder community.

DHS S&T developed the conceptual framework for the function of the First Responder IPT and the structure for its operation in connection with a large group of knowledgeable persons internal and external to DHS. The First Responder Technology Council was created to identify and prioritize the technology requirements and capability gaps and identify solutions to address those identified gaps. The council will be advised by the First Responder RDT&E Working Group. The working group will be comprised of first responder officials specializing in the fields of emergency management, emergency medical services, fire service, and law enforcement. These first responder officials will represent federal, state, local and territorial jurisdictions, Native American and key first responder associations from across the nation. DHS S&T will gain valuable insight from their involvement, commitment and expert understating of responder technology gaps to develop solutions to close gaps in a cost-effective, efficient and timely manner.

Capability Gaps and Enabling Homeland Capabilities

Capstone IPTs generate several outputs that guide the development and fielding of technologies and systems for DHS' stakeholders. The primary role of the Capstone IPTs is to conduct strategic needs analyses to determine and prioritize the capability gaps that exist within a given functional area. Capability gaps are broad descriptions of department level identified mission needs that are not met given current products and/or standards. Capability gaps catalog opportunities for enhanced mission effectiveness or address deficiencies in national capability. Capability gaps often start with "We need to be able to do..." statements that identify mission needs rather than suggested solutions. See Figure 3 for the requirements hierarchy diagram.

Requirements Hierarchy (TSA example)

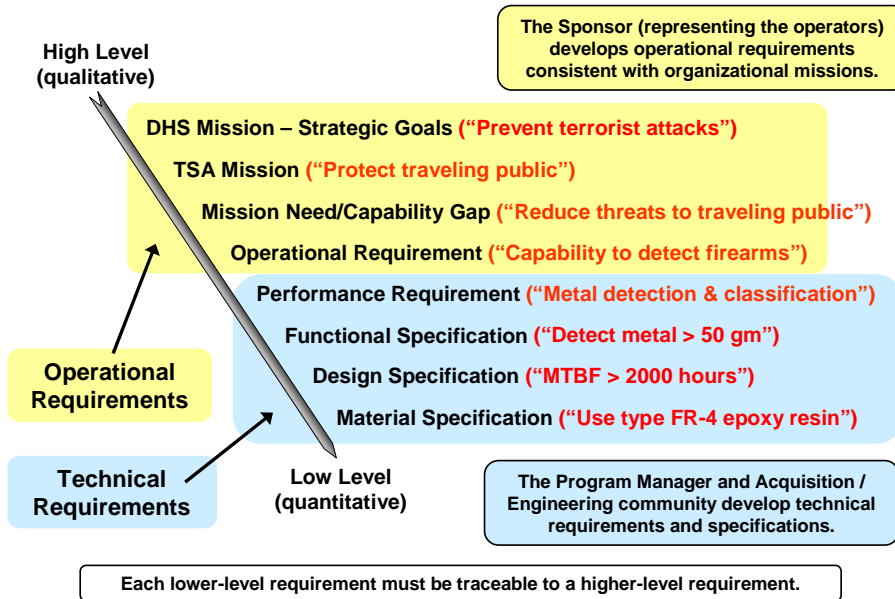


Figure 3: This requirements hierarchy shows the evolution of requirements from a high-level macro set of operational requirements to a low-level micro set of technical requirements. Note that each lower level requirement stems directly from its higher requirement so that all requirements are traceable to the overall DHS Mission.

Led by their IPT Chairs/Co-chairs, Capstone IPTs are responsible for the analysis, identification, and prioritization of their capability gaps. Capability gaps can come in several forms. Some gaps may appear in the form of modified personnel and resource allocation, training, standards, plans/protocols/procedures, resources, technology, systems, etc. For those capability gaps requiring technology-based solutions, a grouping of technology components is identified by DHS S&T to address the various needs delineated in the capability gaps. These grouped technology solutions, or Enabling Homeland Capabilities (EHCs), collectively deliver new gap closing capabilities to the customers. EHCs focus on the technology pieces that develop, mature and deliver to DHS acquisition programs, are commercialized or are validated as a standard within a three-year period or less. DHS S&T develops EHCs that contain quantifiable metrics that allow for effective management of development progress. These metrics define how the EHC will address/close the related capability gap the cost and schedule over the life of the EHC, identify the specific S&T efforts addressing the EHC and endorsements and recommendation of proposed EHCs and corresponding deliverables by the relevant Capstone IPT. EHCs enable customers and DHS S&T engineers to focus on discussions related more broadly to overall capability needs rather than discussions simply about potential solutions to problems.

Project-IPTs: Managing the Day-to-Day Development of Capabilities

The Capstone IPT process enables our DHS S&T divisions to interact regularly with their customer(s) to address capability gaps. These capability gaps, in many ways

are just the beginning. Additional detailed requirements must be articulated to enable the cost-effective and efficient development of a technology or product. In order to achieve greater insight into the details that comprise each Capstone IPT, Project-IPTs are created to manage specific project areas within a functional area. While Capstone IPT meetings occur at regular intervals throughout the year, Project-IPTs are created to manage closing capability gaps gathered from the larger Capstone IPT on a daily basis. For example, Border Officer Tools and Safety, and Container Security are Project-IPTs for the Border Security and Cargo Security Capstone IPTs, respectively. Project-IPTs consist of several DHS S&T subject matter experts who are responsible for clarifying the capability gaps derived from the Capstone IPTs and for articulating operational requirements with the customers for the overall capability enhancement that is necessary. These requirements assist in decomposing a high-level capability gap into the individual components that may comprise a potential solution. Through this process the grouping of individual technologies into an integrated system creates the overall EHC.

The Project-IPTs work closely with DHS customers to develop a robust understanding of customer needs, through an operational requirements document (ORD), to define clearly the specific requirements that must be met in order for a technological solution to address a given problem. Development of detailed ORDs further enhances the direction in which technology and product development efforts progress and further reduces duplication of effort across various Project and Capstone IPTs. These subject matter experts are also involved in conducting market surveys, analyses of alternatives and other functions related to technology and product evaluation ensuring that developed capabilities are aligned to customers' needs. Additionally, Project-IPTs serve a critical role in integrating developed capabilities into EHCs and fully deployable systems that provide customers with enhanced mission capabilities. All DHS agencies are responsible for integrating and fielding the technology deliverables into operational systems scheduled for delivery to their Operating Component.

Management – DHS Leadership and DHS-S&T

The Capstone IPTs prioritize EHC proposals that respond to customer capability requirements. DHS leadership has a critical role in determining Capstone IPT funding levels and investments once prioritized EHCs are identified. Once approved, budgets are submitted, solicitations may be issued, pre-award technical reviews are conducted, and commercialization efforts are considered. DHS leadership conducts reviews of current EHCs every six months to ensure that EHCs meet cost objectives and that technical development is progressing along milestones. DHS leadership also reviews new EHCs and continually reviews on-going EHCs in order to make informed decisions regarding continued funding of programs.

The Transition Office manages the process to develop and deliver required technologies/products as defined in the EHCs. Working with its customer requirements, DHS S&T proposes the technology-based solutions approved EHCs to the Capstone IPTs. By understanding the needs and requirements of its customers, DHS S&T identifies the programs that are ineffective/insufficient in meeting the EHC expectations and offer technical solutions to address the stated requirements. DHS S&T works to conduct

market and technology scans to find technology-based solutions that can be developed, matured and delivered to DHS acquisition programs, commercialized or validated as a standard within a three-year period.

There are several ways products can transition into fully developed, widely distributed products for the large customer communities. Figure 4 identifies possible transition paths to deliver products to customers. DHS S&T may recommend available commercial-of-the-shelf (COTS) products or other non-S&T alternatives in lieu of developing a new DHS S&T solution. DHS S&T also reviews private sector responses to solicitations for capabilities that cannot be readily addressed with COTS products. Once development plans are approved, DHS S&T engages and involves the customer via technology demonstrations and experimentation to ensure adequate customer feedback throughout the development life cycle. DHS S&T manages costs, schedules and technical performance of programs under the oversight of the Capstone IPT. The Director of Transition chairs monthly status meetings that allow technology execution problems to be discussed and resolved in a timely and effective manner.

Transition Approaches

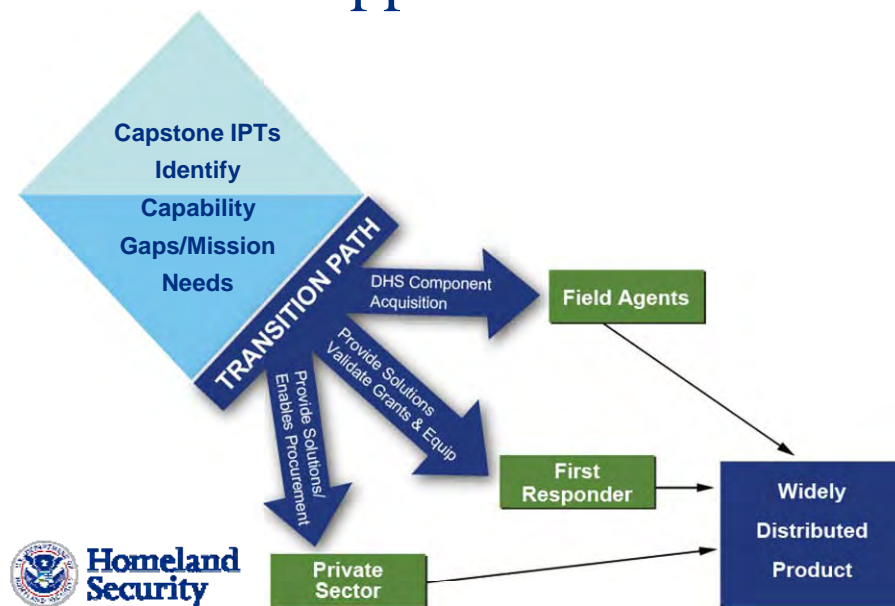


Figure 4: DHS has three major methods to transition products to end-users. DHS field agents are captive end-users of the Capstone IPT process; while the First Responder community is typically able to select its own solutions, all newly proposed DHS programs must now identify technologies/products already in development in the private sector that are aligned with end-user requirements for DHS field agents and/or to enable First Responders to make informed purchasing decisions.

Technology Transition Agreements (TTAs)

Technology Transition Agreements (TTAs) represent a good-faith contract between the DHS S&T developer and the DHS customer. The TTA is negotiated and

signed at the product level by those communities responsible for a delivering or advocating a specific product or technology. As a consensus agreement, the TTA is signed by all of the stakeholders responsible for the technology/product in order for continued funding. This good faith agreement determines the specific exit criteria that must be demonstrated in order for the “hand off” of the technology/product to the customer.

The TTA provides a detailed description of the deliverable promised by the DHS S&T program managers. The customer program manager certifies that the need for the product or technology is consistent with the needs/requirements as defined by their operating component, and the requirements or acquisition agents state their commitment to integrate the successfully demonstrated technology/product or into an identified and funded acquisition program. The TTA ensures that all parties explicitly understand the deliverable is aligned to customer needs and that a funding source is available and aligned with the customer’s needs. If any problems are identified by DHS S&T, customer agency or acquisition offices, all parties are informed and decisions are made regarding continued funding. Once the TTA has been signed the next step is to move forward with product development and eventual product deployment to the customers.

Using Technology to Give Boots on the Ground a Voice

Traditional communication through e-mail and phone calls has proven insufficient in gathering and compiling input from the sheer number of stakeholders responsible for providing protection to our homeland. There remains room for improvement in gathering requirements from the “boots on the ground.” In many ways, the private sector possesses much more reliable information than is seen from DHS’ previous, seemingly disjointed approach. Continued work through the Capstone IPTs and DHS’ Requirements Development Initiative training materials will reduce the inefficiency of DHS personnel by providing a single point of entry for end-user representatives.

Just as needed is deployable technology to create a Community of Practitioners (CoP). DoD has invested in these kinds of technologies to enable reaching not only the millions of first responders nation-wide but also other customers and potentially authorized stakeholders (other federal agencies, private sector, venture community, etc). Advanced technologies like the “Semantic Web 3.0” will aid in the communal and open development of capability gaps, ORDs, potential available market sizing/applications, etc. all at the benefit of the American taxpayer, Government and private sector. We are finalizing plans to initiate a pilot program to harness these technologies to engage various user communities, including members of the First Responder Capstone IPT to enable broad-based development of widely accepted operational requirements. Figure 5 shows graphically the anticipated evolution of developing requirements customers at DHS S&T.

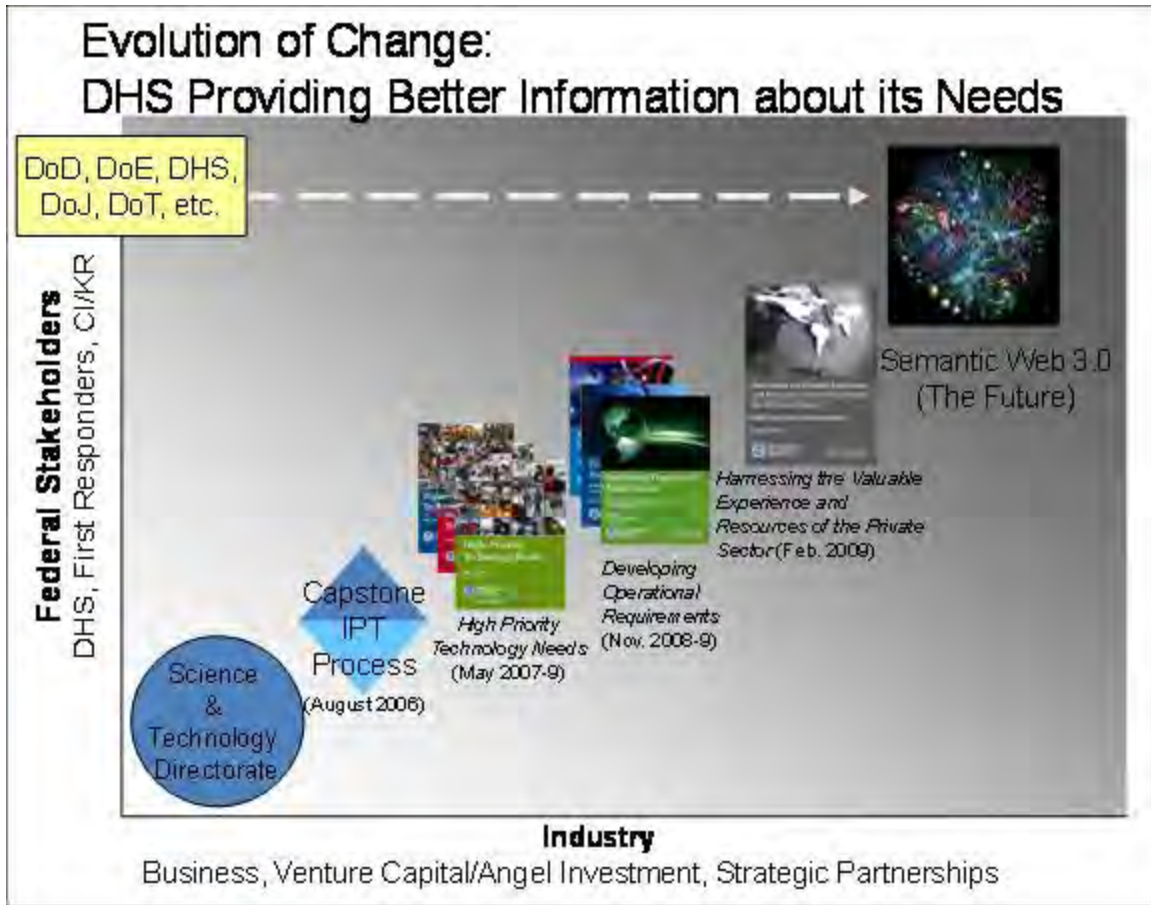


Figure 5: DHS has progressed in the way that it reaches out to its stakeholders to learn about their needs. Advanced social networking technologies have the potential to greatly enhance communications and understanding of needs.

It is clear that DHS S&T needs to lead the development of an easy-to-use technology to generate a CoP for its customer communities. The vast majority of the millions of DHS' stakeholders need to be invited to play an active role in creating, editing and prioritizing detailed operational requirements to be used by DHS in order to provide (or facilitate through its commercialization efforts) solutions for the stakeholders communities. This approach enables both a "bottom-up" and "top-down" view of detailed user requirements – avoiding the age-old discussion of whether a "bottom-up" or "top-down" approach is superior. New social networking technologies have opened new opportunities that allow communication to flow and leverage the merit of both approaches.

DHS S&T plans to create a set of detailed operational requirements of a system prototype that, in general:

- Effectively leverages advanced social networking and information sharing (utilizing semantic architecture and TRL management) using genuine DHS scenarios such as developing/editing ORDs, all at the benefit of taxpayers in an open and transparent way for all to participate easily

- Captures First Responder feedback from a live community of >10,000 users
- Expandable to millions of users in the First Responder, CIKR, and potential solution providers (private sector) communities
- Expandable to include vital interagency partners like DoE, DoD, and National Laboratories for gauging potential users and potential available market sizing
- Expandable to include Venture Capital, Angel Investor and Corporate Investor Communities, if desired and/or required

Next steps

In our outreach efforts with the private sector, DHS S&T realizes that we must work with our customers to produce detailed operational requirements documents in order to relay effective requirements to the private sector. DHS is forging a new paradigm with far-reaching positive consequences. These benefits are felt by DHS' customers, private sector partners, and U.S. taxpayers through the rapid, cost-effective and efficient development and deployment of products and services to protect the Homeland of the United States. DHS is creating a "commercialization mindset" utilizing public-private partnerships to expedite the development of products and services to protect the nation. Recently announced commercialization initiatives (like our innovative SECURE™ and FutureTECH™ programs) are truly groundbreaking approaches to foster a mutually beneficial relationship between the public and private sectors by creating an open and freely competitive program accessible by small, medium and large firms. These efforts are a natural extension of the Capstone IPT process.

The future of these initiatives looks bright; we have already experienced an overwhelmingly positive response to the initial private sector outreach initiative. DHS S&T stands at the forefront of innovative thinking within the public sector and we will continue to monitor and measure the benefits this program will provide. For more information on these commercialization efforts, please visit http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm

Summary

The Capstone IPT process is a model that requires the participation and input from several DHS stakeholders. This collaborative effort centers on the principle that the customer is "the focus" of this process. The product and technology outputs of the Capstone IPT process are customer-requirements-driven from start to finish. The customer is involved throughout the process to ensure that they receive products and technologies specifically aligned to their detailed operating requirements. Ultimately, our customers receive quality products that effectively deliver the necessary, mission-critical capabilities to secure our nation.

Acknowledgment:

We would like to acknowledge the valuable assistance of Mark Protacio, Caroline Greenwood, Morgan Motto and Steve Roberts in the preparation of this document.



Richard V. Kikla is the Director of Transition for the United States Department of Homeland Security, Science and Technology Directorate in Washington, D.C. He manages the operations of the Capstone IPT process, ensuring that technologies/products are moving along respective transition paths.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer in Washington, D.C. He leads the private sector outreach initiatives for DHS S&T has written a series of books to facilitate the development and articulation of operational requirements for DHS stakeholders.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





Commercialization Office: Offering Transformational Change Beyond DHS

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security

June 2009



**Homeland
Security**

Science and Technology

Commercialization Office: Offering Transformational Change Beyond DHS

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security
Science & Technology Directorate

The U.S. Department of Homeland Security, through the Science & Technology Directorate (S&T) initiated an innovative commercialization-based public-private partnership called the SECURE Program. Through the SECURE Program, the Department provides to potential solution providers detailed operational requirements and a conservative estimate of the potential available market(s) offered by DHS stakeholders, such as DHS operating components (FEMA, TSA, CBP, Secret Service, ICE, USCIS and Coast Guard) first responders and critical infrastructure/key resources (CIKR) owners and operators. In exchange for this valuable information, the private sector offers deployable products and services (along with recognized third party test and evaluation data) that meet these stated requirements in an open and free way that creates an ergonomic “clearinghouse of solutions” available to DHS stakeholders. Because of the success and “win-win-win” nature of this program in that it provides benefits for the American taxpayer, the private sector and DHS, DHS-S&T recently introduced the FutureTECH Program that describes the long-term capabilities/technologies required by DHS stakeholders. Please see http://www.dhs.gov/xres/programs/gc_1211996620526.shtm and http://www.dhs.gov/xres/programs/gc_1242058794349.shtm to review these programs.

While it is gratifying that our commercialization process and private sector outreach programs are being incorporated and mandated by the Department in the forthcoming and updated Acquisition Management Directive (MD 102-01), it is worth noting that our model can be readily extended to and adopted by other agencies in the federal government. Examination of Table 1 clearly shows how the incorporation of Commercialization adds a “valuable tool to an agency’s toolbox” in providing increased speed-of-execution of deploying technologies/products/services to solve problems as well as provide an increase in the net realizable budget of an agency. In addition, as evidenced by Table 2, the potential return-on-investment of these commercialization-based public-private partnerships can yield impressive results.

Why a Commercialization Office?

DHS S&T Commercialization Office-- Four Major Activities Creating and Demonstrating Value

Parameter	Requirements Development Initiative	Commercialization Process	Public-Private Partnerships	S&T Private Sector Outreach
1) Increases speed-of-execution of DHS programs/projects	✓	✓	✓	✓
2) DHS and its stakeholders receive products more closely aligned to specific requirements/needs	✓	✓	✓	✓
3) Increases effective and efficient communication	✓	✓	✓	✓
4) End users can make informed purchasing decisions	✓	✓	✓	✓
5) Large savings of cost and time for DHS and its stakeholders	✓	✓	✓	✓
6) Increases goodwill between taxpayers, private sector and DHS	✓	✓	✓	✓
7) Fosters more opportunities for small, medium and large businesses	✓	✓	✓	✓
8) Large taxpayer savings	✓	✓	✓	✓
9) Possible product "spinoffs" can aid other commercial markets	✓	✓	✓	✓
10) Promotes open and fair competition	✓	✓	✓	✓

Return-on-DHS Investment is LARGE!

Table 1 - The major activities of the Commercialization Office demonstrate positive results for the American taxpayer, private sector and DHS.

Commercialization Office - Return on Investment (ROI)

Assumptions for Conservative ROI Projections:

- *Return on Investment* – (Gain on Investment/Cost Savings – Cost of Investment) / Cost of Investment
- *Gain on Investment/Cost Savings* – conservative estimate of potential savings of nominally expended R&D dollars at S&T; in general, estimated savings is 75% of given/related FY09 enabling homeland capability (EHC), which is identified through Capstone IPT process
- *SECURE Program – Cost of Investment* – 20% of Commercialization Office personnel salary + (10% Other expenses such as OGC, OPA, CCD, etc.); divided by 20 operational requirements documents (ORDs) completed and publically released in given year
- *R&D Funds at DHS S&T* – R&D funds do not include labor or overhead (not fully burdened cost of managing program/projects/EHCs)

SECURE Program – ORD	ROI
Blast Resistant Autonomous Video Equipment (BRAVE) ORD Requirements for a forensic camera deployed in public transportation vehicles to assist in incident cause analysis.	290x
National Emergency Response Interoperability Framework and Resilient Communication System of Systems ORD Requirements for a system to provide interoperable communications on a national framework for remote use by first responders.	525x
Interoperable Communications Switch ORD Requirements for an interoperability switch-based communications system that provides networked communications between any number of agencies and personnel.	525x
Crisis Decision-Support Software ORD Requirements for a system with a user-centric approach matched with an expansive database of past decisions and a proven method to quickly reach critical decisions in high pressure environments for wide operational use.	1023x
Blast Mitigation of Fuel Tank Explosions ORD Requirements for an explosion suppression system to protect fuel containers. A "fuel container" ranges from fuel tanks found in vehicles, boats or trains to fuel storage tanks at airports, seaports and the neighborhood gas station.	727x
Integrated Intrusion Protection ORD Requirements for an adaptable, scalable surveillance capability that provides automated, real-time protection for a wide range of operational scenarios.	290x
Predictive Modeling for Counter-Improvised Explosive Devices (IED) ORD Requirements for a system to predict the threat of an IED attack and further data fusion from law enforcement, intelligence partners and other sources to support the common operating picture.	870x

Return on DHS Investment is LARGE when compared to Angel Investors (4x to 7x) and Venture Capitalists (5x to 20x)

Table 2 - The use of Commercialization has the potential to realize significant Return-on-Investment (ROI) values as evidenced by the SECURE pilot program at DHS.

We have shown through the SECURE and FutureTECH programs that the federal government can engage and influence - in a positive way - the private sector by offering detailed requirements and conservative estimates of market potential. The reason that these partnerships are successful is simple and straightforward. Firms spend significant resources in trying to understand market needs and market potential through their business and market development efforts. By offering this information, government saves the private sector both time and money while demonstrating its genuine desire to work cooperatively to develop technologies and products to meet DHS stakeholders' needs in a cost-effective and efficient way that benefits the private and public sectors – but also, most importantly, to the American taxpayers' benefit.

Because of its obvious benefits, it is reasonable to examine the possibility of extending the concepts developed at DHS to other federal agencies. Logic dictates that in cases where operational requirements can be developed across agencies, the size of a given potential available market would increase. It is also certainly conceivable that various agencies across the federal government share similar requirements for products and services. Just as business experts discuss “technology platform” strategies and models, one can envision a detailed requirements document delineating core requirements with additional agency-driven “options” -- analogous to the variety of options offered on automobiles. Just as consumer products are developed with a variety of options (at varying price points), a detailed requirements document could outline all the options required by agencies through a “requirements platform.” Figure 1 shows how an agency like DHS is related to other government and non-government ancillary markets.

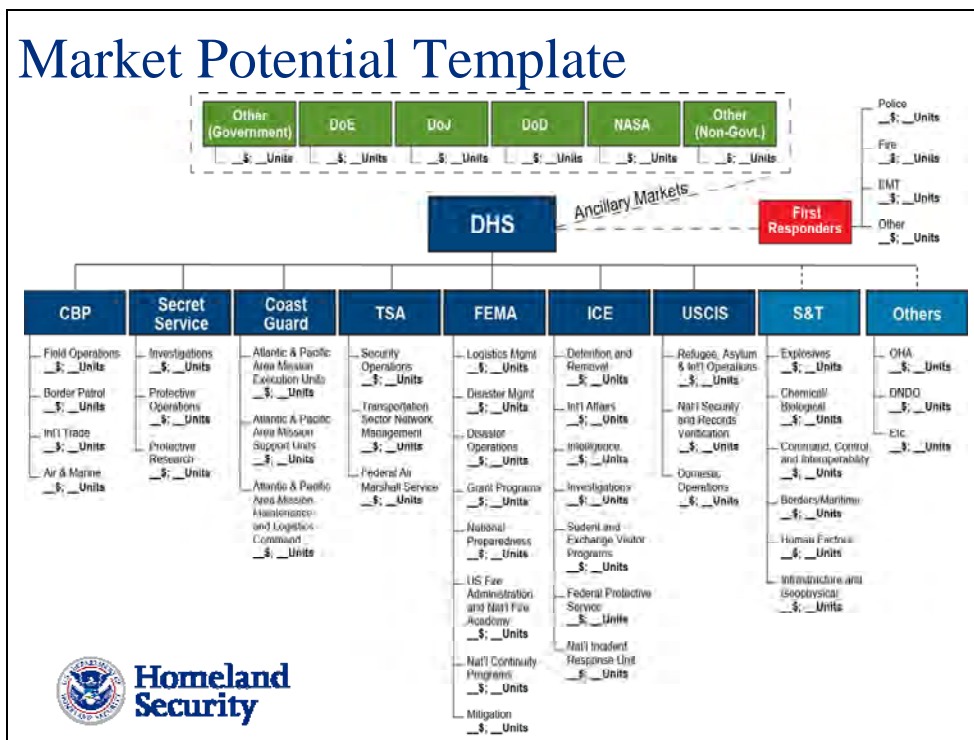


Figure 1 - The Market Potential Template for DHS outlines potential user communities within DHS markets but also to “ancillary markets” represented by other federal government agencies.

The more crosscutting a set of requirements becomes, the more opportunities exist to save taxpayers' resources. How could this be accomplished in a practical way? The answer is simple: It has already begun... The DHS Science & Technology Directorate is planning to utilize of the semantic web (also known as Web 3.0). In order to gather and communicate requirements across such a large-scale community of users, there is a need to use deployable technology to create a Community of Practitioners (CoP). DoD, for example, has invested in these kinds of technologies. Technology will enable the ability to reach not only the millions of first responders but also other potentially authorized stakeholders (other federal agencies, private sector, venture community, etc). Advanced technologies like the Semantic Web 3.0 will aid in the communal and open development of detailed operational requirements, potential available market sizing/applications, etc. all at the benefit of the American taxpayer, government and private sector. We are finalizing plans to initiate a pilot program to harness these technologies to engage various user communities to enable broad-based development of widely accepted operational requirements. Figure 2 shows graphically the evolution of developing detailed requirements culminating in the establishment of CoPs.

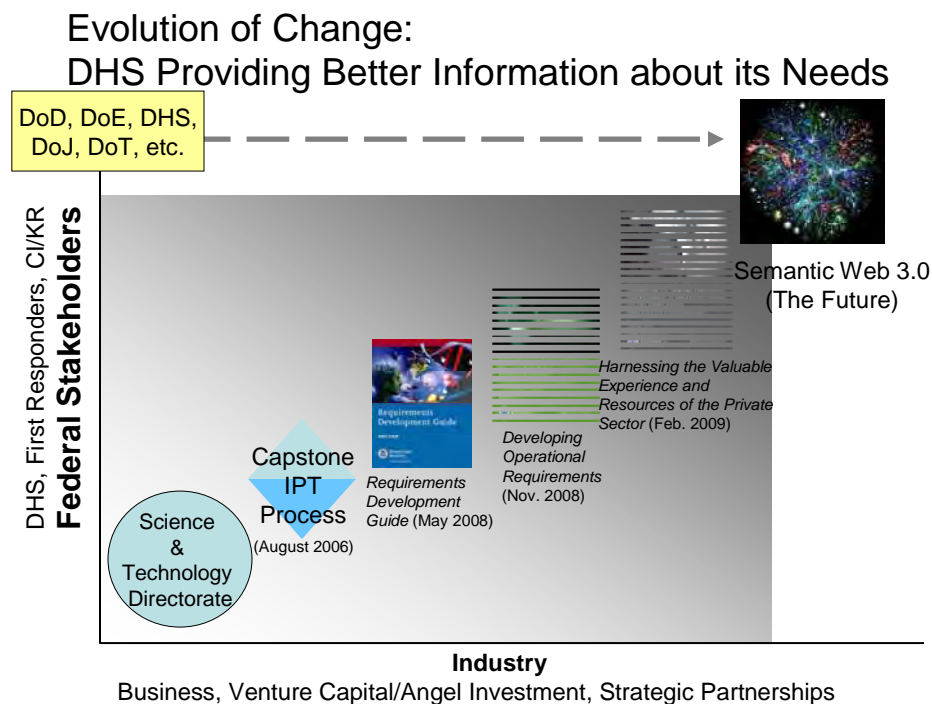
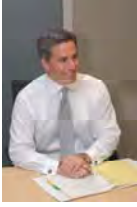


Figure 2 - DHS is transforming the way that it reaches out to its stakeholders to learn about their needs. Advanced social networking technologies have the potential to greatly enhance communications and the understanding of needs to allow open and free competition to provide the best solutions at the best price for government.

To conclude, commercialization is a tool that has genuine value well beyond DHS. In fact, commercialization can offer more and more opportunities to increase the speed-of-execution of government programs and increase the net realizable budget of the government -- all at the benefit of taxpayers the more the model is used across and within government.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published four comprehensive books: *Requirements Development Guide*, *Developing Operational Requirements*, *Developing Operational Requirements (Version 2.0)* and *Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good: DHS's Entry into Commercialization* to aid in effective requirements development and communication for the Department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector. He is also the first federal official on the Council of Competitiveness representing the U.S. Department of Homeland Security.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





***Helping Everyday Heroes Get What They Need:
A Systematic Approach to Understanding First Responder Requirements and Delivering Cost-Effective Solutions***

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security**

June 2009



**Homeland
Security**

Science and Technology

Helping Everyday Heroes Get What They Need: A Systematic Approach to Understanding First Responder Requirements and Delivering Cost-Effective Solutions

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security
Science and Technology Directorate

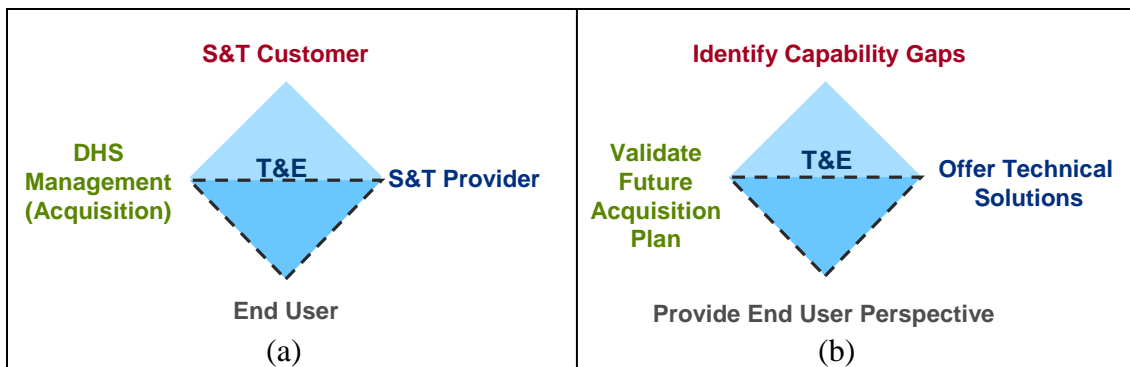
Our nation's first responders play a critical role in protecting Americans on a daily basis – whether fighting fires, law enforcement, coordinating preparedness or rescue efforts as well as responding to large-scale man-made or natural crises. First responders are increasingly relied upon for action in all-hazard response efforts as the first line of defense for many communities across the country. Given their critical roles and responsibilities, new efforts are underway to increase the speed at which effective products and services are developed and deployed to first responders to handle the many challenges that they face in the normal day-to-day activities as well as valuable in crisis scenarios.

The U.S. Department of Homeland Security (DHS), through its operating components such as the Federal Emergency Management Agency (FEMA) and supporting DHS organizational elements like the Office of Infrastructure Protection (OIP) and the National Protection Programs Directorate (NPPD), is responsible to work with first responders at the federal, state, local and tribal levels to coordinate and prepare for the mitigation of and response to a plethora of potential hazards. These groups work closely together to develop plans to protect our most critical assets – our people. One additional DHS organizational element critical to understanding the detailed operational requirements of the first responder communities is the Science and Technology Directorate (S&T).

S&T's mission is to support, enhance and enable the mission-critical objectives of DHS operating components as well as DHS stakeholders including first responders and the critical infrastructure/key resources owners and operators. Given S&T's role to support such a wide variety of homeland security stakeholders, significant efforts have been made to enhance the coordination and understanding of needs from our customers' customers. In August 2006 the Capstone Integrated Product Team (IPT) process formalized the way in which S&T interacts with its stakeholders to understand and respond to capability gaps found across the homeland security mission space. An extension of capability-based planning, the Capstone IPT process focuses on gathering and addressing capability gaps received directly from DHS stakeholders, related to six major functional areas; explosives, chemical and biological, borders and maritime security, infrastructure and geophysical protection, command, control and interoperability, and human factors.

The Capstone IPT process represents the requirements-driven, output-oriented portion of DHS’s technology development investments to assist our numerous customers to perform their mission-critical objectives. Capstone IPTs are chartered to ensure that technologies and products are engineered and integrated into systems scheduled for delivery or made available to DHS customers. Consistent with the Homeland Security Act of 2002, Capstone IPTs establish a lean and agile world-class S&T management team that delivers the technological expertise necessary to ensure DHS stakeholders achieve mission success. The IPTs oversee the research and development efforts of DHS-S&T and enable the proper allocation of resources to the highest priority needs established by the DHS stakeholders.

Capstone IPTs bring together S&T division heads, acquisition partners and end-users (operating components, field agents, first responders, etc. – the customers of DHS) involved in the Research, Development, Testing and Evaluation (RDT&E) and acquisition activities. Working together, the IPT members identify, evaluate and prioritize the necessary requirements to complete missions successfully. IPTs also assess current commercial market offerings and the technological and system readiness of products that will ultimately be deployed into the field. Figure 1 shows the organization of a Capstone IPT and the key participants in the newly established First Responder Capstone IPT. Each Capstone IPT has a DHS operating component/council chair or co-chairs. The chair/co-chair, representing end-users, is responsible to identify, define and prioritize current and future requirements and ensure that planned technology and/or product transitions to acquisition programs, commercialization efforts or standards development are initiatives optimally suited to specific requirements.



First Responder Capstone IPT

DHS First Responder RDT&E Coordinating Council
(Requirement Sponsor)

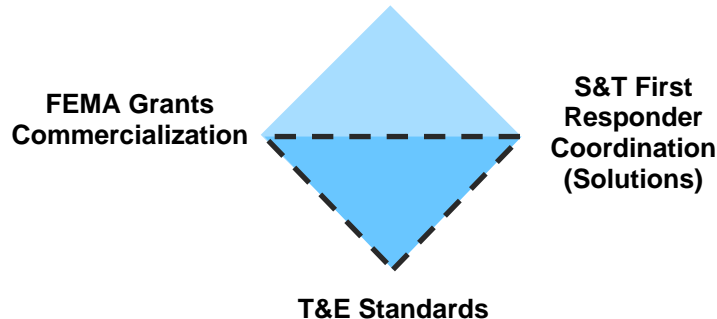


Figure 1 (a) This diagram shows the structure of the Capstone IPT model with (b) the models’ output functions carried out by each IPT member and (c) a graphical depiction of the First Responder Capstone IPT.

Capstone IPTs have been created across thirteen major homeland security core functional areas: Information Sharing/Management, Cyber Security, People Screening, Border Security, Chemical/Biological Defense, Maritime Security, Counter-Improvised Explosive Devices, Transportation Security, Incident Management, Interoperability, Cargo Security, Infrastructure Protection, and the newly introduced First Responder IPT. In this way, technology development is functionally aligned, rather than by operating component “stove pipes” so as to allow technologies to be used in support of multiple stakeholders within DHS. This broad focus aids in reducing the duplication of efforts across various operating components/stakeholders of DHS. All DHS operating components with an interest in a particular Capstone IPT are invited to send a representative to participate as an IPT member. See Figure 2 for the captive members for each IPT.

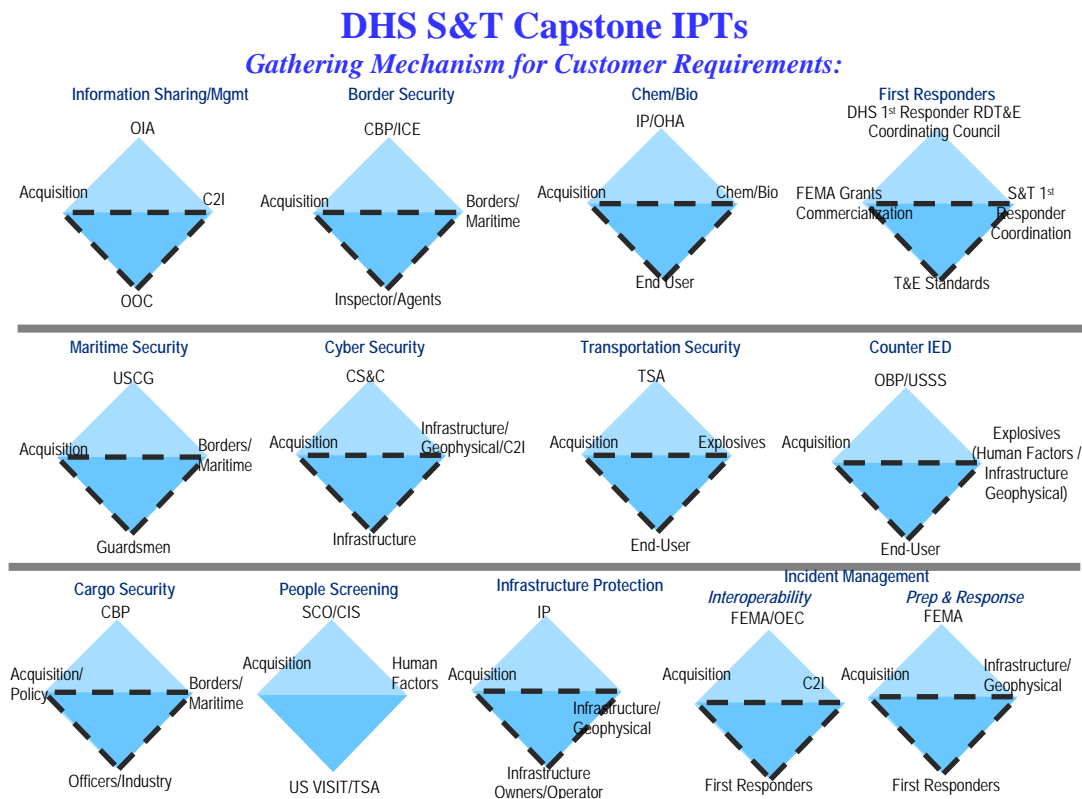


Figure 2 - This diagram shows the thirteen Capstone IPTs, the DHS operating component/stakeholder, DHS end-user(s), the S&T Division technical provider, and, when applicable, the Acquisition conducted by DHS management.

The First Responder IPT, the newest capstone IPT, was established in FY 2009. This Capstone IPT coordinates the identification and prioritization of the capability gaps and detailed operational requirements of federal, state, local, tribal and territorial first responders in keeping with S&T’s “customer drive, customer focus” process. The IPT was organized to provide a more direct line of communication for first responders to

share their unique requirements and needs with S&T. Given the variety and scope of first responder duties, the IPT was formed to address the requirements of these first responder groups in order to respond to all hazards and threats, including preparation for catastrophic natural and man-made crises. Identified technology solutions will be designed, tested and assessed for effectiveness and reliability before they are produced for the first responder community.

S&T developed the conceptual framework for the function of the First Responder IPT and the structure for its operation in connection with a large group of knowledgeable persons internal and external to DHS. The First Responder Technology Council was created to identify and prioritize the technology requirements and capability gaps and identify solutions to address those identified gaps. The council will be advised by the First Responder RDT&E Working Group (WG). The WG will be comprised of 31 first responder officials representing the fields of emergency management, emergency medical services, fire, and law enforcement. These first responder officials will represent federal, state and local jurisdictions, Native American and key first responder associations from across the nation. S&T will gain from their involvement, commitment and expert understating of responder technology gaps to develop solutions to close gaps in a cost-effective, efficient and timely manner. In order to achieve greater insight into the facets that comprise each Capstone IPT, Project-IPTs are created to manage specific project areas within a functional area.

The First Responder Technology Council (FRTC) shall provide a round-table for the sharing of information regarding the technology/product/service/standards needs of the over 25 million first responders in the United States, as shown in Figure 3. It will serve as a vehicle for the coordination of investment, programs, technology, research, development and delivery of technological tools to first responders at the federal, state, local, tribal and territorial levels. It will serve to facilitate effective interactions between S&T Program Managers and appropriate stakeholders within the first responder communities.

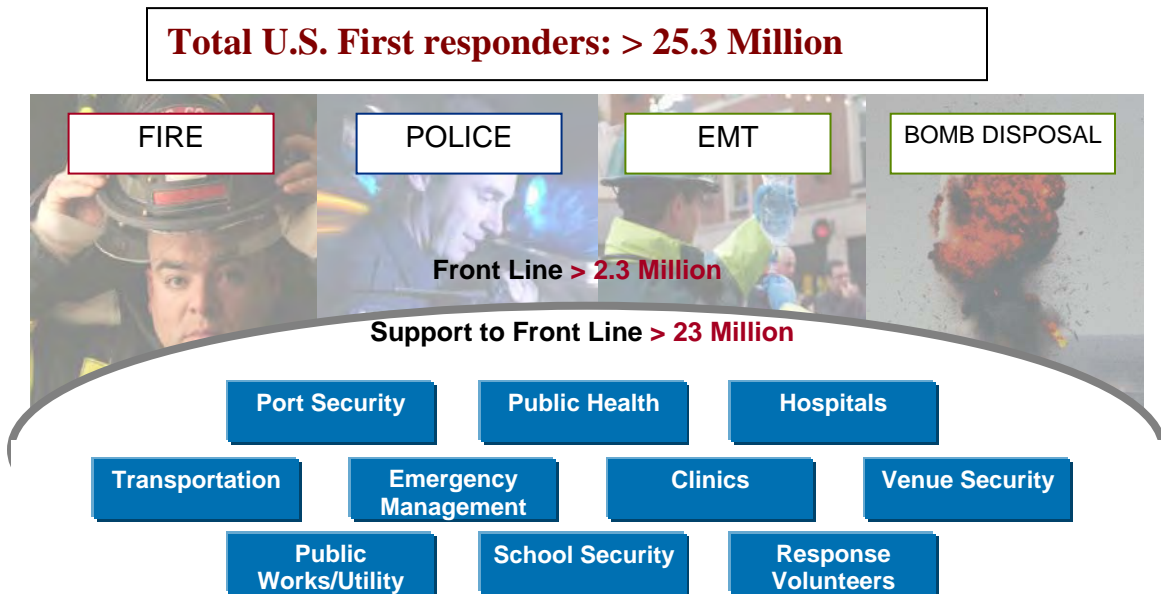


Figure 3- Homeland Security Presidential Directive (HSPD) - 8 classifies those individuals considered first responders in the United States. A conservative estimate shows that over 25.3 Million people work or volunteer as first responders. For a complete segmentation of the first responder market map, please refer to Appendix I of DHS’s Developing Operational Requirements book available online at http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf.

Our nation’s first responders represent a large number of citizens involved in providing protection to the country during any number of crises and emergencies. The community of first responders has numerous needs at all levels in order to perform their mission critical tasks. With coordinated outreach and open communication through efforts like those that are being established within the First Responder Capstone IPT, the foundation is being laid to further improvement of understanding the needs and operational requirements for the many challenges that must be addressed.

This improved understanding, through communication and the articulation of detailed operational requirements documents is changing the way in which the needs of first responders can be addressed in ways that are both cost-effective and efficient. The vast majority of needs coming from the first responder community require the development and deployment of widely distributed products, in many cases requiring thousands – if not millions – of units nation-wide. DHS is now adopting and implementing a new commercialization process and public-private partnerships to address the needs of first responders and the many other DHS stakeholders.

In an effort to leverage the free market system and the ingenuity, experience and resources of the private sector, new programs have been introduced to foster public-private partnerships to develop products and services aligned to the requirements of DHS stakeholders. The SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) program is one such partnership program. Through the SECURE program DHS shares with the private sector the two most critical pieces of

information that the private sector needs to generate a business case for their potential involvement in using their resources to develop products/services: 1) a detailed articulation of the operational requirements for a given problem; and 2) a conservative estimate of the potential available market (PAM) of users across DHS, the first responder communities and the critical infrastructure/key resources (CIKR) owners and operators. With this information, the private sector is able to assess the opportunity to pursue the development of products and/or services to address the needs of the large potential available markets represented by DHS stakeholders. See Figure 4 for a market potential template that shows the broad scope of DHS stakeholders and just as important, the ancillary markets and other federal agencies to which DHS is a conduit.

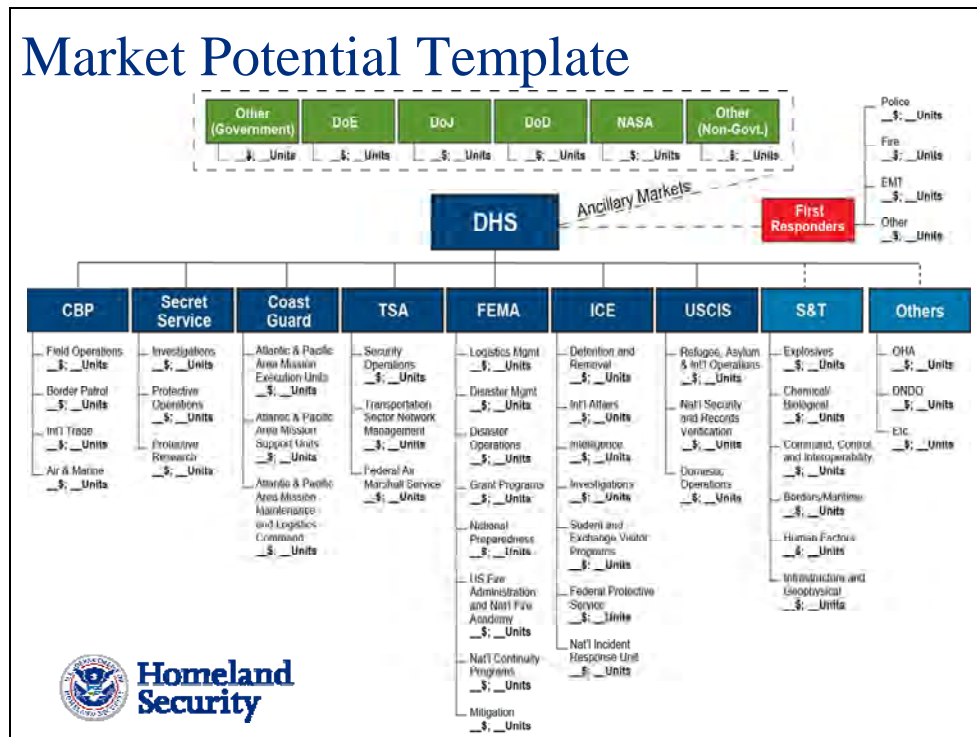


Figure 4 - The Market Potential Template for DHS outlines potential user communities within DHS markets but also shows its relationship to “ancillary markets” represented by other federal government and non-government agencies.

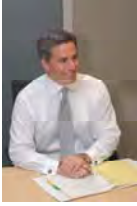
These large markets often represent attractive business opportunities for the private sector especially combined with the valuable information provided by the detailed operational requirements found in an operational requirements document (ORD). In return for providing this critical information and saving the private sector considerable time and money related to market and business development activities, DHS expects the private sector to offer solutions – utilizing the free market system with open and fair competition – to meet published requirements. DHS will review test and evaluation data from recognized, third party independent test and evaluation reports provided by the private sector to ensure that a product or service meets or exceeds its specifications and is aligned with stated operational requirements. Successful products or services are then certified by DHS and companies can share in the imprimatur of DHS through the

certification mark or seal provided by DHS. Simply stated, the private sector receives significant business opportunities, DHS and its supported entities receive products and services developed at faster execution rates at the private sector’s cost - all to the benefit of the American taxpayer. See Table 1 for a breakdown of the benefits realized when the SECURE program is used to foster public-private partnerships; simply put, a “win-win-win” situation occurs.

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Table 1 - A benefit analysis of the SECURE Program shows positive outcomes for taxpayers as well as the public and private sectors.

In summary, it is easy to see that new efforts to reach out to first responders will have a significant impact on the way in which first responders’ mission capabilities are enhanced through fielding quality products and services aligned to their needs at increased speed and lower cost. The Capstone IPT and commercialization processes are tools that add genuine value to DHS stakeholders, especially the first responder community. In fact, these efforts can offer more and more opportunities to increase the speed-of-execution of technology and product development programs and ensure that the best solutions at the best prices are made available to our everyday heroes.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published four comprehensive books: *Requirements Development Guide*, *Developing Operational Requirements*, *Developing Operational Requirements (Version 2.0)* and *Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good: DHS's Entry into Commercialization* to aid in effective requirements development and communication for the Department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector. He is also the first federal official on the Council of Competitiveness representing the U.S. Department of Homeland Security.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





Opportunities to do Business with DHS S&T

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security

December 2009



**Homeland
Security**

Science and Technology

Opportunities to do Business with DHS S&T

Overview

Simply put, the mission of the Department of Homeland Security (DHS) is to protect our nation's most valuable asset, our people. DHS' stakeholders cover a wide variety of mission spaces and threat mitigation responsibilities. These stakeholders include the seven operating components, the nation's first responder communities, and the critical infrastructure/key resources (CIKR) owners and operators who maintain the backbone of the American economy. It is nowhere more important than to provide these groups with the necessary resources and capabilities that enable them to ensure mission success. Addressing the needs and requirements of DHS' myriad stakeholders continues to be a challenge requiring new ideas to gather resources and innovative technologies and products effective at combating the numerous threats facing our nation.

Many situations arise within the Department, First Responder Community and Private sector where there is a need for widely distributed products. Recognizing this fact, the Department recently began fostering a "Commercialization Mindset"¹ in order to leverage the vast capability and resources of the private sector through innovative "win-win" public-private partnerships stressing the need for detailed requirements. Commercialization represents another "tool in the toolbox" that can be used to provide much needed products and services to the DHS stakeholders. The process of partnering with the private sector to work cooperatively on many of the steps in the system engineering life cycle will allow more groups to be involved in developing competing solutions to DHS' customer needs, when low-unit-volume custom systems are not required. Not only is this a new way of thinking about developing and procuring products, it necessitates clear and precise communications between the public and private sectors.

From a business person's perspective it is important to understand the important actors tasked with ensuring homeland security. Within the Department, there are seven operating components: Transportation Security Administration (TSA), U.S. Customs & Border Protection (CBP), U.S. Citizenship & Immigration Services (USCIS), U.S. Immigration & Customs Enforcement (ICE), U.S. Secret Service (USSS), Federal Emergency Management Agency (FEMA) and the U.S. Coast Guard (USCG). These are the primary components that lead the daily efforts to provide protection to the American people. All other organizational elements within DHS are responsible to enhance, enable and support the mission critical objectives of the Department.

The DHS Science and Technology Directorate (S&T) is the organizational element responsible for understanding and bridging the capability gaps of the operating components that require technology and products to enable these organizations to meet their objectives. S&T is organized with six divisions that focus on the functional aspects of the gang of seven: Explosives, Chemical/Biological, Command, Control & Interoperability, Borders &

¹ See, for example, *Developing Operational Requirements, Version 2, Product Realization Chart, DHS Implements a Commercialization Process* and other valuable resources online at http://www.dhs.gov/xres/programs/gc_1211996620526.shtm

Maritime Security, Human Factors, and Infrastructure & Geophysical. These divisions are tasked to understand the unmet needs and requirements of not only the seven operating components but the first responder community as well as the CIKR owners and operators.

Capstone Integrated Product Teams (IPTs)

The Capstone Integrated Product Teams (IPTs) are chartered to ensure that technologies and products are engineered and integrated into systems aligned to the needs of DHS customers. Capstone IPTs establish a management team that delivers the technological advantage necessary to ensure DHS agency mission success. The Capstone IPT process² is the framework used to determine whether developed capabilities meet operational needs, analyzes gaps in strategic needs and capabilities, and creates programs and projects to close capability gaps and expand mission competencies. This process is a customer-led forum through which the identification of functional capability gaps and the prioritization of these gaps across the Department are formalized. The Capstone IPTs manage the research and development efforts of DHS S&T and enable the proper allocation of resources to the highest priority needs established by the DHS operating components.

Capstone IPTs bring together S&T division heads, acquisition partners and end-users (operating components, field agents, first responders, and CIKR owners and operators) involved in the Research, Development, Testing and Evaluation (RDT&E) and acquisition activities. Working together, the IPT identifies, evaluates and prioritizes the necessary requirements to complete missions successfully. IPTs also assess the technological and system readiness of products that will ultimately be deployed into the field. Figure 1 shows the organization of a Capstone IPT.

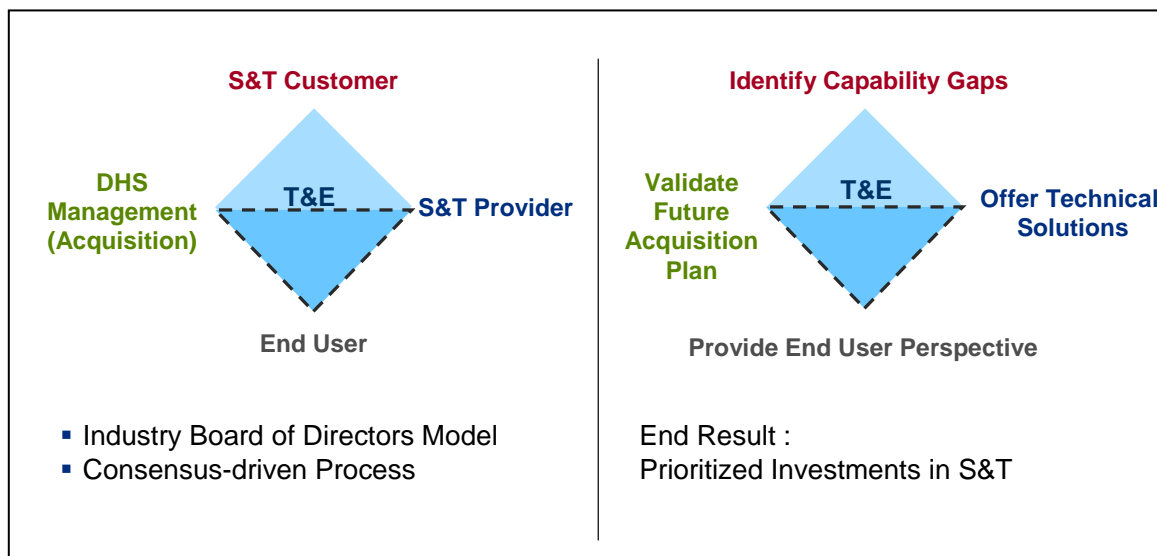


Figure 1. (a) This diagram shows the structure of the Capstone IPT model with (b) the models' output functions carried out by each IPT member.

² Kikla, Richard V. and Cellucci, Thomas A. "Capstone IPTs: Even in Government the Customer Comes First," April 2008.

The formation of the IPT at an early stage allows key stakeholders to identify and address critical capability gaps. Each Capstone IPT has a DHS Operating Component chair or co-chairs. The chair/co-chair, engage throughout the process to identify, define and prioritize current and future requirements and ensure that planned technology and/or product transitions and acquisition programs, commercialization efforts and standards development are optimally suited to their operational requirements. The Capstone IPT process is a model that requires the participation and input from several DHS stakeholders. This collaborative effort centers on the principle that the customer is “the focus” of this process. The product and technology outputs of the Capstone IPT process are customer-requirements-driven from start to finish. The customer is involved throughout the process to ensure that they receive products and technologies specifically aligned to their detailed operating requirements. Ultimately, our customers receive quality products that effectively deliver the necessary, mission-critical capabilities to secure our nation.

Commercialization Office Initiatives at DHS

As a natural extension of the Capstone IPT process, the Department’s Commercialization Office has taken the lead in developing innovative programs and processes that significantly increase the fostering of public-private partnerships to develop and deploy much needed capabilities with the speed-of-execution and efficiency needed to match the demands of DHS’ stakeholders. The Commercialization Office focuses on bringing improved clarity and communication of stakeholders’ needs across the Department and to private sector partners who have resources to assist in product and technology development. Working in a constructive way in which all the participants, including the private sector, public sector, and taxpayer, benefit enables the high probability of expediting the cost effective and efficient development of products and services to meet the unsatisfied needs and wants of the Department, its operating components, first responders and the CIKR owners and operators.

The Commercialization Office, found within S&T’s Office of Transition, is responsible for accelerating the delivery of enhanced technological capabilities to meet the requirements and close the capability gaps to support DHS agencies and its stakeholders in accomplishing their missions. The major activities that enable the accomplishment of the goals of the Commercialization Office are the requirements development initiative, commercialization process, creation of public-private partnerships and outreach to the private sector.

To facilitate the development of new products and technologies a clear understanding is necessary so that efforts are well coordinated and move with a common purpose. To build upon the capability gaps that are outputs of the Capstone IPT process, DHS recognized the importance in developing operational requirements at an early stage in product development. This discipline enables DHS personnel to articulate, in detail, a given problem and its associated requirements. Stakeholders can communicate those needs to both internal and external audiences. This effort addresses a long-standing need for DHS to fully articulate its requirements and explain in detail the capabilities necessary for mission

success. Figure 2 clearly shows how an Operational Requirement Document (ORD) takes a capability gap to “much higher resolution,” a necessary step required for product developers to assist DHS in its goal of expediting the deployment of cost-effective and efficient widely distributed products.

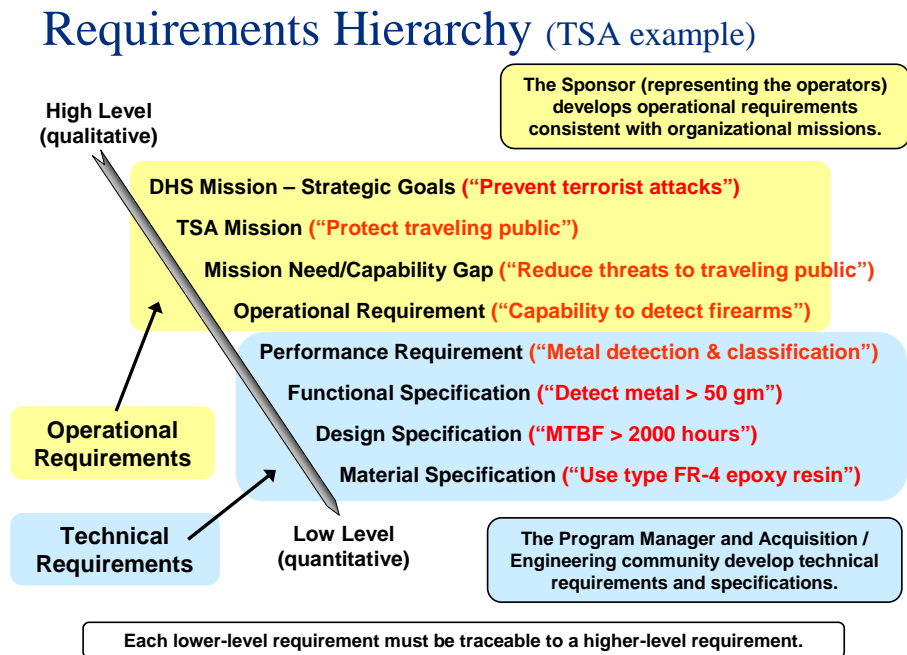


Figure 2. This requirements hierarchy shows the evolution of requirements from a high-level macro set of operational requirements to a low-level micro set of technical requirements. Note that each lower level requirement stems directly from its higher requirement so that all requirements are traceable to the overall DHS Mission.

Through the publication of a number of books including the *Requirements Development Guide* and *Developing Operational Requirements*³, the Commercialization Office provides resources for understanding the importance of requirements and guidelines and templates for creating ORDs. The clear communication of requirements ensures that all parties involved are “on the same page” and that product and technology development moves along clearly defined paths.

Market Potential is Catalyst for Rapid New Product Development

It is important to understand not only the detailed operational requirements necessary to provide DHS stakeholders with mission-critical capabilities, but also understand the volume of potential users of these solutions. DHS itself can represent a substantial potential available market; in many instances requiring hundreds, if not thousands of product or service units to address unsatisfied needs. Couple to this the fact that DHS is connected to many ancillary markets (e.g. first responders, critical infrastructure and key resource owners and operators, etc.) representing large potential available markets, it is evident that

substantial business opportunities exist for the private sector as these large pools of potential customers and users represent the “lifeblood” for businesses (See Figure 3).

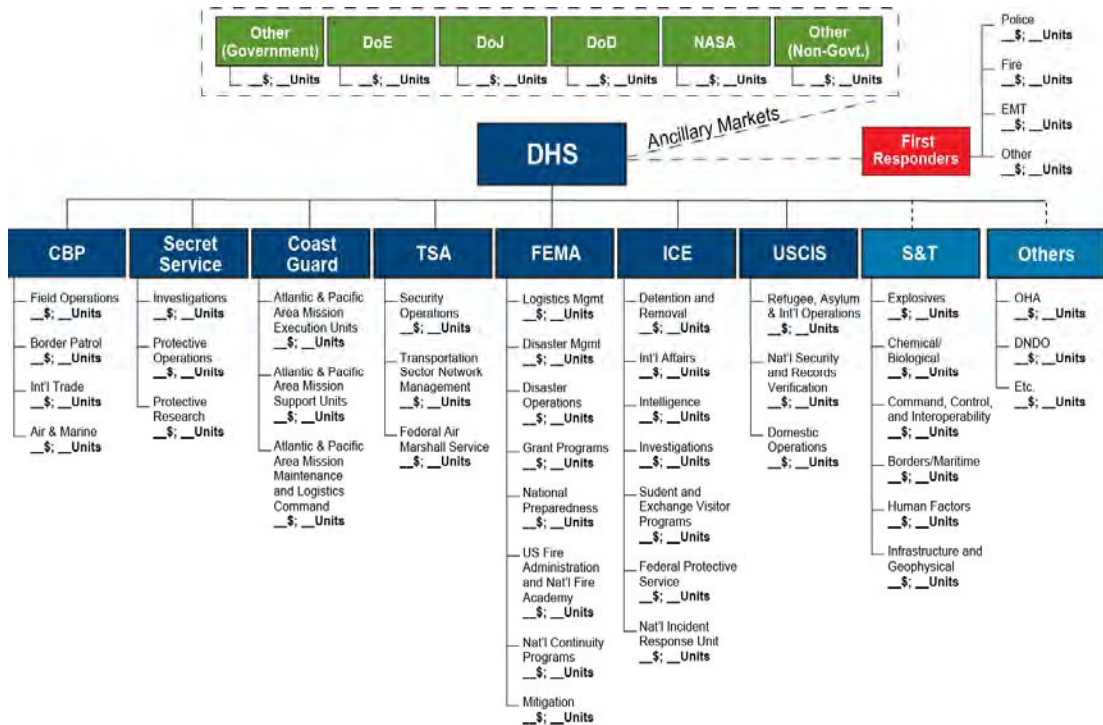


Figure 3 This market potential template maps out many potential available markets to which DHS has direct control and responsibility or acts as a conduit

In order to provide opportunities for a greater number of private sector entities to get involved in addressing the needs of these markets, it is the hope that the market analysis and proper articulation of requirements encourages innovative thinking on the part of the private sector to market valuable solutions given that many needs may be shared across both public and private sector communities.

Keep it Simple Make it Easy

The DHS commercialization process is based upon the simple premise that the private sector is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and resources to such activities, if and when an attractive business case can be made related to large revenue/profit opportunities. Market analyses clearly demonstrate that large potential available markets exist for DHS and its ancillary markets. In order to actively engage with the private sector DHS must share two pieces of critical information: 1. detailed operational requirement(s), and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in the program.

success. Figure 2 clearly shows how an Operational Requirement Document (ORD) takes a capability gap to “much higher resolution,” a necessary step required for product developers to assist DHS in its goal of expediting the deployment of cost-effective and efficient widely distributed products.

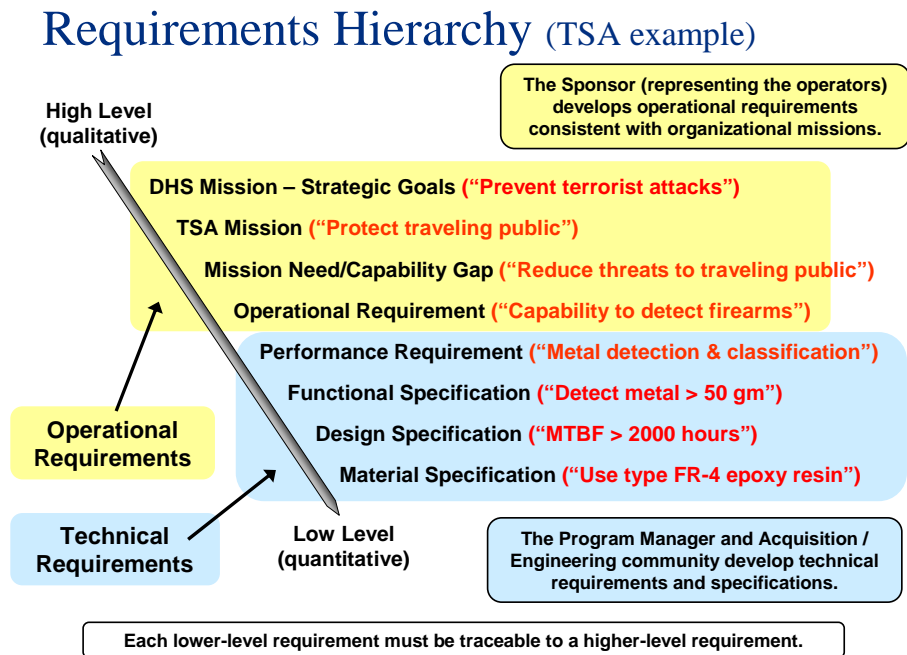


Figure 2. This requirements hierarchy shows the evolution of requirements from a high-level macro set of operational requirements to a low-level micro set of technical requirements. Note that each lower level requirement stems directly from its higher requirement so that all requirements are traceable to the overall DHS Mission.

Through the publication of a number of books including the *Requirements Development Guide* and *Developing Operational Requirements*³, the Commercialization Office provides resources for understanding the importance of requirements and guidelines and templates for creating ORDs. The clear communication of requirements ensures that all parties involved are “on the same page” and that product and technology development moves along clearly defined paths.

Market Potential is Catalyst for Rapid New Product Development

It is important to understand not only the detailed operational requirements necessary to provide DHS stakeholders with mission-critical capabilities, but also understand the volume of potential users of these solutions. DHS itself can represent a substantial potential available market; in many instances requiring hundreds, if not thousands of product or service units to address unsatisfied needs. Couple to this the fact that DHS is connected to many ancillary markets (e.g. first responders, critical infrastructure and key resource owners and operators, etc.) representing large potential available markets, it is evident that

substantial business opportunities exist for the private sector as these large pools of potential customers and users represent the “lifeblood” for businesses (See Figure 3).

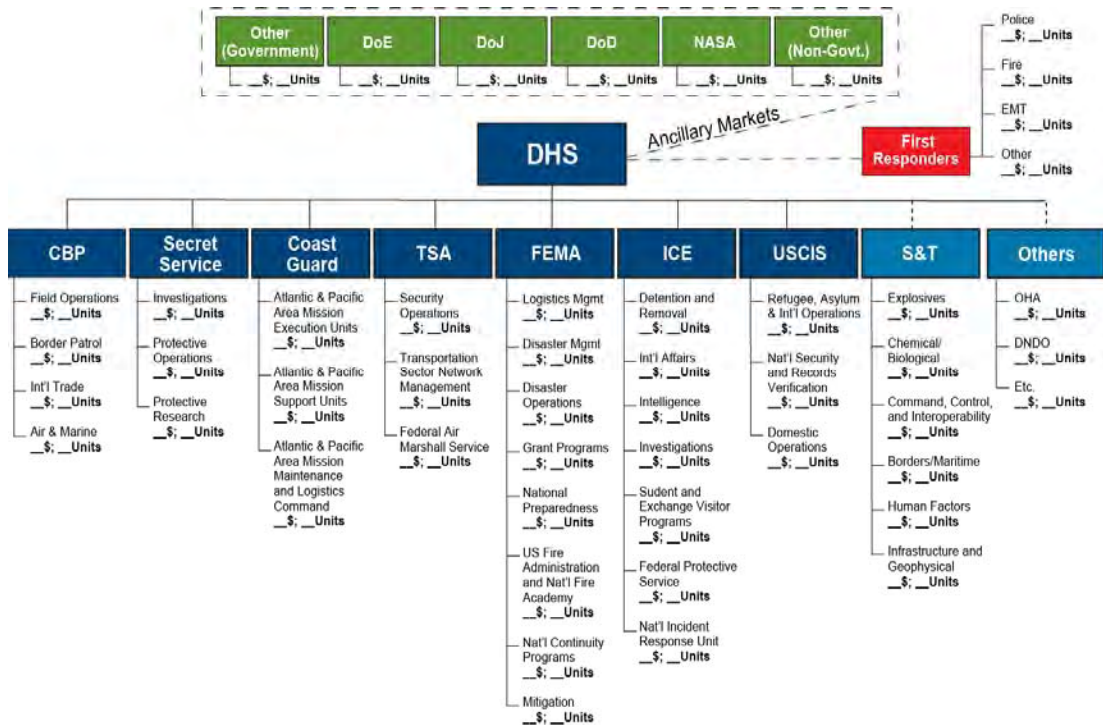


Figure 3 This market potential template maps out many potential available markets to which DHS has direct control and responsibility or acts as a conduit

In order to provide opportunities for a greater number of private sector entities to get involved in addressing the needs of these markets, it is the hope that the market analysis and proper articulation of requirements encourages innovative thinking on the part of the private sector to market valuable solutions given that many needs may be shared across both public and private sector communities.

Keep it Simple Make it Easy

The DHS commercialization process is based upon the simple premise that the private sector is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and resources to such activities, if and when an attractive business case can be made related to large revenue/profit opportunities. Market analyses clearly demonstrate that large potential available markets exist for DHS and its ancillary markets. In order to actively engage with the private sector DHS must share two pieces of critical information: 1. detailed operational requirement(s), and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in the program.

In its new Commercialization model, S&T acts as a facilitator between its customers - DHS' operating components and ancillary markets - and the private sector entities who may potentially develop products for use by DHS' stakeholders. S&T must work with its valued customers in the creation of ORDs that accurately reflect their mission-critical operational requirements through active participation in the requirements development initiatives. S&T also conducts market surveys and technology scans to ensure that needed technical capabilities and/or products can be made accessible in response to the requirements of generated ORDs. This analysis also leads to understandings of the number of potential users and applications for potential solutions. This allows the private sector to understand in a clear and transparent way what the Department and its customers need in order to use their time, money, and resources to create products, services or technologies where market potential is large. Oftentimes, private sector entities have products in development that are closely aligned with current homeland security capability gaps and can be transitioned to the field rapidly and cost-effectively.

SECURE™ and FutureTECH™

The Commercialization Office created two innovative public-private partnership programs to engage the private sector for cooperative product development efforts. The SECURE™ (System Efficacy through Commercialization Utilization Relevance and Evaluation) program seeks to find highly developed (TRL 5-9) private sector product offerings aligned to DHS generated and vetted ORDs posted on the DHS website. Its sister program, FutureTECH™, focuses on the long-term needs of the Department that require the development of new technologies (TRL 1-6) to address future capability gaps. We have demonstrated through the SECURE™ and FutureTECH™ programs that the federal government can engage and influence - in a positive way - the private sector by offering detailed requirements and conservative estimates of market potential. The reason that these partnerships are successful is simple and straightforward. Firms spend significant resources in trying to understand market needs and potential through their business and market development efforts. By offering this information, government saves the private sector both time and money while demonstrating its genuine desire to work cooperatively to develop technologies and products to meet DHS stakeholders' needs in a cost-effective and efficient way that benefits the private and public sectors – but also, most importantly, to the American taxpayers' benefit.

Through the SECURE™ Program, the Department provides to potential solution providers detailed operational requirements and a conservative estimate of the potential available market(s) offered by DHS stakeholders. In exchange for this valuable information, the private sector offers deployable products and services (along with recognized third party test and evaluation data) that meet these stated requirements in an open and free way that creates an ergonomic “clearinghouse of solutions” available to DHS stakeholders. Because of the success and “win-win-win” nature of this program in that it provides benefits for the American taxpayer, the private sector and DHS, DHS-S&T recently introduced the FutureTECH™ Program that describes the long-term capabilities/technologies required by DHS stakeholders.

FutureTECH™ identifies and focuses on the future needs of the Department as fully deployable technologies and capabilities, in some cases, are not readily available in the private sector or Federal government space. While the SECURE™ Program is valuable to all DHS operating components, organizational elements and DHS stakeholders, FutureTECH™ is intended for DHS S&T use only, particularly in the fields/portfolios related to Research and Innovation.

After providing independent third-party testing and evaluation of potential products, services, or technologies to show they do in fact meet or exceed the specifications listed in the detailed operational requirements, private sector entities can potentially enter into a partnership with the Department in order to deliver commercial-off-the-shelf products to the Department's stakeholders. In addition to providing products to DHS and its stakeholders, these partnership programs, SECURE™⁴ and FutureTECH™⁵, give the much needed assurance to the First Responder and CIKR communities that a certified product or service works as specified and is aligned to the requirements document.

Outreach to the Private Sector

In order for these programs to be successful in providing needed products, services, and technologies to DHS and its stakeholders, partnerships with the private sector are imperative. The private sector outreach efforts of the Commercialization Office are designed to provide information to the public on "How to do Business with DHS." Efforts demonstrate the value of engaging in mutually beneficial relationships to provide business opportunities to produce products/services to DHS components and ancillary markets. The private sector outreach efforts of the Commercialization Office center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department.

Through websites⁶, speeches, conferences, seminars, and publications the Commercialization Office is able to provide to the private sector information on partnership opportunities and helpful resources and contacts to foster a public-private partnership. A "full response package" can be requested that includes more background on the SECURE™ and FutureTECH™ programs as well as a template company overview that can be submitted and entered into our repository that is available for the whole Department to review.

Doing business with DHS creates a number of ancillary benefits for the private sector. The communication of detailed requirements and conservative estimates of potential available markets helps guide businesses as they continue to pursue new opportunities. The involvement of the Venture Capital and Angel Investor communities is a critical function in assisting small businesses and start-up companies with innovative new technologies for the

⁴ Cellucci, Thomas A. "Commercialization Office: Offering Transformational Change Beyond DHS," June 2009.

⁵ Cellucci, Thomas A. "FutureTECH: Guidance to Understanding Future DHS S&T Critical Research/Innovation Focus Areas," April 2009.

⁶ See Commercialization Office websites at www.DHS.gov. Homepage found at: http://www.dhs.gov/xabout/structure/gc_1234194479267.shtm.

homeland security market place. These groups are traditionally entrepreneurial seeking opportunities to advance cutting-edge technology with a primary focus on speed-of-execution. Partnerships within the private sector itself are fostered regularly to bring fully deployable solutions to these new markets. Companies are enabled to approach potential partnerships with a stronger business case based on a credible understanding of the needs of their potential customers that show true business opportunities. Funding new and innovative technologies that have the potential to address numerous large markets is an attractive opportunity for venture capitalists and angel investors. In addition, there has been a marked increase in the number of strategic partnerships between small businesses and large companies as each has something to offer.

Small businesses are the “engines of innovation”⁷. These small businesses are creative entities, offering new solutions and ideas to solve many complex challenges. However, many small businesses lack the resources for proper business development and sales development practices. In these cases strategic partnerships offer opportunities to grow sales and market channels that can bring their innovative technologies to the field where they can be of the greatest benefit. Figure 4 below is a benefit analysis demonstrating how all participants receive positive outcomes as a result of fostering public-private partnerships.

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through Private Sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy through creation of jobs and business opportunities	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Potential strategic partnership and commercialization opportunities between small, medium and large businesses result

Figure 4: The Commercialization Office’s public-private partnerships are viewed positively by DHS stakeholders. The success of the program lies in the fact that all participants receive significant benefits.

⁷ Cellucci, Thomas A. “Focus on Small Business: Opportunities Abound for the Engines of Innovation,” March 2009.

Other Business Opportunities within S&T

DHS S&T has many other business opportunities beyond its commercialization efforts and public-private partnerships. DHS S&T relies heavily on the private sector to conduct product and technology development for needed capabilities that may not have large potential available markets. In these cases, traditional Acquisition practices are adopted and a competitive selection process begins. The DHS S&T Solicitations Portal contains a listing of several solicitations on a broad range of topics. Learning about opportunities and submitting applications is often a simple and straightforward process. Please visit <https://baa.st.dhs.gov> for more information.

The SAFETY (Support Anti-Terrorism by Fostering Effective Technologies) Act of 2002 is a congressionally mandated program intended to provide critical incentives for the development and deployment of anti-terrorism technologies by providing protections for vendors of “qualified anti-terrorism technologies.” The SAFETY Act creates systems of “risk management” and “litigation management” to ensure that the threat of liability does not deter potential manufacturers of vendors of anti-terrorism technologies from developing and commercializing technologies that could save lives. Please visit <https://www.safetyact.gov> for more information.

In order to further outreach efforts with potential solutions providers in the first responder markets, the TechSolutions program was established to provide information, resources and technology solutions that address mission capability gaps identified by the emergency response community. The goal of TechSolutions is to field technologies that meet 80% of the operational requirements in a 12 to 15 month time frame at a cost commensurate with the proposal, not to exceed \$1 million per project. Goals will be accomplished through rapid prototyping or the identification of existing technologies that satisfy identified requirements. For more information please visit http://www.dhs.gov/xfrstresp/training/gc_1174057429200.shtm.

Summary

The potential to do business with DHS has never been greater. New programs have opened significant business opportunities to work in cooperative public-private partnerships. The private sector can now play a critical role in developing needed capabilities for DHS’ stakeholders in a freely competitive way that shows demonstrable benefits for many different groups. New collaborative business practices will enable DHS to field fully developed products with a speed-of-execution not seen before in many government programs. Continued participation and engagement through these partnership programs will only increase as more requirements are gathered and shared creating the opportunities necessary for businesses to get involved. The private sector shows everyday its willingness to be an active partner through genuine interest in ensuring that DHS’ stakeholders are better able to carry out their mission and protect the people of the United States. DHS will continue to enable these relationships with the goal of facing the many challenges that lay ahead.

If you have any questions on how to get involved with these public-private partnerships, please send a note to SandT_Commercialization@dhs.gov

Acknowledgement

I would like to acknowledge the valuable assistance of Caroline Greenwood and Mark Protacio in the preparation of this document.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer in Washington, D.C. He leads the private sector outreach initiatives for DHS S&T has written a series of books to facilitate the development and articulation of operational requirements for DHS stakeholders.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





Focus on Small Business

Opportunities abound for “Engines of Innovation.”

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security

March 2009



**Homeland
Security**

Science and Technology

Focus on Small Business

Opportunities abound for “Engines of Innovation.”

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

The Commercialization Office prides itself with the attention it pays to small businesses of all kinds – including minority-owned, HUBZone, veteran-owned and other disadvantaged business. It is well known that much of our nation’s (and the world’s) innovation emanates from small business, but they often find some of their most difficult challenges with raising capital or performing effective market research necessary for business growth. To address these challenges, we have visited and met with thousands of small business owners, CEOs and entrepreneurs/innovators across the United States to inform them of the business opportunities that exist at the U.S. Department of Homeland Security (DHS). In addition, we have developed a series of books recently published by DHS that small businesses can use to augment and enhance their ability to efficiently and cost-effectively develop market-driven products and/or services. We have also produced numerous well-received articles and materials germane to small business. Refer to http://www.dhs.gov/xres/programs/gc_1234200779149.shtm for more detailed information and access to all of these useful resources.

The Commercialization Office continues to travel extensively throughout the United States to meet with small business through our Science and Technology (S&T) Directorate private sector outreach efforts. Statistical information on these efforts is posted to our website and updated on a quarterly basis. It is also important to note that DHS has a number of valuable resources small business may explore. Below is a handy reference for small business:

U.S. Department of Homeland Security and other Federal Contact Information:

DHS and/or Federal Contact	Description	Contact Information
Private Sector Office	Part of the DHS Office of Policy, the Private Sector Office engages individual businesses, trade associations and other non-governmental organizations to foster dialogue with the Department. It also advises the Secretary on prospective policies and regulations and in many cases on their economic impact. The Private Sector Office promotes public-private partnerships and best practices to improve the nation’s homeland security, and promotes Department policies to the private sector.	http://www.dhs.gov/xabout/structure/gc_1166220191042.shtm
Federal Business Opportunities (Fed Biz Opps)	“Virtual marketplace” that captures the official Federal government procurement opportunities allowing contractors to retrieve services posted by government buyers.	https://www.fbo.gov/

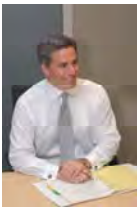
Small Business Innovation Research (SBIR)	SBIR is a set-aside program (2.5% of an agency's extramural budget) for domestic small business concerns to engage in Research/Research and Development (R/R&D) that has the potential for commercialization.	https://www.sbir.dhs.gov/
Small Business Assistance	Provides numerous resources, links and contacts to ensure that small companies have a fair opportunity to compete and be selected for Department of Homeland Security contracts.	http://www.dhs.gov/xopnbiz/smallbusiness/
Mentor-Protégé Program	Designed to motivate and encourage large business prime contractor firms to provide mutually beneficial developmental assistance to small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns.	http://www.dhs.gov/xopnbiz/smallbusiness/editorial_0716.shtm
SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program	An efficient and cost-effective program to foster cooperative "win-win" partnerships between the U.S. Department of Homeland Security and the private sector. The Department works with the private sector to develop products, systems or services aligned to the needs of its operating components, first responders and critical infrastructure/key resources owners and operators – representing in many cases, large potential available markets.	http://www.dhs.gov/xres/programs/gc_1211996620526.shtm

S&T Directorate – Homeland Security:

DHS and/or Federal Contact	Description	Contact Information
TechSolutions Program	Established to provide information, resources and technology solutions that address mission capability gaps identified by the emergency response community. The goal of TechSolutions is to field technologies that meet 80% of the operational requirement, in a 12 to 15 month time frame, at a cost commensurate with the proposal but less than \$1 million per project.	http://www.dhs.gov/xfrstresp/training/gc_1174057429200.shtm
SBIR	Please refer to the description above.	https://www.sbir.dhs.gov/
SAFETY (Support Anti-terrorism by Fostering Effective Technologies) Act	Part of the Homeland Security Act of 2002, the SAFETY Act encourages the development and deployment of anti-terrorism technologies to protect the nation and provide “risk management” and “litigation management” protections for sellers of qualified anti-terrorism technologies and others in the supply and distribution chain.	https://www.safeyact.gov/
Homeland Security Advanced Research Projects Agency (HSARPA)	Manages a broad portfolio of solicitations and proposals for the development of homeland security technology. HSARPA performs this function in part by awarding procurement contracts, grants, cooperative agreements, or other transactions for research or prototypes to public or private entities, businesses, federally funded research and development centers,	https://baa.st.dhs.gov/

	and universities.	
SECURE Program	Please refer to the description above.	http://www.dhs.gov/xres/programs/gc_1211996620526.shtm
Unsolicited Proposals	Composed of several component agencies which handle different types of acquisitions. This Department has several resources, links and contacts if a given small company has products or services which may be of interest to one or more of DHS component agencies.	http://www.dhs.gov/xopnbiz/opportunities/editorial_0617.shtm

To put it simply, the Commercialization Office welcomes the prospect of working with all kinds of small businesses. In fact, we make it a point in ALL of our briefs/presentations to discuss small business opportunities as well as provide seminars and resources on how to raise capital and form strategic partnerships. Feel free to contact the Chief Commercialization Officer (CCO), Dr. Tom Cellucci directly at 202-254-5309 if we can provide any additional information or answer any questions.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published four comprehensive books: *Requirements Development Guide*, *Developing Operational Requirements*, *Developing Operational Requirements (Version 2.0)* and *Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good: DHS's Entry into Commercialization* to aid in effective requirements development and communication for the Department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector. He is also the first federal official on the Council of Competitiveness representing the U.S. Department of Homeland Security.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*





FutureTECH: Guidance to Understanding Future DHS S&T Critical Research/Innovation Focus Areas

New program in the Commercialization Office enables the private sector and others to peer into the critical research/innovation focus areas of interest to the DHS Science and Technology (S&T) Directorate.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security

April 2009



**Homeland
Security**

Science and Technology

FutureTECH: Guidance to Understanding Future DHS S&T Critical Research/Innovation Focus Areas

New program in the Commercialization Office enables the private sector and others to peer into critical research/innovation focus areas of interest to the DHS Science and Technology (S&T) Directorate.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

Due to the popularity of the SECURE Program introduced by the recently formed Commercialization Office, the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate has now introduced a “sister program” called FutureTECH. The SECURE Program leverages the experience and resources of the private sector to develop fully deployable [i.e., technology readiness level nine, (TRL-9)] products and/or services based on DHS generated and vetted detailed operational requirements documents (ORDs) and a conservative estimate of the potential available market (represented by DHS operating components and ancillary markets comprised of first responders, critical infrastructure/key resources (CI/KR) owners/operators and other DHS stakeholders). The FutureTECH Program, on the other hand, is reserved for those critical research/innovation focus areas that could be inserted eventually into DHS acquisition or commercialization programs when development reaches TRL-6 based on metrics and milestones more specific than those of a broad technology need statement alone, yet not as specific as a detailed ORD.

FutureTECH identifies and focuses on the future needs of the Department as fully deployable technologies and capabilities, in many cases, are not readily available in the private sector or Federal government space. While the SECURE Program is valuable to all DHS operating components, organizational elements and DHS stakeholders, FutureTECH is intended for DHS S&T use only, particularly in the fields/portfolios related to Research and Innovation (see for example, http://www.dhs.gov/xabout/structure/editorial_0531.shtm for details on research and innovation activities and programs).

DHS S&T Basic Research Portfolio

The DHS S&T Basic Research Portfolio creates fundamental knowledge for enhancing homeland security, normally at a time frame exceeding 8 years. These efforts emphasize (but are not limited to) university fundamental research and governmental lab discovery and invention. Basic Research programs are executed in the Directorate’s six divisions, facilitated by the Office of National Laboratories and the Office of University Programs and are closely coordinated with other government agencies.

Typically, the basic research efforts at S&T are motivated by one or more of the following:

1. The research addresses an important DHS issue (such as a High-Priority Technology Need) without a viable near-term solution.
2. The research pursues a creative solution that addresses a unique, long-term DHS need that is not addressed elsewhere.
3. The research exploits new scientific breakthroughs (e.g., from universities, laboratories, or industry) that could strengthen homeland security.

The Research Leads in S&T’s six divisions developed Basic Research focus areas that represent the technological areas in which S&T seeks to create and/or exploit new scientific breakthroughs. These focus areas, generated with input from the research community and vetted through S&T’s Research Council, will help guide the direction of the S&T Basic Research Portfolio, within resource constraints, to provide long-term science and technology advances for the benefit of homeland security.

DHS S&T Innovation Portfolio

The DHS S&T Innovation Portfolio focuses on homeland security research and development (R&D) that could lead to significant technology breakthroughs that could greatly enhance DHS operations.

The Office of the Director of Innovation oversees S&T’s Homeland Security Advanced Research Projects Agency (HSARPA). Established by the Homeland Security Act of 2002 (P.L. 107-296), HSARPA funds R&D of homeland security technologies to “support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security; advance the development, testing and evaluation, and deployment of critical homeland security technologies; and accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities.”

Innovation/HSARPA personnel work closely with the Under Secretary for Science and Technology, S&T divisions, DHS components, industry, academia, and other government organizations to determine topic areas for projects. Innovation’s efforts are complementary to S&T’s other programs and projects, pushing scientific limits to address gaps in areas where current technologies and R&D are inadequate or non-existent. Please see Table 1 for a current delineation of Innovation project areas.

Table 1: Description of Innovation Project Areas Categorized as High Impact Technology Solutions (HITS) and High Innovative Prototypical Solutions (HIPS) Projects.

High Impact Technology Solutions (HITS) Projects	
Cell-All Ubiquitous Chem/Bio Detect	Examines proofs-of-concept for integrating miniaturized chemical and biological agent detectors into personal devices, such as cellular telephones, in order to create a widely distributed network for detection, classification and notification in the event of a chemical release, and with possible extensions to detect chemical components of some biological agents. Individual device owners on the network would control the detection and transmission of the data, sensor timing and global positioning satellite (GPS) location information. The goals of this project include significant improvement to chemical and biological detectors’ integration, size, costs, power, maintenance, durability and response

	characteristics.
Wide Areas Surveillance	Focuses on surveillance and tracking in densely populated infrastructure settings and urban landscapes (such as airports, train stations, city streets and squares) to protect the nation's highest priority infrastructure. In FY 2008, the project constructed an array of multiple high-resolution cameras that are digitally integrated into a single view with an overall resolution of 100 megapixels. The system provides high-resolution imagery and allows multiple operators to simultaneously view and manipulate (e.g., zoom and scan) regions of the scene in high-resolution detail while maintaining a full 360-degree field of view. The system includes automated change detection capabilities, and users can rapidly scan video images for forensic analysis. In FY 2009, the project plans to conduct a demonstration to evaluate the effectiveness of the system in a densely populated environment and also significantly advance the system hardware to more than double the current resolution and ultimately improve system cost effectiveness.
Resilient Tunnel Project	The project focuses on designing an inflatable tunnel plug to protect mass transit tunnels from fires, smoke and flooding. In FY 2008, the project initiated a partnership with the Washington Metropolitan Area Transit Authority (WMATA) and conducted a demonstration in a WMATA subway tunnel in August 2008. The results illustrated that a full-scale plug can be inflated quickly and efficiently in a real-world transit environment and that the plug effectively seals against the tunnel walls. In FY 2009, the project plans to conduct numerical modeling to optimize plug structure and performance; construct new small-scale plugs with stronger materials and optimized geometries; and subject these plugs to pressurized testing in the laboratory to simulate tunnel flooding.
Tunnel Detect Project	Develops detection technologies to locate clandestine underground tunnels that are used for cross-border illegal activities such as smuggling. In FY 2008, the project conducted a series of demonstrations of an electromagnetic gradiometer (radio frequency) mounted on an unmanned aircraft system, which is planned for further evaluation by Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) in FY 2009. Research and development activities include incorporating other sensors such as a hyper-spectral camera that detects differences in the environmental characteristics (e.g., moisture) at or near the tunnels that are indicators of the presence of a tunnel. The project initiated a parallel effort to prototype and test advanced ground-penetrating radar for tunnel detection. In FY 2009, S&T will test and demonstrate an advanced ground-penetrating radar and investigate additional technologies by leveraging Department of Defense (DOD) tunnel-detection efforts for border protection applications.
Homeland Innovative Prototypical Solutions (HIPS) Projects	
Future Attribute Screening Technologies Mobile Module (FASTM2) (formerly Future Attribute Screening Technologies) Project	<p>Develops real-time, mobile screening technologies to automatically and remotely detect behavior indicative of intent to cause harm (identified as malintent) at screening checkpoints. In FY 2008, the project identified potential behavioral (illustrative gestures, gait, blinking, eye-gaze, etc.), physiological (change in heart beat, respiration, thermal, etc.), and paralinguistic cues that are likely indicative of malintent and identified remote sensors capable of detecting the associated physiological signals. The feedback from initial peer review and independent, nationally recognized subject matter experts was positive.</p> <p>In FY 2008, the project demonstrated the FAST laboratory module which is a functional test laboratory for the development, integration and implementation of real-time, mobile screening and future sensing technologies. In FY 2009, the project will continue validating and updating the malintent theory, sensors, and the module environment and incorporate the initial elements of data fusion and machine learning to improve screening accuracy. Independent peer review will be an ongoing element of the project to promote objectivity and ensure all aspects of the project are addressed. In FY 2009, the project will conduct an operational demonstration of a real-time intent detection capability.</p>

Hurricane & Storm Surge Mitigation Project	<p>Develops methods to better understand and accurately predict the behavior of a hurricane to help better predict its future track and to reduce the intensity and/or duration of a hurricane or storm. The focus will be on understanding the dynamics of storms as they grow from depressions to full hurricanes, and to try to determine if any of the dynamic variables can be used or manipulated against the storm itself in order to prevent further growth in strength. State and local officials will be able to more accurately and quickly determine which areas to evacuate. This project will focus on discovering variables to affect that could reduce the intensity and/or duration of a hurricane or storm before the storm reaches a point of runaway growth in strength. This project, in partnership with the National Oceanic and Atmospheric Administration (NOAA), will apply knowledge gained in the last 25 years (since the last attempt to modify hurricanes) to understand and model the life-cycle of a hurricane and identify/evaluate the effects of salt seeding, carbon black aerosol, upper ocean cooling, ion generators and monolayer films. The goal is not to stop hurricanes, which are an important part of the natural cycle, but to mitigate damage to life and property.</p>
Levee Strengthening & Damage Mitigation Project	<p>Develops techniques to rapidly repair breaches. Innovation has been able to work with S&T's Infrastructure and Geophysical Division to demonstrate technology for rapid repair.</p> <p>In September of FY 2008, the project successfully demonstrated technologies for rapid repair of levee breaches at the United States Department of Agriculture (USDA) facilities in Stillwater, Oklahoma. This proof-of-concept attracted the attention of potential end users and will lead to the development of full-scale systems. In FY 2009, the project will further develop the rapid repair prototypes for a full-scale demonstration and develop a concept of operations.</p>
Resilient Electric Grid (REG) Project	<p>Demonstrates Inherently Fault Current Limiting High-Temperature Superconducting (IFCL-HTS) technologies for reliable distribution and protection of electrical power. This technology would save millions-to-billions of dollars by providing continuous power in the event of a terrorist attack, brown outs, or black outs, and provide more efficient power distribution in the course of normal day-to-day operations.</p> <p>In FY 2008, the project conducted proof-of-concept demonstrations of a 3-meter, IFCL-HTS cable. The first demonstration in December 2007 showed that an HTS cable could transmit power with no electrical losses and simultaneously prevent cascading failures under normal conditions (i.e., no current overloads). Subsequently, the February 2008 demonstration was an important Go/No-go decision point because it confirmed that the HTS cable provides significant fault current limiting and also identified potential challenges due to higher than expected Alternating Current (AC) losses in the HTS cable. The project team conducted additional experiments and demonstrations in May 2008 to isolate the causes of the higher than expected AC losses and a third 3-meter cable was tested in August 2008. The results justified going forward with a 25-meter demonstration in FY 2009 at Oak Ridge National Laboratory. The project team successfully demonstrated the fault current limiting capability of the 25 meter test cable in March 2009. The project is planning an in-grid demonstration of the IFCL-HTS cable in the Manhattan grid for evaluation under operational conditions.</p>
Safe Container (SAFECON) Project –	<p>Investigates various technologies, including probe systems that detect and identify dangerous cargo and could be mounted on cranes used for on- and off-loading ship-carried containers. SAFECON also looks for sensors and specialized container materials designed to make screening more effective. The project aims to provide the capability to scan containers entering the country while minimizing the impacts to commerce; high reliability, high-throughput detection of weapons of mass destruction (WMD), explosives, contraband and human cargo; and immediate detection and isolation of</p>

	<p>suspected threat containers.</p> <p>In FY 2008, the project completed threat characterization and container characterization studies at the ports of Charleston, South Carolina and Boston, Massachusetts to inform decisions on sensor and prototype development. SAFECON also began the development of a remote vapor inspection system using advanced laser techniques to detect and identify threat chemicals and explosives. In FY 2009, the project will demonstrate integrated chemical and explosives sensor performance in a laboratory.</p> <p>In addition to the approach described above for rapid detection while the container is being moved by crane, DHS S&T is also looking at an alternative approach that takes advantage of the long transit time most shipping containers experience as they transit from their port of origin to the United States. This part of the SAFECON program is called Time Recorded Ubiquitous Sensor Technology (TRUST). It would allow detection of Chemical, Biological, Radiological, Nuclear, Explosive and personnel (CBRNE/P) threats within any container while in its port of embarkation or in transit, thus enabling authorities to route a suspect container to a safe location for special handling and an entry determination prior to entering a U.S. port.</p>
<p>Scalable Common Operational Picture Experiment (SCOPE) Project</p>	<p>Leverages an existing effort by DOD. The DOD effort, called the Joint Concept Technology Demonstration for Global Observer, is developing a high-altitude, long-endurance unmanned aircraft system (GO UAS). This aircraft-mounted system will enable homeland security personnel at the federal, state and local levels to collectively see what is happening during an event and potentially provide a communication platform for regions where infrastructure has been destroyed. This will allow responders to quickly understand the extent of a natural disaster or terrorist attack, enable communications and provide sufficient time to make critical decisions and mount a coordinated response. Today, no such capability exists.</p> <p>In FY 2008, the project developed and integrated modular sensor and communication payloads and began the formal GO Critical Design Review (CDR). In early FY 2009, the project successfully completed CDR and will conduct a series of operational utility assessments that will serve as a proof-of-concept for DHS operational security needs.</p>
<p>Rapid Liquid Component Detector (MagViz) Project</p>	<p>Uses ultra-low-field Magnetic Resonance Imaging (MRI) technology to screen baggage for liquid explosives. To mitigate the liquid explosives threat, airline passengers currently must pack liquids or gels (such as certain toiletries and medicines) in containers that are 3 ounces or smaller. Those containers must be placed in a 1-quart-sized, clear plastic, zip-top bag; and only 1-bag-per-traveller is allowed. These are known as “3-1-1 bags,” which undergo an X-ray inspection and possibly secondary screening using multiple methods, such as visual inspection. The goal of MagViz is to eliminate the 3-1-1 rule and allow passengers to place liquids in their carry-on baggage. MagViz will scan and identify individual materials that may be packaged together or separately as they go through the scanning process and evaluate them against a database that will differentiate between those items considered safe for carrying onto an aircraft (e.g., benign liquids and gels like mouthwash, toothpaste, etc.) and harmful ones. The intent is for the detection of liquids in baggage to be non-contact and to occur at the same rate as current X-ray machines, thus not hindering passenger throughput.</p> <p>In FY 2008, the project built and demonstrated a 3-1-1 bag-screening prototype in a lab. The August 2008 laboratory demonstration of this system showed that it can recognize and compare a wider range of liquids to a stored database and discriminate between harmful and benign liquids and gels with greater sensitivity and discrimination capability than previous demonstrations by overcoming operational challenges such as the orientation of containers and containers within containers.</p>

	<p>In December 2008, the project conducted a full demonstration of the 3-1-1 bag-screening prototype in an airport to assess its ability to detect liquid explosives within baggage in an operational setting. This public demonstration successfully showed that the prototype could distinguish between liquids in an operational environment overcoming challenges that could affect its sensitivity. Also in FY 2009, the project will build an exhaustive database of liquids through magnetic characterization and further address clutter in the operational environment; evaluate the capability of MagViz to detect dangerous solids; and demonstrate the capability of its research prototype to inspect at a depth of 20 cm. In FY 2010, the project plans to continue building the magnetic characterization database of liquids and demonstrate the capability of MagViz to seamlessly screen segregated liquids (without the 3-1-1 bag constraint) in an operational environment and subsequently evaluate termination or transition options.</p>
--	---

DHS S&T Transition Portfolio

The DHS S&T Transition Portfolio focuses on the identification, evaluation and management of the near-term technology portfolio to develop and deliver advanced capabilities to DHS operating components, stakeholders and end-users for homeland security improvements. The Capstone Integrated Product Team (IPT) process is the framework that determines that developed capabilities meet operational needs, analyzes gaps in strategic needs and capabilities, determines operational requirements, and develops programs and projects to close capability gaps and expand mission competencies. This process is a DHS customer-led forum through which the identification of functional capability gaps and the prioritization of these gaps across the Department are formalized. The IPTs oversee the research and development efforts of DHS S&T and enable the proper allocation of resources to the highest priority needs established by the DHS operating components and first responders.

FutureTECH Program

Scope:

This program enables DHS S&T to efficiently and cost-effectively leverage the resources, skills, experience and productivity of the private sector and other non-DHS entities to develop technologies/capabilities in alignment with research/innovation focus areas obtained from DHS S&T (see above for examples). These technologies/capabilities, when successfully developed, may ultimately be used by DHS, the first responder community, critical infrastructure/key resources (CI/KR) owners/operators and other DHS stakeholders. In essence, FutureTECH provides a "window of visibility" or "preview" of research/innovation focus areas that DHS and its stakeholders believe are essential in future products and services where detailed operational requirements documents (ORDs) can not be fully developed at this time. The program also provides insight into areas where Independent Research and Development (IRAD) monies could be spent by firms possessing funding to address DHS research/innovation focus areas.

Analogous to the popular SECURE Program, FutureTECH is another innovative private-public partnership and outreach program that outlines focus areas for which current technology only exists at earlier stages on the technology readiness scale (TRL

1-6). Technologies developed in alignment to stated focus areas could lead to cost-effective and efficient product development (TRL 7-9) when detailed requirements contained in ORDs are available. Like the SECURE Program, DHS will provide information to the public in an open and free way. The private sector and other non-DHS entities may use their own resources (including IRAD) to develop technologies/capabilities that will be of potential benefit to the DHS mission. Like the SECURE Program, DHS may enter into a simple CRADA (Cooperative Research and Development Agreement) document with an organization that shows it has the ability to deliver technology aligned with the research/innovation focus area sought after by DHS.

To state it simply, the SECURE Program focuses on product/service development to create products and services to protect our nation in the shorter term, while FutureTECH focuses on science and technology development related to critical research/innovation focus areas. Like all of the Commercialization Office's programs, all parties "win" in the FutureTECH Program--the private sector and other non-DHS entities by receiving valuable insight into future research/innovation focus areas needed by DHS and its stakeholders. DHS "wins" because it will leverage the valuable skills, experience and resources of the private sector and others to expedite efficient and cost-effective technology development; the non-DHS entities "win" because they receive valuable information useful for their own strategic plans; and most importantly, all American taxpayers "win" because this innovative partnership yields valuable technologies/capabilities aligned with research/innovation focus areas developed in a more cost-effective and efficient way saving taxpayer money.

Overall Process:

Figure 1 is a graphical representation of the overall outreach process the Commercialization Office continues to implement to stimulate and engage the private sector and other non-DHS entities to use their resources to rapidly develop technology aligned with research/innovation focus areas that can yield significant benefits for DHS S&T with a speed-of-execution not typically observed in the public sector.

Outreach to the Private Sector

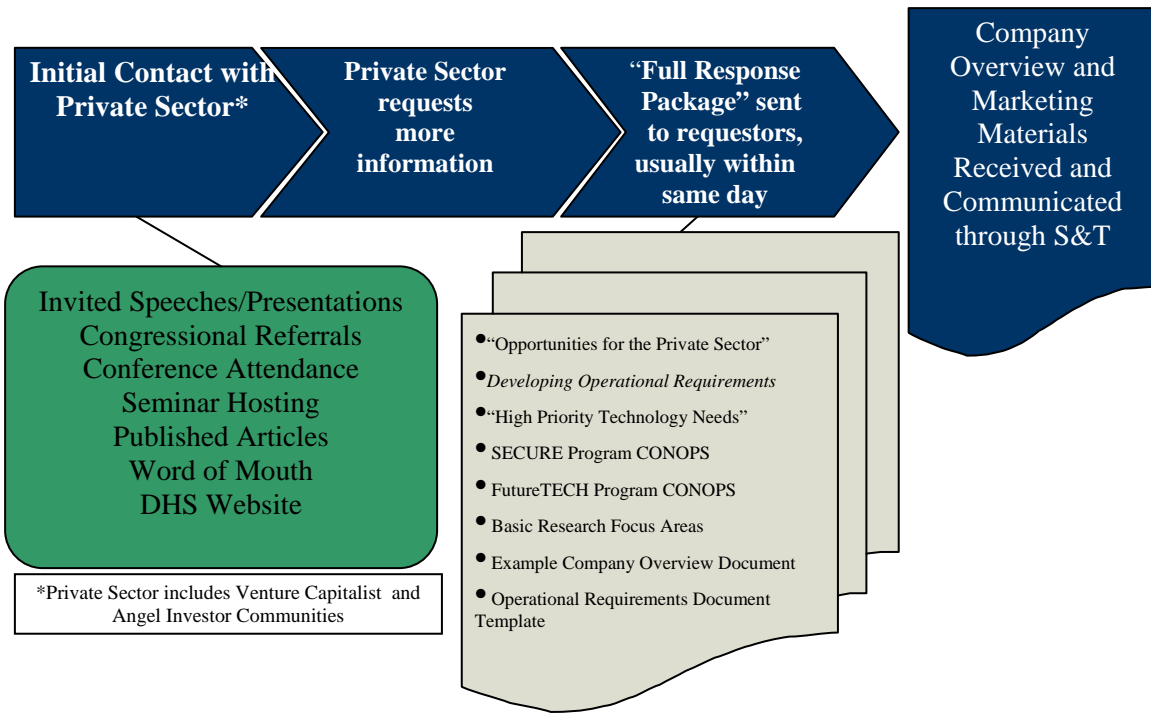


Figure 1: Overview of S&T Directorate Private Sector Outreach Process



Program Process:

DHS S&T will provide this FutureTECH vehicle by which the private sector and other non-DHS entities can identify or develop technology aligned with research/innovation focus areas ranging from TRL-1 through TRL-6 (not fully developed TRL-9 products and/or services) based on DHS S&T's insight and knowledge mainly through its Research and Innovation portfolios/areas.

This approach enables DHS S&T to collaborate on the development of technology aligned with several research/innovation focus areas in an open and free way. The private sector and other non-DHS entities receive information on what new technologies will be required over-the-horizon to protect our nation, removing much of the “guess work” normally associated with predicting future needs.

As with the popular SECURE Program, DHS will review third party, recognized test and evaluation data to ensure that all milestones/objectives of an executed CRADA agreement are met and DHS will place a given research/innovation focus area solution developed by an entity on the FutureTECH website demonstrating that the research/innovation focus area has met DHS's broadly defined requirements (in contrast to the SECURE Program where products or services must demonstrate compliance to detailed operational requirements contained in an ORD).



Expression of Interest:

In the adherence to fairness of opportunity, and in order to capitalize on the free-market system, DHS S&T intends to publish this program and all ancillary requirements documents/information on the DHS website. These materials will be accessible by ALL. Given this information, the private sector and other non-DHS entities may contact DHS S&T if they are interested in developing or enhancing their technology within a research/innovation focus area in cooperation with DHS S&T. Potential research/innovation focus areas for this program (along with a simple CRADA agreement used in the SECURE Program) are provided on our website. The private sector organization or non-DHS entity must provide DHS S&T with basic, non-proprietary business information, contact information and demonstrate their potential alignment to widely available DHS S&T research/innovation requirements that are more detailed than what are commonly referred to as technology need statements, yet not as detailed as a well-defined ORD.



Acceptance:

In order to be fully considered by DHS S&T for cooperative research/innovation focus area technology development:

- An entity must demonstrate they either possess technology at TRL-1 or higher (i.e. basic research) or possess the ability to develop a technology aligned with the research/innovation focus area to TRL-6 for later technology insertion into a potential acquisition or commercialization program.
- The private sector and other non-DHS entities must propose a research/innovation focus area technology development effort that has clear and substantial alignment with any published DHS S&T requirements delineated above.

A DHS committee will be established to review the private sector and/or non-DHS entities’ potential alignment to DHS research/innovation focus areas, and monitor the mutually-agreed-upon roles and responsibilities of partnership participants. The committee will consider these and other DHS proprietary metrics for determining which opportunities to pursue.



CRADA:

The private sector and/or non-DHS entity and DHS S&T could execute a simple, straightforward and binding CRADA whereby the non-DHS entity details milestones with dates and, in most cases, agrees to bear full and total financial responsibility to develop its technology aligned within the research/innovation focus area to a TRL-6 state. Under the Stevenson-Wydler Act (which is the statutory authority enabling DHS to enter into CRADAs), agencies may not contribute funds under a CRADA; however, they may contribute know-how, expertise, materials and equipment. It is important to mention that the execution of a CRADA agreement is at the sole discretion of the corresponding DHS S&T program manager. Additionally, a CRADA with DHS S&T will not necessarily lead to any follow-on contract actions or solicitations by DHS or other government agencies. Any solicitations for funding agreements related to technology areas collaborated upon in a CRADA would be subject to full and open competition. DHS S&T will publish on the DHS S&T website the factual finding(s) of any final assessment. DHS S&T has the right to cancel an agreement if the non-DHS entity does not fulfill/achieve its milestones or performance objectives by the mutually-agreed-upon dates.

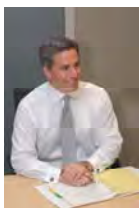


Publication of Results:

It is apparent that the private sector and other non-DHS entities highly value DHS S&T's potential assessment of a given technology's recognized third-party test and evaluation (T&E) data. DHS S&T will openly publish summary findings and an acknowledgement of an entity's attainment of performance objectives on the DHS public web portal for review by the DHS operating components, first responder communities, CI/KR owners/operators and other potential users.

Acknowledgement

Many individuals contributed to the development of this article and the new FutureTECH Program, primarily the scientists, engineers, program managers and others within the S&T Directorate. Special thanks to the Research Leads within the divisions and the rest of the Research Council for development of the Basic Research focus areas. Ryan Policay is also thanked for his substantial contributions to this worthy effort.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published four comprehensive books: *Requirements Development Guide*, *Developing Operational Requirements*, *Developing Operational Requirements (Version 2.0)* and *Harnessing the Valuable Experience and Resources of the Private Sector for the Public Good: DHS's Entry into Commercialization* to aid in effective requirements development and communication for

the Department. He possesses extensive experience as a senior executive and Board Member in high-technology firms in the private sector. He is also the first federal official on the Council of Competitiveness representing the U.S. Department of Homeland Security.

Doing Business with DHS S&T:

All U.S. Government business opportunities can be found at www.fedbizopps.gov.

- **HSARPA:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to the Long Range Broad Agency Announcement solicitation, where multiple awards are anticipated and will be based upon the proposal evaluation, funds availability, and other programmatic considerations. Also link to Representative High Priority Technology Areas, where DHS areas of interest can be found. <http://www.hsarpabaa.com>
- **Small Business Innovation Research(SBIR):** SBIR's goal is to increase the participation of innovative and creative small businesses in Federal Research/Research and Development (R/R&D) programs and challenge industry to bring innovative homeland security solutions to reality. <http://www.sbir.dhs.gov>
- **SAFETY Act:** The SAFETY Act enables the development and deployment of qualified anti-terrorism technologies and provides important legal liability protections for manufacturers and sellers of effective technologies. <https://www.safetyact.gov/>
- **TechSolutions:** The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders by fielding prototypical solutions within 12 months at a cost less than \$1M per project. www.dhs.gov/techsolutions
- **Commercialization:** The mission of S&T's commercialization efforts is to identify, evaluate, and commercialize technologies that meet the specific operational requirements of DHS operating components and first responder communities. The commercialization efforts actively reach out to the private sector to establish mutually beneficial working relationships to facilitate cost-effective and efficient product development efforts. Please contact Chief Commercialization Officer Tom Cellucci at S&T-Commercialization@dhs.gov.



*From Science and Technology...
Security and Trust*



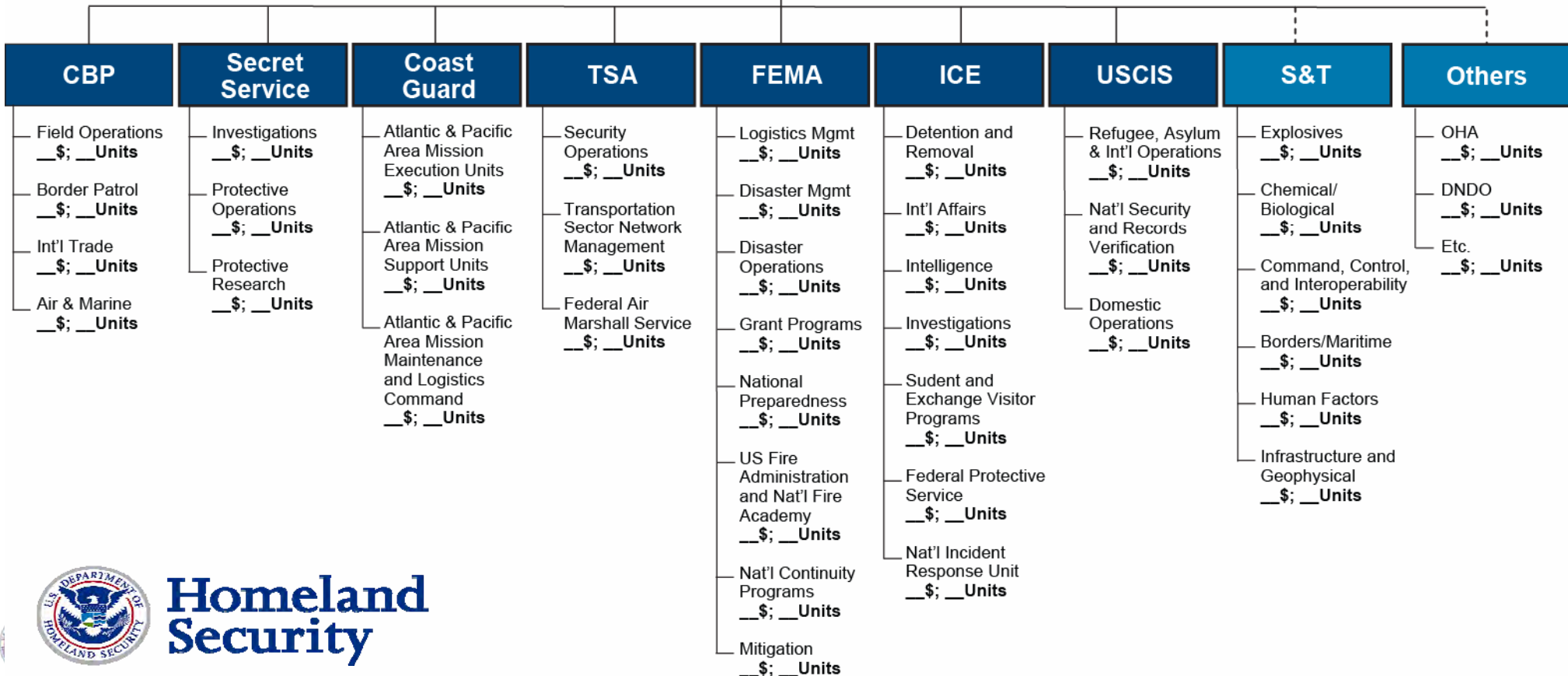
Market Potential Template



DHS

Ancillary Markets

First Responders



Homeland Security

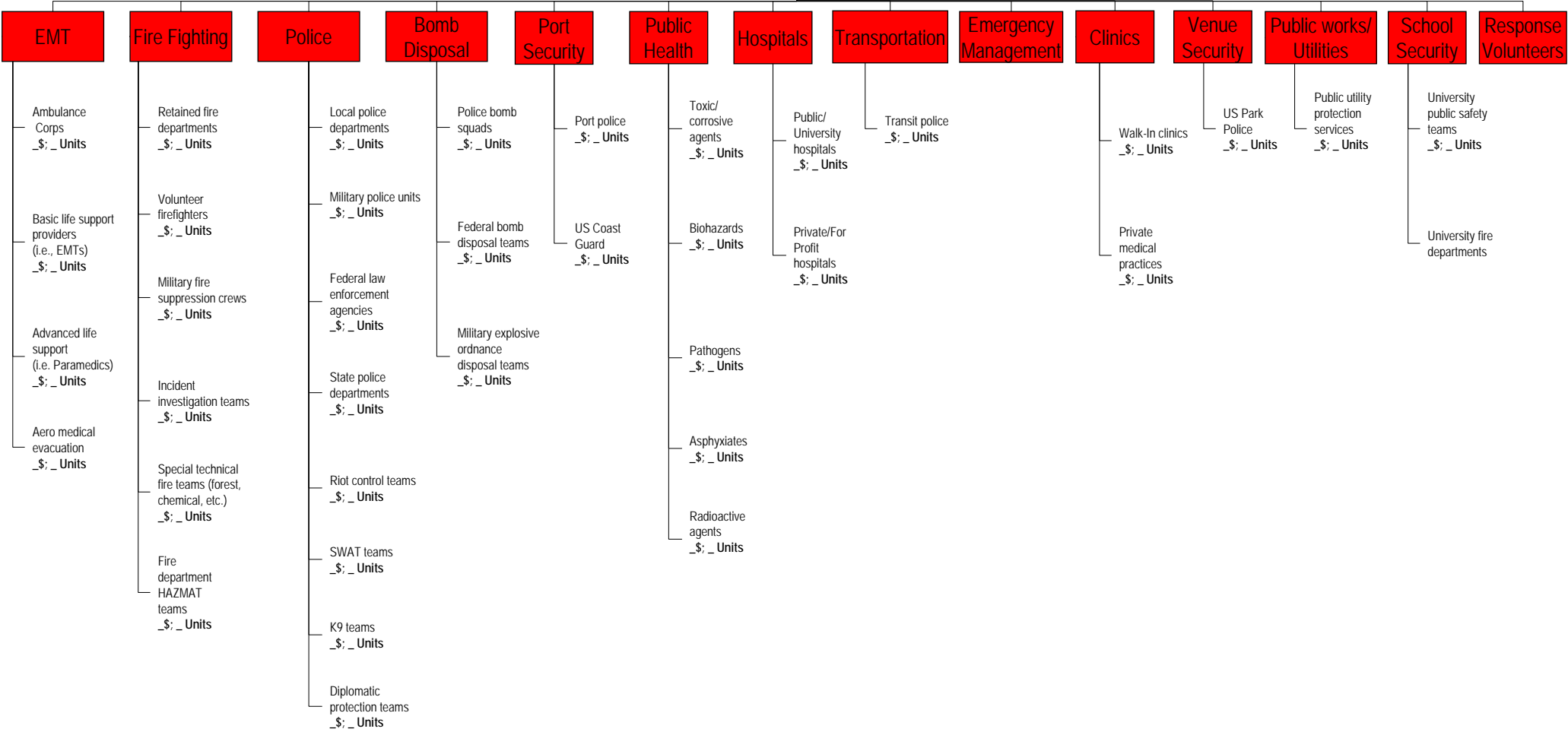
Critical Infrastructure Key Resources (CIKR)

Agriculture and Food	Defense Industrial Base	Energy	Public Health and Healthcare	National Monuments and Icons	Banking and Finance	Water	Chemical	Commercial facilities	Emergency Services	Materials, Reactors and	Telecommunications	Critical Manufacturing	Postal and Shipping Services	Transportation	Information Technology
Food Retail _\$_; _ Units	Defense Contractors _\$_; _ Units	Coal mining operations _\$_; _ Units	Public/University hospitals _\$_; _ Units	Guided tour services _\$_; _ Units	Credit lending institutions _\$_; _ Units	Public utilities _\$_; _ Units	Inorganic chemical production _\$_; _ Units	Hotels _\$_; _ Units	Fire Departments _\$_; _ Units	Electric utilities _\$_; _ Units	Telephone/Cellular services _\$_; _ Units	Iron and Steel mills _\$_; _ Units	United States Postal Service _\$_; _ Units	AMTRAK _\$_; _ Units	Hardware providers _\$_; _ Units
Farm Equipment _\$_; _ Units	Industry analysis _\$_; _ Units	Coal power plants _\$_; _ Units	Private/For Profit hospitals _\$_; _ Units	Travel services _\$_; _ Units	Commercial banking _\$_; _ Units	Desalinization plants _\$_; _ Units	Organic industrial production _\$_; _ Units	Shopping centers _\$_; _ Units	Law enforcement agencies _\$_; _ Units	Reactor and associated materials _\$_; _ Units	Satellite data transmission _\$_; _ Units	Aluminum production and processing _\$_; _ Units	High volume document and parcel shipping _\$_; _ Units	Commuter rail _\$_; _ Units	IT Conglomerates _\$_; _ Units
Meat/Poultry Processing _\$_; _ Units	Think tanks/research institutions _\$_; _ Units	Coal equipment manufacturers _\$_; _ Units	Clinics _\$_; _ Units	Lodging/Hotel _\$_; _ Units	Private equity _\$_; _ Units	Treatment plants _\$_; _ Units	Ceramics _\$_; _ Units	Stadiums and sport arenas _\$_; _ Units	Search and rescue teams _\$_; _ Units	University and educational institutions _\$_; _ Units	Broadcasting entities _\$_; _ Units	Nonferrous metal production and processing _\$_; _ Units	Container shipping services _\$_; _ Units	Intracity rail services _\$_; _ Units	Semiconductor production _\$_; _ Units
Food Processing _\$_; _ Units	University partnership programs _\$_; _ Units	Hydroelectric _\$_; _ Units	Private medical practices _\$_; _ Units	Guest services/tourist hospitality _\$_; _ Units	Consumer banking _\$_; _ Units	Equipment manufacturers _\$_; _ Units	Petrochemicals _\$_; _ Units	Schools _\$_; _ Units	Ambulance companies _\$_; _ Units	Control systems _\$_; _ Units	Broadcast equipment manufacturing _\$_; _ Units	Engine, Turbine and Power transmission _\$_; _ Units	Marine shipping _\$_; _ Units	Commercial airline _\$_; _ Units	Electronics manufacture _\$_; _ Units
Dairy Processing _\$_; _ Units	National laboratories _\$_; _ Units	Dam operations _\$_; _ Units	Medical laboratories _\$_; _ Units	People moving services _\$_; _ Units	Building societies/Private banks _\$_; _ Units	Pipe and water control device manufacturers _\$_; _ Units	Agrochemicals _\$_; _ Units	Commercial office buildings _\$_; _ Units	Mountain/Cave/ Mine rescue teams _\$_; _ Units	Nuclear safety systems _\$_; _ Units	Radio equipment manufacturing _\$_; _ Units	Marine shipping _\$_; _ Units	Trucking industry _\$_; _ Units	Private air services _\$_; _ Units	IT services _\$_; _ Units
Dairy Farms _\$_; _ Units		Wind power _\$_; _ Units	Pharmaceutical _\$_; _ Units	Queuing equipment makers _\$_; _ Units	Merchant banks _\$_; _ Units		Polymers _\$_; _ Units	Museums _\$_; _ Units	Other technical rescue teams _\$_; _ Units	Waste disposal services _\$_; _ Units	Electrical equipment manufacturing _\$_; _ Units	Airborne shipping _\$_; _ Units	Cruise lines _\$_; _ Units	Server and network hardware _\$_; _ Units	IT services _\$_; _ Units
Ranching _\$_; _ Units		Solar power _\$_; _ Units	Health insurance _\$_; _ Units	Private security _\$_; _ Units	Global financial services firms _\$_; _ Units		Elastomer production _\$_; _ Units	Zoos and Aquariums _\$_; _ Units	Bomb disposal units _\$_; _ Units	Uranium processors _\$_; _ Units	Motor Vehicle manufacturing _\$_; _ Units	Trucking industry _\$_; _ Units	Subway systems _\$_; _ Units	Server and network hardware _\$_; _ Units	IT services _\$_; _ Units
Organic Farming/Sustainable Agriculture _\$_; _ Units		Public utilities companies _\$_; _ Units	Medical material providers _\$_; _ Units		Community development _\$_; _ Units		Oleochemicals _\$_; _ Units	Public Libraries _\$_; _ Units	Blood/Organ transplant supply _\$_; _ Units	Protective garment manufacturers _\$_; _ Units	High speed data transmission _\$_; _ Units	Aerospace product & parts manufacturing _\$_; _ Units	Subway systems _\$_; _ Units	Server and network hardware _\$_; _ Units	IT services _\$_; _ Units
Traditional Planning _\$_; _ Units		Oil companies _\$_; _ Units	Medical equipment manufacturers _\$_; _ Units		Community banks _\$_; _ Units		Explosives _\$_; _ Units	Amusement parks _\$_; _ Units	Amateur radio emergency comms _\$_; _ Units	Print media _\$_; _ Units	Internet service providers _\$_; _ Units	Railroad rolling stock _\$_; _ Units	Long-haul maritime shipping _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
Commercial fishing _\$_; _ Units			Medical technology manufacturers _\$_; _ Units		Savings and Loans _\$_; _ Units		Fragrance production _\$_; _ Units		Public utility protection providers _\$_; _ Units	Internet technology providers _\$_; _ Units	Other Transportation equipment _\$_; _ Units	Distribution services _\$_; _ Units	Display/digital TV _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
			Biotechnology _\$_; _ Units		Credit unions _\$_; _ Units		Chemical wholesale _\$_; _ Units		Emergency Road services _\$_; _ Units				Freight rail service _\$_; _ Units	Software production _\$_; _ Units	IT services _\$_; _ Units
					Insurance companies _\$_; _ Units		Exotic chemicals _\$_; _ Units		Emergency Social services _\$_; _ Units				Automobile travel _\$_; _ Units	Gaming _\$_; _ Units	Information security _\$_; _ Units
					Insurance brokerages _\$_; _ Units				Community emergency response teams _\$_; _ Units				Roads, Highways, bridges and tunnels _\$_; _ Units	Information security _\$_; _ Units	Information security _\$_; _ Units
					Reinsurance companies _\$_; _ Units				Disaster relief _\$_; _ Units					Information security _\$_; _ Units	Information security _\$_; _ Units
					Stock brokerages _\$_; _ Units				Famine relief teams _\$_; _ Units					Information security _\$_; _ Units	Information security _\$_; _ Units
					Capital market banks _\$_; _ Units				Poison Control units _\$_; _ Units					Information security _\$_; _ Units	Information security _\$_; _ Units
					Custody services _\$_; _ Units				Animal control teams _\$_; _ Units					Information security _\$_; _ Units	Information security _\$_; _ Units
					Angel investment _\$_; _ Units				Wildlife services _\$_; _ Units					Information security _\$_; _ Units	Information security _\$_; _ Units
					Venture capital _\$_; _ Units									Information security _\$_; _ Units	Information security _\$_; _ Units



Homeland Security

First Responders





Product Realization Guide

Table with columns for DHS S&T Portfolio, Technology Phase, Technology Readiness Level (TRL), Manufacturing Readiness Level (MRL), Key Objectives, Key Deliverables, Management Review, and program labels (FutureTECH, SAFETY Act, SECURE Program).

U.S. Department of Homeland Security Commercialization Office January 2010 Legend: Black Type - Primary Public Sector Blue Type - Primary Private Sector Red Type - Manufacturing related activities Definition: Commercialization - the process of developing markets and producing and delivering products or services for sale.

SECURE™ Program (TRL 5-9)

FutureTECH™ Program (TRL 1-6)

SAFETY Act Designation: TRL 6-9 & Certification: TRL9-Deployment

Product Realization Guide

- This guide is designed as a resource to assist in project execution relative to technology development. This systematic approach facilitates efficient and effective product development by reducing the risk of unidentified errors and product development shortfalls. It is intended that this guide be incorporated as an easy-to-use resource to ensure due diligence throughout the product development life cycle. Please note that this guide presents a general framework for product realization and that individual projects may require a tailored product realization path.
- Additional information on TRLs, MRLs and other product development related resources can be found at the following links:
 - Technology Readiness Assessment (TRA) Deskbook, July 2009 - <https://acc.dau.mil/CommunityBrowser.aspx?id=18545>
 - Definition of Technology Readiness Levels - http://esto.nasa.gov/files/TRL_definitions.pdf
 - Technology Readiness Levels NASA white paper, April 1995 - <http://www.hq.nasa.gov/office/codeq/trl/trl.pdf>
 - Using the Technology Readiness Levels Scale to Support Technology Management in the DoD's ATD/STO Environments, September 2002 - <http://www.sei.cmu.edu/reports/02sr027.pdf>
 - TRL Calculator - <https://acc.dau.mil/CommunityBrowser.aspx?id=25811>
 - Manufacturing Readiness Assessment (MRA) Deskbook, May 2009 - <https://acc.dau.mil/CommunityBrowser.aspx?id=182129>
 - Assessing Manufacturing Risk - <https://acc.dau.mil/CommunityBrowser.aspx?id=18231>
 - GAO Report – Defense Acquisitions: Assessment of Selected Major Weapons Programs - <http://www.gao.gov/new.items/d06391.pdf>
 - About Manufacturing Readiness Assessments - <http://www.wpafb.af.mil/library/factsheets/factsheet.asp?id=9757>



Developing Operational Requirements

A Guide to the Cost-Effective and Efficient
Communication of Needs

Version 2.0

November 2008



Homeland
Security

Editor:
Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer



November 2008



Tom Cellucci

Please find enclosed the expanded version of our popular book entitled “Developing Operational Requirements,” which was published in May 2008 by the U.S. Department of Homeland Security (DHS). You will find many new and updated sections related to developing detailed operational requirements, numerous examples of Operational Requirements Documents (ORDs) and information on our recently implemented Commercialization initiative to cost effectively and efficiently develop products and services for DHS and other related users found in the first responder and critical infrastructure/key resources communities.

Please allow me to take this opportunity to thank the countless people in the Department, members of other various Federal Agencies and the private sector for providing us with valuable feedback on our earlier editions to make this edition even more useful to organizations both within and outside of the Department. I especially thank Mark Protacio, Sam Francis, Ryan Policay and Adam Porter-Price for their individual contributions in the preparation of the materials for this book.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security
Science and Technology Directorate

DHS S&T Commercialization Office

The DHS Science and Technology (S&T) Commercialization efforts are headed by the Chief Commercialization Officer (CCO), a position created in August 2007 within the Transition Office in S&T. The mission of the Commercialization Office is to develop and execute programs and processes that identify, evaluate and commercialize technology through the development of widely distributed products and/or services that meet the operational requirements of the Department of Homeland Security's Operating Components, First Responder community and other Department stakeholders when required. A primary function of the Commercialization Office is developing and managing S&T's outreach effort with the private sector to establish and foster mutually beneficial working relationships leading to the fielding of technology-based products and services to secure the nation. In order to achieve its mission, the Commercialization Office has organized the following initiatives to gather, articulate, communicate and facilitate the development of products and services based upon detailed operational requirements received from DHS' operating components and stakeholders:

Requirements Development Initiative – Efforts that enable the detailed articulation of operational requirements across the Department are implemented to ensure the accurate and timely development and deployment of products and services to aid in the implementation of the mission-critical objectives of the Operating Components, First Responders and other DHS stakeholders.

Commercialization Process – A new “hybrid” commercialization model has been created that combines the best attributes of the well-known Acquisition and “pure” Commercialization models. This hybrid model begins with DHS needs assessment and results in widely distributed products and services for use by DHS and its wide range of stakeholders.

SECURE Program – An innovative public-private sector partnership based on DHS's new commercialization model. DHS S&T conducts private sector outreach efforts to communicate DHS requirements along with potential available market information to create business case scenarios for possible private sector investment in technology and product development aligned to DHS needs.

S&T Private Sector Outreach – One of the key roles of the Chief Commercialization Officer is to act as a liaison with the private sector connecting DHS requirements and potential technology-based solutions offered by industry. Outreach efforts center on notifying the private sector about opportunities that exist for partnership to address the needs of the Department and its stakeholders. Several articles have been written about our Commercialization efforts. Outreach efforts are conducted through invited briefs to a number of venues reaching small, medium and large businesses. Efforts also extend to regularly meeting with minority, disadvantaged and HUB Zone groups as evidenced from our Private Sector Outreach Statistics.

Table of Contents

DEVELOPING OPERATIONAL REQUIREMENTS.....	1
DHS S&T COMMERCIALIZATION OFFICE	3
TABLE OF CONTENTS	4
INTRODUCTION	6
Product Realization	7
Why Requirements?	8
The Requirements Hierarchy and Traceability	10
Characteristics of Good Requirements	12
Developing Operational Requirements (ORDs): Customer Input.....	13
Addressing Requirements versus Proposing Solutions.....	19
Operational Requirements Document Template:.....	20
DHS Implements a Commercialization Process to Harness Requirements.....	25
Conservative Estimates of Potential Available Markets	26
Summary.....	30
Additional Requirements Development Readings	30
APPENDIX A: ORD EXAMPLES	33
APPENDIX B: MAKING IT EASIER TO WORK WITH DHS (ARTICLE)	131
APPENDIX C: BRIDGING THE COMMUNICATIONS GAP (ARTICLE).....	140
APPENDIX D: COMMERCIALIZATION: IT'S NOT BUSINESS AS USUAL AT DHS S&T (ARTICLE)	148
APPENDIX E: PARTNERSHIP PROGRAM BENEFITS TAXPAYERS, PRIVATE AND PUBLIC SECTORS (ARTICLE).....	157
APPENDIX F: COMMERCIALIZATION BRIEFING TO INDUSTRY	161
APPENDIX G: CAPABILITY GAP-BASED THINKING	184
APPENDIX H: PRODUCT REALIZATION CHART.....	195
APPENDIX I: MARKET POTENTIAL TEMPLATES	197
APPENDIX J: REQUIREMENTS DEVELOPMENT GUIDE (APRIL 2008)	

List of Figures

Figure 1. The requirements hierarchy	10
Figure 2. The contents of an Operational Requirements Document.....	13
Figure 3. The Market Potential Template.....	26

Introduction

The purpose of this guide is simple and straightforward: to enable the reader to articulate detailed requirements or needs and effectively communicate them (either internally within DHS or externally to other Federal agencies or the private sector) through an Operational Requirements Document (ORD) vehicle. Often, we have heard expressions like “It all boils down to a lack of communications,” or “We’re not sure what you need,” or “DHS has been difficult to work with because they really don’t have a clear picture of their problems, needs or requirements.” We can remedy this situation by implementing some fundamental practices in a disciplined manner.

A well-written ORD can be an effective vehicle or tool to relay the needs of a given component, group or agency in an easily understood format to sedulously avoid the countless hours of time and other resources wasted speculating needs. Research conclusively shows that the foremost reason why programs or projects do not succeed is due to the lack of detailed requirements at the initiation of a program or project. Efforts invested up front to develop a clear understanding of the requirements pay dividends in the positive outcome of programs -- not to mention the savings in both time and money in corrective actions taken to get a program back on track (if it is even possible!).

We intend to make writing an ORD simple and easy. To that end, we have provided in this book an easy-to-follow ORD template, along with several real world examples of ORDs. In the numerous appendixes accompanying this book, you will find articles and briefings that provide additional context to the role that creating detailed operational requirements play in effective product realization. For your convenience, we have also included Appendix J, which contains the original *Requirements Development Guide* (April 2008) for those interested in a more detailed discussion on requirements development and product development life cycles.

If you have any questions or need any assistance – any at all – please feel free to contact Dr. Thomas A. Cellucci, DHS-S&T Chief Commercialization Officer at Thomas.Cellucci@dhs.gov.

Product Realization

If you think about it, there are numerous examples in our professional and private lives where the lack of communication or unclear terminology has created misunderstandings, problems and a myriad of other issues. As in any worthwhile pursuit, effective communication is critical in the cost-effective and efficient interactions between various parties seeking a mutually beneficial relationship or partnership.

At every step of product development, it is critical to understand and meet user needs. The Commercialization Office has created a Product Realization Chart that is a useful guide that shows the due diligence necessary for the productive development of products or services (See Appendix H). Product development is not a trivial effort; but with proper planning, tracking and communication, successful product development can yield measurable positive results and provide DHS operating components with resources necessary to carry out their mission-critical objectives to protect our country.

The initial phase of product realization is a mission needs assessment. This assessment should be conducted relative to the overall mission for a given organization. This exercise identifies capabilities needed to perform required functions, highlights deficiencies in a functional capability and documents the results of the analysis. Some of these capabilities may already be addressed with existing products, systems or services currently accessible by an organization. Additionally, a mission needs assessment serves to identify deficiencies in current and projected capabilities. In the event that current products are not able to address a particular capability; a capability gap exists. Briefly, capability gaps are defined by the difference between current operational capabilities and those necessary capabilities needed to perform mission-critical objectives that remain unsatisfied. Capability gaps must be listed in terms of an overall need to perform a specific task and should avoid explaining how that task should be achieved. See appendix G for further reading.

For example, faced with the problem of potential intruders to a sensitive facility, we might define the requirement as “build a wall” whereas the real requirement is “detect, thwart, and capture intruders.” Our wall might “thwart” intruders (or might not, if they’re adept at tunneling), but it would not detect them or facilitate their capture. In short, the solution would not solve the problem.



The robust capability gap to “detect, thwart, and capture intruders” includes no preconceived solutions and prompts us to analyze alternative conceptual solutions and choose the best.

One way to ensure that we are defining a problem, rather than a solution is to begin the statement of the requirement with the phrase “we need the capability to ...” It’s nearly impossible to complete this sentence with a solution (“a wall”), and much easier to complete the sentence with a problem (“capability to detect intruders”). Capability gaps and requirements should address what a system should do, rather than how to do it. This approach is sometimes called capability-based planning. It is a very simple, yet powerful concept.

Properly defining clear and concise capability gaps is a necessary first step in product realization. This high-level understanding of a problem is a key part in the communication of needs. One may find that capability gaps are oftentimes common across multiple cross-sections of DHS operating components and supporting elements such as the first responder community and private sector critical infrastructure owner/operators. Discovering these commonalities is a fundamental aspect of the DHS S&T Capstone IPT Process, which seeks to reduce duplication of efforts and expedite product transition. See Appendix B for further information.

Why Requirements?

A *requirement* is an attribute of a product, service or system necessary to produce an outcome(s) that satisfies the needs of a person, group or organization. Requirements therefore define “the problem.” In contrast, “the solution” is defined by technical *specifications*.

Defining requirements is the process of determining what to make before making it. Requirements definition creates a method in which appropriate decisions about product or system functionality and performance can be made before investing the time and money to develop it. Understanding requirements early removes a great deal of guesswork in the planning stages and helps to ensure that the end-users and product developers are “on the same page.”

Requirements provide criteria against which solutions can be tested and evaluated. They offer detailed metrics that can be used to objectively measure a possible solution’s effectiveness, ensuring informed purchasing decisions on products, systems or services that achieve the stated operational goals. A detailed requirements analysis can uncover hidden requirements as well as discover common problems across programs and various DHS operating components. Detailed operational requirements will guide product development so that solutions specifications actively solve the stated problems.

We could save ourselves a lot of work if we jump straight to “the solution” without defining “the problem.” Why don’t we do that? Because if we take that shortcut we are

likely to find that our solution may not be the best choice among possible alternatives or, even worse we're likely to find that our "solution" doesn't even solve the problem!

Defining requirements and adhering to developing solutions to address those needs is often referred to as "requirements-pull." In this situation, user requirements drive product development and guide the path forward as the requirements dictate. This is a powerful circumstance in which fulfilling requirements becomes the central focus of product development and no possible solution is disregarded given it facilitates

At the other extreme from the "requirements-pull", approach is its opposite: "technology push." Here we start with a solution (perhaps a new technology) and see what problems it might enable us to solve. The danger in this approach is to become enamored of "the solution" and neglect to ensure that it actually solves a problem. With technology push, it is likely that actual user requirements may be modified, or even ignored in order to "force-fit" the desired solution. A historical example was the product known as Picture Phone introduced (and discontinued) in the 1960s when the advance of telecommunications technology first made possible the transmission and display of video as well as voice. Picture Phone, which allowed telephone users to see each other during a call, was a technological success but a market disaster. It turned out that callers generally don't want to be seen, as a bit of unbiased market analysis would have disclosed.

Technology push should not be ignored, but if the goal is successful transition to the field with acceptable risk, the technology being pushed must be compared with alternative solutions against a real set of user requirements.

Aside from assuring that the "solution" actually solves the "problem," requirements-driven design has a further advantage in that the requirements provide criteria against which a product's successful development can be measured. Specifically, if the product was developed to address a set of quantified operational requirements, then its success is measured by Operational Test and Evaluation (OT&E) to validate that an end-user can use the product and achieve the stated operational goals.

Prior to OT&E, it is common practice to subject products to Developmental Test and Evaluation (DT&E). The purpose of DT&E is to verify that the product meets its technical specifications, which are the engineers' interpretation of the operational requirements. Such DT&E does not obviate the need for OT&E, which validates that the engineers' solution is not only technically successfully but also represents a successful interpretation of the end users' needs, satisfying the original operational requirements (not just the technical specifications) when operated by representative users.

Often requirements are stated in terms of "threshold values" and "objective values," where the "objective value" is the desired performance and the "threshold value" is the minimum acceptable performance. This formalism is useful in allowing stretch goals to be asserted without saddling the system development with unacceptable risk.

The Requirements Hierarchy and Traceability

To reiterate the definitions above, the documents that govern product realization include requirements, which define the problem, and specifications, which define the solution. Nevertheless, the hierarchy of requirements and specifications is more complex than that simple dichotomy, as depicted in Figure 1.

The hierarchy is divided into two domains, operational requirements and technical requirements, highlighted in yellow and blue in the figure, representing the “problem space” and the “solution space” respectively. The DHS Operating Component, representing the end users in the field (the operators), is responsible for all operational requirements, from the top-level mission requirements to the detailed system-level operational requirements. A system developer is responsible for translating the operational requirements into a system solution, documented in a hierarchy of technical specifications.

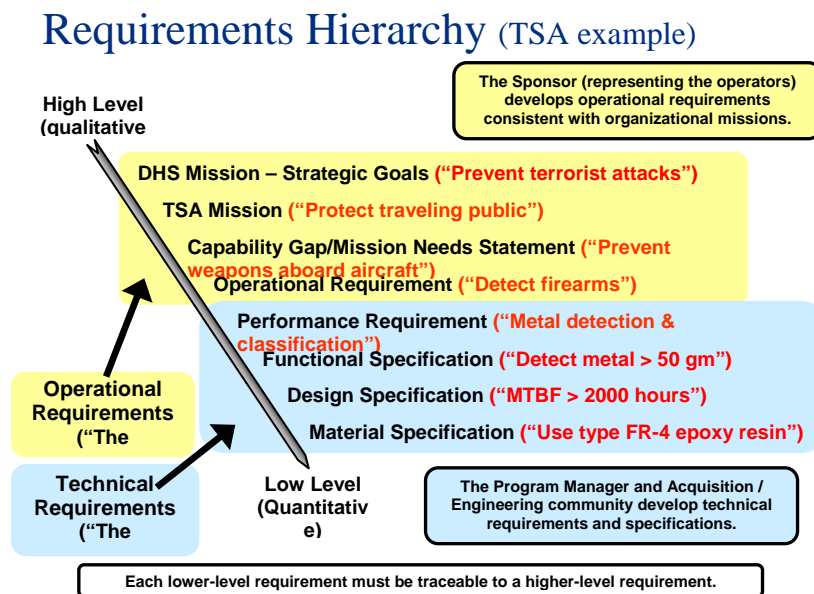


Figure 1. The requirements hierarchy

The highest-level type of technical “specification” is actually called a performance “requirement.” A performance requirement actually represents a bridge from operational requirements to the engineering interpretation of those requirements. Put another way, in the course of developing a new system it is necessary to transform the system operational requirements, which are stated from a given Operating Component’s perspective as required outcomes of system action, into a set of system performance requirements, which are stated in terms of engineering characteristics.

Working through the requirements hierarchy, requirements development is the process of decomposing the problems broadly outlined in the capability gaps gleaned from the mission needs assessment.

The requirements and specifications are described below, first those that define the problem and then those that define the solution:

- **Problem Definition**

- **Mission Needs Statement (MNS)** is required by the DHS *Investment Review Process* (Management Directive 1400, Appendix G) and is developed by the DHS sponsor (S&T's customer) who represents the end users. The MNS provides a high-level description of the mission need (or, equivalently, capability gap), and is used to justify the initiation of an Acquisition program.
- **Operational Requirements Document (ORD)** is also required by the DHS *Investment Review Process* and, like the MNS, is developed by the DHS sponsor. The ORD specifies operational requirements and a concept of operations (CONOPS), written from the point of view of the end user. The ORD is independent of any particular implementation, should not refer to any specific technologies and does not commit the developers to a design.

- **Solution Definition**

- **Performance Requirements** represent a bridge between the operationally oriented view of the system defined in the ORD and an engineering-oriented view required to define the solution. Performance requirements are an interpretation, not a replacement of operational requirements. Performance requirements define the functions that the system *and its subsystems* must perform to achieve the operational objectives and define the performance parameters for each function. These definitions are in engineering rather than operational terms.
- **Functional Specifications** define the system solution functionally, though not physically. Sometimes called the "system specification" or "A-Spec," these specifications define functions at the system, subsystem, *and component level* including:
 - Configuration, organization, and interfaces between system elements
 - Performance characteristics and compatibility requirements
 - Human engineering
 - Security and safety
 - Reliability, maintainability and availability
 - Support requirements such as shipping, handling, storage, training and special facilities
- **Design Specifications** convert the functional specifications of *what* the system is to do into a specification of *how* the required functions are to be

implemented in hardware and software. The design specifications therefore govern the materialization of the system components.

- **Material Specifications** are an example of lower-level supporting specifications that support the higher-level specifications. Material specifications define the required properties of materials and parts used to fabricate the system. Other supporting specifications include **Process Specifications** (defining required properties of fabrication processes such as soldering and welding) and **Product Specifications** (defining required properties of non-developmental items to be procured commercially).

Characteristics of Good Requirements

Requirements engineering is difficult and time-consuming, but must be done well if the final product or system is to be judged by the end users as successful. From the International Council of Systems Engineers (INCOSE) Requirements Working Group¹, here are eight attributes of good requirements:

- Necessary: Can the system meet prioritized, real needs without it? If yes, the requirement isn't necessary.
- Verifiable: Can one ensure that the requirement is met in the system? If not, the requirement should be removed or revised.
- Unambiguous: Can the requirement be interpreted in more than one way? If yes, the requirement should be clarified or removed. Ambiguous or poorly worded requirements can lead to serious misunderstandings and needless rework.
- Complete: Are all conditions under which the requirement applies stated? In addition, does the specification include all known requirements?
- Consistent: Can the requirement be met without conflicting with any other requirement? If not, the requirement should be revised or removed.
- Traceable: Is the origin (source) of the requirement known, and is there a clear path from the requirement back to its origin?
- Concise: Is the requirement stated simply and clearly?
- Standard constructs: Requirements are stated as imperative needs using "shall." Statements indicating "goals" or using the words "will" or "should" are not imperatives.

¹ Kar, Pradip and Bailey, Michelle. Characteristics of Good Requirements. International Council of Systems Engineers, Requirements Working Group. INCOSE Symposium, 1996. Found online: <http://www.afis.fr/nav/gt/ie/doc/Articles/CHARACTE.HTM>.

Developing Operational Requirements (ORDs): Customer Input

So far, we've discussed operational requirements but have not provided any insight into how to develop them. In an effort to provide a basic framework for the articulation and documentation of operational requirements, the Operational Requirements Document (ORD) was created. ORDs provide a clear definition and articulation of a given problem, providing several layers of information that comprise the overall problem. Using resources such as this book and the accompanying template, we have tried to simplify and streamline the process of communicating requirements. ORDs can be used in Acquisition, Procurement, Commercialization and Outreach Programs –any situation that dictates detailed requirements (e.g. RFQ, BAA, RFP, RFI, etc.). It's clear to see that it's cost-effective and efficient for both DHS and all of its stakeholders to communicate needs clearly and effectively.

Let's first look at the contents of a typical Operational Requirements Document (ORD) shown in Figure 2.

OPERATIONAL REQUIREMENTS DOCUMENT

- 1.0 General Description of Operational Capability
 - 1.1. Capability Gap
 - 1.2. Overall Mission Area Description
 - 1.3. Description of the Proposed System
 - 1.4. Supporting Analysis
 - 1.5. Mission the Proposed System Will Accomplish
 - 1.6. Operational and Support Concept
 - 1.6.1. Concept of Operations
 - 1.6.2. Support Concept
- 2.0 Threat
- 3.0 Existing System Shortfalls
- 4.0 Capabilities Required
 - 4.1 Operational Performance Parameters
 - 4.2 Key Performance Parameters (KPPs)
 - 4.3 System Performance
 - 4.3.1 Mission Scenarios
 - 4.3.2 System Performance Parameters
 - 4.3.3 Interoperability
 - 4.3.4 Human Interface Requirements
 - 4.3.5 Logistics and Readiness
 - 4.3.6 Other System Characteristics
- 5.0 System Support
 - 5.1 Maintenance
 - 5.2 Supply
 - 5.3 Support Equipment
 - 5.4 Training
 - 5.5 Transportation and Facilities
- 6.0 Force Structure
- 7.0 Schedule
- 8.0 System Affordability
- Appendixes
- Glossary

Figure 2. The contents of an Operational Requirements Document

The complexity of the intended system and its operational context will govern the required level of detail in the ORD. The most difficult sections to develop are probably Section 4.0, which describes the capabilities required of the system to be developed, and Section 1.6, which describes the operational and support concepts.

There is no “silver bullet” to solve the potential challenges in developing an ORD, but since the issues are universal, there is a wealth of literature that offers approaches to requirements development. As an example, here are nine requirements-elicitation techniques described in the *Business Analyst Body of Knowledge* (from the International Institute of Business Analysis)².

1. Brainstorming
 - Purpose
 - An excellent way of eliciting many creative ideas for an area of interest. Structured brainstorming produces numerous creative ideas.
 - Strengths
 - Able to elicit many ideas in a short time period.
 - Non-judgmental environment enables outside-the-box thinking.
 - Weaknesses
 - Dependent on participants’ creativity.
2. Document Analysis
 - Purpose
 - Used if the objective is to gather details of the “As Is” environment such as existing standard procedures or attributes that need to be included in a new system.
 - Strengths
 - Not starting from a blank page.
 - Leveraging existing materials to discover and/or confirm requirements.
 - A means to crosscheck requirements from other elicitation techniques such as interviews, job shadowing, surveys or focus groups.
 - Weaknesses
 - Limited to “as-is” perspective.
 - Existing documentation may not be up-to-date or valid.
 - Can be a time-consuming and even tedious process to locate the relevant information.

² International Institute of Business Analysis. *A Guide to the Business Analyst Body of Knowledge*, Release 1.6. 2006. Found online: http://www.theiiba.org/Content/NavigationMenu/Learning/BodyofKnowledge/Version16/BOKV1_6.pdf.

3. Focus Group

○ Purpose

- A means to elicit ideas and attitudes about a specific product, service or opportunity in an interactive group environment. The participants share their impressions, preferences and needs, guided by a moderator.

○ Strengths

- Ability to elicit data from a group of people in a single session saves time and costs as compared to conducting individual interviews with the same number of people.
- Effective for learning people's attitudes, experiences and desires.
- Active discussion and the ability to ask others questions creates an environment where participants can consider their personal view in relation to other perspectives.

○ Weaknesses

- In the group setting, participants may be concerned about issues of trust, or may be unwilling to discuss sensitive or personal topics.
- Data collected (what people say) may not be consistent with how people actually behave.
- If the group is too homogenous, the group's responses may not represent the complete set of requirements.
- A skilled moderator is needed to manage the group interactions and discussions.
- It may be difficult to schedule the group for the same date and time.

4. Interface Analysis

○ Purpose

- An interface is a connection between two components. Most systems require one or more interfaces with external parties, systems or devices. Interface analysis is initiated by project managers and analysts to reach agreement with the stakeholders on what interfaces are needed. Subsequent analysis uncovers the detailed requirements for each interface.

○ Strengths

- The elicitation of the interfaces' functional requirements early in the system life cycle provides valuable details for project management:
 - Impact on delivery date. Knowing what interfaces are needed, their complexity and testing needs enables more accurate project planning and potential savings in time and cost.
 - Collaboration with other systems or projects. If the interface to an existing system, product or device and the interface already exist, it may not be easily changed. If the interface is new, then the ownership, development and testing of the interface needs to be addressed and coordinated in both projects' plan. In either case, eliciting the interface requirements will require negotiation and cooperation between the owning systems.

- Weaknesses
 - Does not provide an understanding of the total system or operational concept since this technique only exposes the inputs, outputs and key data elements related to the interfaces.
- 5. Interview
 - Purpose
 - A systematic approach to elicit information from a person or group of people in an informal or formal setting by asking relevant questions and documenting the responses.
 - Strengths
 - Encourages participation and establishes rapport with the stakeholder.
 - Simple, direct technique that can be used in varying situations.
 - Allows the interviewer and participant to have full discussions and explanations of the questions and answers.
 - Enables observations of non-verbal behavior.
 - The interviewer can ask follow-up and probing questions to confirm own understanding.
 - Maintain focus using clear objectives for the interview that are agreed upon by all participants and can be met in the time allotted.
 - Weaknesses
 - Interviews are not an ideal means of reaching consensus across a group of stakeholders.
 - Requires considerable commitment and involvement of the participants.
 - Training is required to conduct good interviews. Unstructured interviews, especially, require special skills. Facilitation/virtual facilitation and active listening are a few of them.
 - Depth of follow-on questions may be dependent on the interviewer's knowledge of the operational domain.
 - Transcription and analysis of interview data can be complex and expensive.
 - Resulting documentation is subject to interviewer's interpretation.
- 6. Observation
 - Purpose
 - A means to elicit requirements by assessing the operational environment. This technique is appropriate when documenting details about current operations or if the project intends to enhance or change a current operational concept.
 - Strengths
 - Provides a realistic and practical insight into field operations by getting a hands-on feel for current operations.

- Elicits details of informal communication and ways people actually work around the system that may not be documented anywhere.
 - Weaknesses
 - Only possible for existing operations.
 - Could be time-consuming.
 - May be disruptive to the person being shadowed.
 - Unusual exceptions and critical situations that happen infrequently may not occur during the observation.
 - May not well work if current operations involve a lot of intellectual work or other work that is not easily observable.
- 7. Prototyping
 - Purpose
 - Prototyping, when used as an elicitation technique, aims to uncover and visualize user requirements before the system is designed or developed.
 - Strengths
 - Supports users who are more comfortable and effective at articulating their needs by using pictures or hands-on prototypes, as prototyping lets them “see” the future system’s interface.
 - A prototype allows for early user interaction and feedback.
 - A throwaway prototype is an inexpensive means to quickly uncover and confirm user interface requirements.
 - A revolutionary prototype can demonstrate what is feasible with existing technology, and where there may be technical gaps.
 - An evolutionary prototype provides a vehicle for designers and developers to learn about the users’ interface needs and to evolve system requirements.
 - Weaknesses
 - Depending on the complexity of the target system, using prototyping to elicit requirements can take considerable time if the process is bogged down by the “how’s” rather than “what’s”.
 - Assumptions about the underlying technology may need to be made in order to present a starting prototype.
 - A prototype may lead users to set unrealistic expectations of the delivered system’s performance, reliability and usability characteristics.
- 8. Requirements Workshop
 - Purpose
 - A requirements workshop is a structured way to capture requirements. A workshop may be used to scope, discover, define, prioritize and reach closure on requirements for the target system. Well-run workshops are considered one of the most effective ways to deliver high quality

requirements quickly. They promote trust, mutual understanding, and strong communications among the project stakeholders and project team, produce deliverables that structure, and guide future analysis.

- Strengths
 - A workshop can be a means to elicit detailed requirements in a relatively short period of time.
 - A workshop provides a means for stakeholders to collaborate, make decisions and gain a mutual understanding of the requirements.
 - Workshop costs are often lower than the cost of performing multiple interviews.
 - A requirements workshop enables the participants to work together to reach consensus which is typically a cheaper and faster approach than doing serial interviews as interviews may yield conflicting requirements and the effort needed to resolve those conflicts across all interviewees can be very costly.
 - Feedback is immediate, if the facilitator's interpretation of requirements is fed back immediately to the stakeholders and confirmed.
- Weaknesses
 - Due to stakeholders availability it may be difficult to schedule the workshop.
 - The success of the workshop is highly dependent on the expertise of the facilitator and knowledge of the participants.
 - Requirements workshops that involve too many participants can slow down the workshop process thus negatively affecting the schedule. Conversely, collecting input from too few participants can lead to overlooking requirements that are important to users, or to specifying requirements that do not represent the needs of the majority of the users.

9. Survey/Questionnaire

- Purpose
 - A means of eliciting information from many people, anonymously, in a relatively short time. A survey can collect information about customers, products, operational practices and attitudes. A survey is often referred to as a questionnaire.
- Strengths
 - When using 'closed-ended' questions, effective in obtaining quantitative data for use in statistical analysis.
 - When using open-ended questions, the survey results may yield insights and opinions not easily obtainable through other elicitation techniques.
 - Does not typically require significant time from the responders.
 - Effective and efficient when stakeholders are not located at one place.
 - May result in large number of responses.

- Quick and relatively inexpensive to administer.
- Weaknesses
 - Use of open-ended questions requires more analysis.
 - To achieve unbiased-results, specialized skills in statistical sampling methods are needed when the decision has been made to survey a sample subset.
 - Some questions may be left unanswered or answered incorrectly due to their ambiguous nature.
 - May require follow up questions or more survey iterations depending on the answers provided.
 - Not well suited for collecting information on actual behaviors.

Addressing Requirements versus Proposing Solutions

When employing efforts to elicit and explain requirements using any of these methods, it is imperative to steadfastly avoid requirements that define potential solutions or otherwise restrict the potential solution space. While it is necessary and useful to understand the current state-of-the-art within a given technology space and knowledge about potential solutions that may already be in development, requirements are meant to simply define problems. Properly drafted requirements allow for a variety of solutions, each with their own advantages and disadvantages, to be considered as potential ways to address a problem. Solution-agnostic requirements prevent limiting and defining the outcome of product realization. Within the context of the Operational Requirements Document Template described in detail below, the solution definition aspect of the Requirements Hierarchy is purposefully not addressed.

This is useful given that an open and honest review of one's needs might show that a preconceived notion about a desired solution may turn out not to be the best solution, or that modifications to existing products or services may be necessary and useful to end users.

Operational Requirements Document Template:

1. General Description of Operational Capability

In this section, summarize the capability gap which the product or system is intended to address, describe the overall mission area, describe the proposed system solution, and provide a summary of any supporting analyses. Additionally, briefly describe the operational and support concepts.

1.1. Capability Gap

Describe the analysis and rationale for acquiring a new product or system, and identify the DHS Component, which contains or represents the end users. Also, name the Capstone IPT, if any, which identified the capability gap.

1.2. Overall Mission Area Description

Define and describe the overall mission area to which the capability gap pertains, including its users and its scope

1.3. Description of the Proposed System

Describe the proposed product or system. Describe how the product or system will provide the capabilities and functional improvements needed to address the capability gap. Do not describe a specific technology or system solution. Instead, describe a conceptual solution for illustrative purposes.

1.4. Supporting Analysis

Describe the analysis that supports the proposed system. If a formal study was performed, identify the study and briefly provide a summary of results.

1.5. Mission the Proposed System Will Accomplish

Define the missions that the proposed system will be tasked to accomplish.

1.6. Operational and Support Concept

1.6.1. Concept of Operations

Briefly describe the concept of operations for the system. How will the system be used, and what is its organizational setting? It is appropriate to include a graphic that depicts the system and its operation. Also, describe the system's interoperability requirements with other systems.

1.6.2. Support Concept

Briefly describe the support concept for the system. How will the system (hardware and software) be maintained? Who will maintain it? How, where, and by whom will spare parts be provisioned? How, where, and by whom will operators be trained?

2. Threat

If the system is intended as a countermeasure to a threat, summarize the threat to be countered and the projected threat environment.

3. Existing System Shortfalls

Describe why existing systems cannot meet current or projected requirements. Describe what new capabilities are needed to address the gap between current capabilities and required capabilities.

4. Capabilities Required

4.1. Operational Performance Parameters

Identify operational performance parameters (capabilities and characteristics) required for the proposed system. Articulate the requirements in output-oriented and measurable terms. Use Threshold/Objective format and provide criteria and rationale for each requirement.

4.2. Key Performance Parameters (KPPs)

The KPPs are those attributes or characteristics of a system that are considered critical or essential. Failure to meet a KPP threshold value could be the basis to reject a system solution.

4.3 System Performance.

4.3.1 Mission Scenarios

Describe mission scenarios in terms of mission profiles, employment tactics, and environmental conditions.

4.3.2 System Performance Parameters

Identify system performance parameters. Identify KPPs by placing an asterisk in front of the parameter description.

4.3.3 Interoperability

Identify all requirements for the system to provide data, information, materiel, and services to and accept the same from other systems, and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

4.3.4 Human Interface Requirements

Discuss broad cognitive, physical, and sensory requirements for the operators, maintainers, or support personnel that contribute to, or constrain, total system performance. Provide broad staffing constraints for operators, maintainers, and support personnel.

4.3.5 Logistics and Readiness

Describe the requirements for the system to be supportable and available for operations. Provide performance parameters for availability, reliability, system maintainability, and software maintainability.

4.3.6 Other System Characteristics

Characteristics that tend to be design, cost, and risk drivers.

5. System Support

Establish support objectives for initial and full operational capability. Discuss interfacing systems, transportation and facilities, and standardization and interoperability. Describe the support approach including configuration management, repair, scheduled maintenance, support operations, software support, and user support (such as training and help desk).

5.1 Maintenance

Identify the types of maintenance to be performed and who will perform the maintenance. Describe methods for upgrades and technology insertions. Also, address post-development software support requirements.

5.2 Supply

Describe the approach to supplying field operators and maintenance technicians with necessary tools, spares, diagnostic equipment, and manuals.

5.3 Support Equipment

Define the standard support equipment to be used by the system. Discuss any need for special test equipment or software development environment

5.4 Training

Describe how the training will ensure that users are certified as capable of operating and using the proposed system.

5.5 Transportation and Facilities

Describe how the system will be transported to the field, identifying any lift constraints. Identify facilities needed for staging and training.

6. Force Structure

Estimate the number of systems or subsystems needed, including spares and training units. Identify organizations and units that will employ the systems being developed and procured, estimating the number of users in each organization or unit.

7. Schedule

To the degree that schedule is a requirement, define target dates for system availability. If a distinction is made between Initial Capability and Full Operational Capability,

clarify the difference between the two in terms of system capability and/or numbers of fielded systems.

8. System Affordability

Identify a threshold/objective target price to the user at full-rate production. If price is a KPP, include it in the section on KPPs above.

Signatures

Sponsor's Acquisition Program Manager [print and sign] Date

Sponsor's Representative [print and sign] Date

S&T Project Manager [print and sign] Date

S&T Division Head [print and sign] Date

Please Note : See Appendix A for a full set of real-world examples ORDs that clearly illustrate how to effectively use this template and other previously described requirements elicitation methods.

DHS Implements a Commercialization Process to Harness Requirements

The U.S. Department of Homeland Security (DHS) possesses an “Acquisition Mindset,” as do so many government agencies. While the Acquisition model has been utilized effectively in developing “custom, one-off” products such as aircraft carriers, it is not particularly germane to a majority of the needs at DHS as well as the first responders (a DHS ancillary market). The timely design, development and deployment of lower priced, widely distributed products for both DHS operating components and the first responder communities represents a critical step in protecting our nation. Recognizing this fact, the Department recently started implementing a “Commercialization Mindset” in order to leverage the vast capabilities and resources of the private sector through an innovative “win-win” private-public partnership called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program.

DHS experienced several challenges merging twenty-two disparate organizations into a cohesive organization with a unified mission and culture. Those familiar with Merger and Acquisition activities realize that while integration of organizations poses difficulties, it also represents opportunities to infuse new processes and values into the newly created organization. Through both “top-down” and “bottom-up” approaches, DHS has been successful in developing, socializing and now implementing an innovative commercialization framework that has started to gain traction throughout the agency. The creation of a “Commercialization Mindset” has caught the attention of DHS managers and employees and has been embraced by senior management because of its significant benefits to the Department’s internal and external activities.

Why is there a need for a Commercialization Mindset in DHS? DHS requirements, in most instances, are characterized by the need for widely distributed COTS (Commercial-Off-The-Shelf) products. Oftentimes, the need is for thousands, if not millions, of products for DHS’ seven operating components and the fragmented, yet substantial first responder and critical infrastructure markets. The DHS commercialization process relies on providing two key pieces of information to potential solution providers in order for them to invest their valuable time, money and resources to develop products and services for use by DHS Operating Components, First Responder communities, Critical Infrastructure and Key Resources (CIKR) owner/operators and other stakeholders: 1) a clear and detailed delineation and explanation of the operational requirements, and 2) a conservative estimate of the potential available market for a potential commercialization partner to offer potential solution(s). We have forged and promulgated the development of Operational Requirements Documents (ORDs) through the publication of several books, training materials and articles to address the first half of this equation, and the following pages of a comprehensive market potential template address the latter.

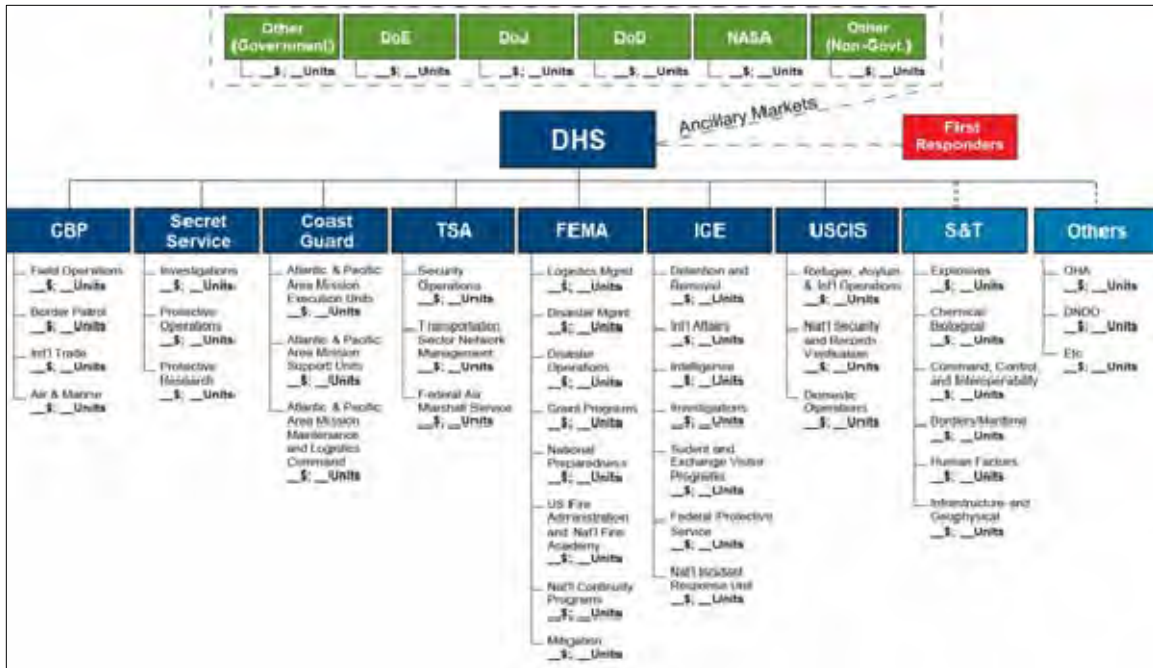


Figure 3 This market potential template maps out many potential available markets to which DHS has direct control and responsibility or acts as a “conduit” For more information on market potential templates, please refer to Appendix I.

Conservative Estimates of Potential Available Markets

It is important to understand not only the detailed operational requirements necessary to provide DHS stakeholders with mission-critical capabilities, but also understand the volume of potential users of these solutions. DHS itself can represent a substantial potential available market; in many instances requiring hundreds, if not thousands of product or service units to address unsatisfied needs. Couple to this the fact that DHS has responsibility for so many ancillary markets (e.g. First Responders, Critical Infrastructure and Key Resources, etc.) representing large potential available markets, it is evident that substantial business opportunities exist for the private sector as these large pools of potential customers and users represent the “lifeblood” for a business (see Figure 3). We first outline top level markets. In turn, each “branch” of the template has been further segmented to hone in on detailed market opportunities.

Figure 4 shows the major differences between a “pure” Acquisition versus “pure” commercialization processes, along with the recently developed and implemented DHS “hybrid” commercialization process.

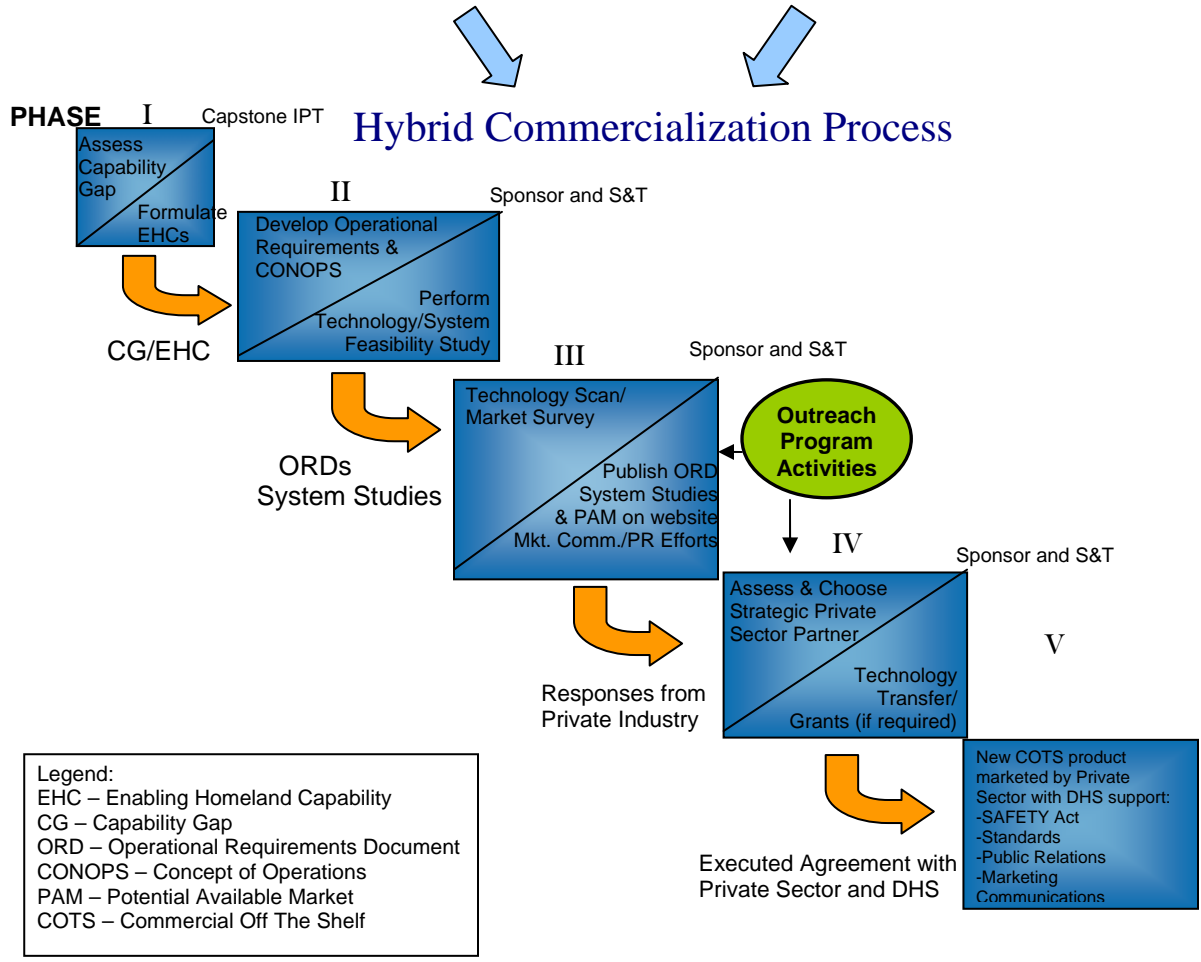
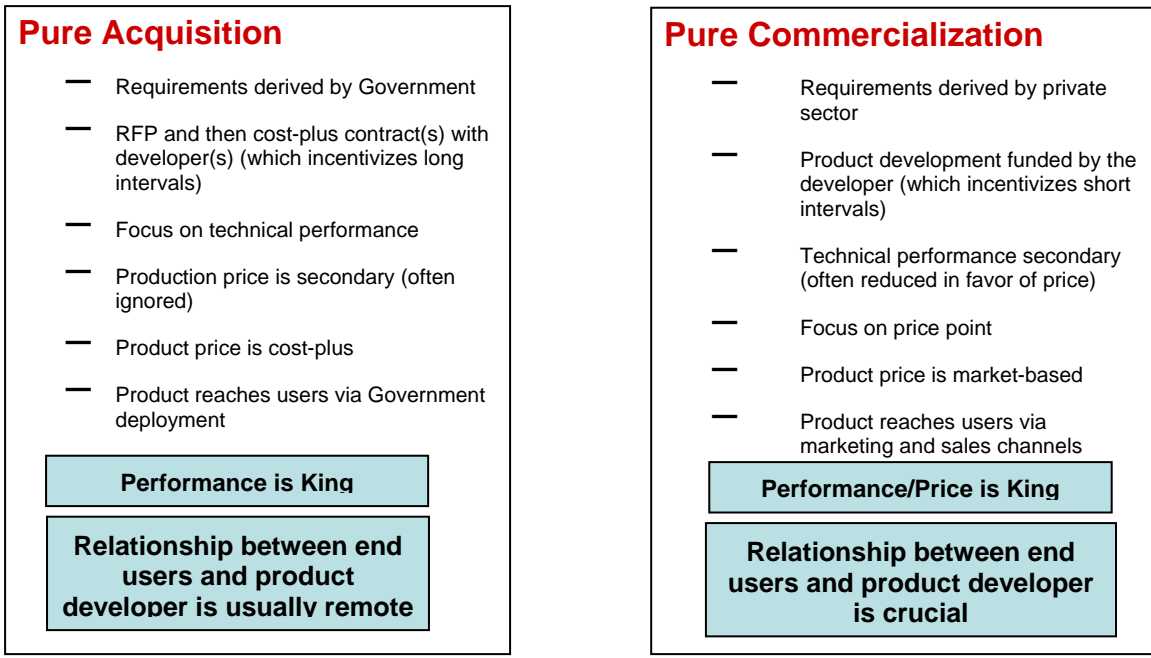


Figure 4 Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system

Figure 5 delineates the overall description of DHS’ new commercialization model and its first private sector outreach program called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program to develop products and services in a private-public “win-win” partnership described in detail at www.dhs.gov/xres/programs/gc_1211996620526.shtm. Briefly, the SECURE Program is based on the simple premise that the private sector is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and resources to such activities, if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. As previously stated, the private sector requires two pieces of critical information from DHS: 1. detailed operational requirement(s), and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in the program.

A New Model for Commercialization...

- Develop Operational Requirements Documents (ORDs)
- Assess addressable market(s)
- Publish ORD and market assessment on public DHS web portal, solicit interest from potential partners in a way that is open to small, medium and large businesses
- Execute no-cost (CRADA-like) agreement with multiple private sector entities and transfer technology and/or IP(if necessary)
- Develop supporting grants and standards as necessary
- Assess T&E findings after product is developed to assure DHS and ancillary markets that product meet its published specifications
- New Commercial-Off-The-Shelf (COTS) product marketed by private sector with DHS support

SECURE Program



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized third-party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal to provide confidence to potential customers at DHS and its ancillary markets that product(s) meet or exceed their published specifications in reference to their actual performance.

Early response from groups within DHS, the private sector, and first responders about this guide and programs like SECURE has been very favorable³⁻⁴. The Department plans to regularly update its website with Operational Requirements Documents (ORDs) to continually expand this innovative private-public partnership. In addition, as evidenced in Figure 6, the taxpayers, private sector and public sector view programs like this as “win-win-win.”

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Figure 6 The SECURE Program is viewed positively by DHS stakeholders. The success of the program lies in the fact that all participants receive significant benefits.

³ See Cellucci, T. “Opportunities for the Private Sector,” 2008, 43pp. [Available online: http://www.dhs.gov/xres/programs/gc_1211996620526.shtm].

⁴ Margetta, R. “S&T Official Working to Move Product Development Out of DHS, Into Private Sector,” Congressional Quarterly Homeland Security. June 27, 2008.

Summary

This document has offered a brief summary of the role of requirements at DHS, with particular emphasis on the requirements hierarchy including defining capability gaps and demonstrating that operational requirements govern the development of an end-user system. Acknowledging the difficulty of requirements development, it presented nine best practices to elicit requirements from an end-user community and eight criteria to judge the “goodness” of requirements. It illustrated how an Operational Requirements Document (ORD) is generated using an ORD template. We also several provided real-world examples. The additional readings listed below are a collection of short articles that provide a number of explanations on the importance of requirements development as well as some additional methods not described in this resource. We encourage you to seek out supplemental information on the topic of requirements development as this book is just one resource among many that can be of value to those developing and understanding requirements in a detailed and thoughtful way. Please take the effort to review the carefully prepared appendixes that follow as they reveal important and practical knowledge in developing operational requirements to enhance our nation’s security in a cost-effective and efficient manner. For your convenience, we have also included Appendix J, which contains the original *Requirements Development Guide* (April 2008) for those interested in a more detailed discussion on requirements development and product development life cycles.

Additional Requirements Development Readings

AntFarm, Inc. “Uncovering Hidden Customer Needs to Grow Your Services Business”. 2007.

http://www.antfarm-inc.com/docs/Growing_Services.pdf.

Byrd, T.A., Cossick, K.L. and Zmud, R.W. A Synthesis of Research of Requirements Analysis and knowledge Acquisition Techniques. *MIS Quarterly*, 16 (1). 117-138.

Coplenish Consulting Group. “New Product Best Practices: Over 100 Ideas for Better NPD”. 2004.

<http://www.coplenish.com/FreeStuffPages/npdbp.pdf>.

David. “Undreamt Requirements.” Weblog entry. David’s Software Development Survival Guide. March 12, 2007.

<http://softwaresurvival.blogspot.com/2007/03/undreamt-requirements.html>.

Davis, Alan. “Just Enough Requirements Management, Part I.” CodeGear. November 10, 2004.

<http://conferences.codegear.com/print/32301>.

- Derby, Esther. Building a Requirements Foundation Through Customer Interviews. Amplifying Your Effectiveness. 2004.
<http://www.ayeconference.com/buildingreqtsfoundation/>.
- Graham, Ian. Requirements Engineering and Rapid Development: An Object Oriented Approach. Addison-Wesley Professional. 1999.
- Japenga, Robert. "How to Write a Software Requirements Specification." Micro Tools, Inc. 2003.
<http://www.microtoolsinc.com/Howsrs.php>.
- Korman, Jonathan. "Putting People Together to Create New Products." Cooper. 2001.
http://www.cooper.com/insights/journal_of_design/articles/putting_people_together_to_cre.html.
- Kotonya, G. and Sommerville, I. Requirements Engineering: Processes and Techniques. John Wiley & Sons, 1998.
- Larson, Elizabeth, and Richard Larson. "Projects without Borders: Gathering Requirements on a Multi-Cultural Project." The Project Manager Homepage. August 3, 2006.
<http://www.allpm.com/print.php?sid=1587>.
- Miller, Hal. "Customer Requirements Specifications." The Usenix Magazine. Vol. 30, No. 2. 2004.
<http://www.usenix.org/publications/login/2005-04/pdfs/miller0504.pdf>.
- Olshavsky, Ryan. "Bridging the Gap with Requirements Definition." Cooper. 2002.
http://www.cooper.com/insights/journal_of_design/articles/bridging_the_gap_with_requirem_1.html.
- Pande, Peter S., Robert Neuman, and Roland Cavanagh. "Defining Customer Requirements: Six Sigma Roadmap Step 2." *The Six Sigma Way: How GE, Motorola, and Other Top Companies are Honing Their Performance*. McGraw-Hill, New York. 2000.
<http://www.sixsig.info/research/chapter13.php>.
- "Requirements analysis." *Wikipedia, The Free Encyclopedia*. Wikimedia Foundation, Inc. April 8, 2008.
http://en.wikipedia.org/w/index.php?title=Requirements_analysis&oldid=204196812.
- Sehlhorst, Scott. "Elicitation Techniques for Processes, Rules, and Requirements." Weblog entry. Tyner Blain. September 13, 2007.
<http://tynerblain.com/blog/2007/09/13/elicitation-techniques-2/>.

Sehlhorst, Scott. "Ten Requirements Gathering Techniques." Weblog entry. Tyner Blain. November 21, 2006.

<http://tynerblain.com/blog/2006/11/21/ten-requirements-gathering-techniques/>.

Silverman, Lori L., "Customers or Consumers? Focus or Obsession?" Partners for Progress. 2000.

<http://www.partnersforprogress.com/Articles/Customers%20or%20Consumers.pdf>.

Sisson, Derek. "Requirements and Specifications". Philosophe.com. January 9, 2000.

<http://www.philosophe.com/design/requirements.html>.

U.S. Department of Defense. Defense Acquisition Guidebook, Chapter 4. Dec. 2004.
https://akss.dau.mil/DAG/TOC_GuideBook.asp?sNode=R&Exp=Y.

Ward, James. "It Is Still the Requirements: Getting Software Requirements Right." Sticky Minds. June 7, 2005.

http://www.stickyminds.com/s.asp?F=S9150_ART_2.

Wieggers, Karl E., and Sandra McKinsey. "Accelerate Development by Getting Requirements Right." 2007.

<http://www.serena.com/docs/repository/products/dimensions/accelerate-developme.pdf>.

Wilson, William. "Writing Effective Requirements Specifications." NASA Software Assurance Technology Center. April 1997.

http://satc.gsfc.nasa.gov/support/STC_APR97/write/writert.html.

Winant, Becky. "Requirement #1: Ask Honest Questions." Sticky Minds. April 3, 2002.

http://www.stickyminds.com/s.asp?F=S3264_COL_2.

Appendix A: ORD Examples

Learn by Doing:

**Developing a detailed Operational Requirements Document
(ORD)**

**Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security
November 2008**

Requirements Development Initiative – Operational Requirements Document (ORD) Examples

This compilation of ORDs is meant to present the reader with several real-world examples of detailed operational requirements drafted by implementing an easy-to-use ORD template that provides a basic framework in guiding the understanding and articulation of needs.

Please keep in mind the following points as you consider writing an ORD to describe and define an existing problem:

1. Writing an ORD is **not** as difficult as you think → so just “jump in” and give it a try
2. We’re here to help! Please use the many resources available online at http://www.dhs.gov/xres/programs/gc_1211996620526.shtm and <https://dhsonline.dhs.gov/portal/jhtml/community.jhtml?index=15&community=S%26T&id=2041380003> for guidance:
 - ORD templates
 - Example ORDs
 - “Developing Operational Requirements” (Version 2)
3. Some simple things to remember:
 - **Requirements** define problems while **specifications** define solutions
 - An ORD describes a problem, not a solution
 - Make sure your ORD is product/service/solution agnostic (that is, it does **not** presuppose a certain solution)
 - Make the solution space as wide as possible
 - Keep it simple and make it easy for a reader to understand your problem/requirement
4. Review the attached ORD template examples and contact us if you have any questions or comments!
 - SandT_Commercialization@dhs.gov

ORD Template and Examples

Operational Requirements Document Template36

National Emergency Response Interoperability Framework and Resilient Communication System of Systems (Example ORD).....42

Persistent Intelligence, Surveillance and Reconnaissance Family of Systems Services (Example ORD).....77

Interoperable Communications Switch (Example ORD).....103

**OPERATIONAL REQUIREMENTS DOCUMENT
TEMPLATE**

[Name of System or Product]

**to be developed by the
[Name of Acquisition Program]**

**[Name of Program Manager]
Program Manager, [Name of Acquisition Program]
[Name of PM's Organization]**

**[Name of Sponsor]
Sponsor, [Name of Acquisition Program]
[Name of Sponsor's Organization]**

**[Name of S&T Project Manager]
Project Manager, [Name of S&T Project]
[Name of S&T Division]
Science and Technology Directorate**

**Date
Version X.X**

Template Only

Contents

1. GENERAL DESCRIPTION OF OPERATIONAL CAPABILITY38

1.1 Capability Gap 38

1.2 Overall Mission Area Description 38

1.3 Description of the Proposed Product or System..... 38

1.4 Supporting Analysis..... 38

1.5 Mission the Proposed System Will Accomplish 38

1.6 Operational and Support Concept 38

 1.6.1 Concept of Operations.....38

 1.6.2 Support Concept.....38

2 THREAT.....38

3 EXISTING SYSTEM SHORTFALLS39

4 CAPABILITIES REQUIRED39

4.1 Operational Performance Parameters 39

4.2 Key Performance Parameters (KPPs)..... 39

4.3 System Performance..... 39

 4.3.1 Mission Scenarios.....39

 4.3.2 System Performance Parameters.....39

 4.3.3 Interoperability39

 4.3.4 Human Interface Requirements.....39

 4.3.5 Logistics and Readiness.....39

 4.3.6 Other System Characteristics39

5 SYSTEM SUPPORT40

5.1 Maintenance..... 40

5.2 Supply 40

5.3 Support Equipment 40

5.4 Training 40

5.5 Transportation and Facilities 40

6 FORCE STRUCTURE40

7 SCHEDULE40

8 SYSTEM AFFORDABILITY40

9 SIGNATURES.....41

10 APPENDIXES.....41

11 GLOSSARY41

1. General Description of Operational Capability

In this section, summarize the capability gap which the product or system⁴ is intended to address, describe the overall mission area, describe the proposed system solution, and provide a summary of any supporting analyses. Additionally, briefly describe the operational and support concepts.

1.1 Capability Gap

Describe the analysis and rationale for acquiring a new product or system, and identify the DHS Component which contains or represents the end users. Also name the Capstone IPT, if any, which identified the capability gap.

1.2 Overall Mission Area Description

Define and describe the overall mission area to which the capability gap pertains, including its users and its scope

1.3 Description of the Proposed Product or System

Describe the proposed product or system. Describe how the product or system will provide the capabilities and functional improvements needed to address the capability gap. Do not describe a specific technology or system solution. Instead, describe a conceptual solution for illustrative purposes.

1.4 Supporting Analysis

Describe the analysis that supports the proposed system. If a formal study was performed, identify the study and briefly provide a summary of results.

1.5 Mission the Proposed System Will Accomplish

Define the missions that the proposed system will be tasked to accomplish.

1.6 Operational and Support Concept

1.6.1 Concept of Operations

Briefly describe the concept of operations for the system. How will the system be used, and what is its organizational setting? It's appropriate to include a graphic which depicts the system and its operation. Also describe the system's interoperability requirements with other systems.

1.6.2 Support Concept

Briefly describe the support concept for the system. How will the system (hardware and software) be maintained? Who will maintain it? How, where, and by whom will spare parts be provisioned? How, where, and by whom will operators be trained?

2 Threat

If the system is intended as a countermeasure to a threat, summarize the threat to be countered and the projected threat environment.

⁴ In this document, the terms "product" and "system" are synonymous. The word "system" is used to refer to either.

3 Existing System Shortfalls

Describe why existing systems cannot meet current or projected requirements. Describe what new capabilities are needed to address the gap between current capabilities and required capabilities.

4 Capabilities Required

4.1 Operational Performance Parameters

Identify operational performance parameters (capabilities and characteristics) required for the proposed system. Articulate the requirements in output-oriented and measurable terms. Use Threshold/Objective⁵ format and provide criteria and rationale for each requirement.

4.2 Key Performance Parameters (KPPs)

The KPPs are those attributes or characteristics of a system which are considered critical or essential. Failure to meet a KPP threshold value could be the basis to reject a system solution.

4.3 System Performance.

4.3.1 Mission Scenarios

Describe mission scenarios in terms of mission profiles, employment tactics, and environmental conditions.

4.3.2 System Performance Parameters

Identify system performance parameters. Identify KPPs by placing an asterisk in front of the parameter description.

4.3.3 Interoperability

Identify all requirements for the system to provide data, information, materiel, and services to and accept the same from other systems, and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

4.3.4 Human Interface Requirements

Discuss broad cognitive, physical, and sensory requirements for the operators, maintainers, or support personnel that contribute to, or constrain, total system performance. Provide broad staffing constraints for operators, maintainers, and support personnel.

4.3.5 Logistics and Readiness

Describe the requirements for the system to be supportable and available for operations. Provide performance parameters for availability, reliability, system maintainability, and software maintainability.

4.3.6 Other System Characteristics

Characteristics that tend to be design, cost, and risk drivers.

⁵ The threshold value for a requirement is the minimum acceptable performance. The objective value is the desired performance.

5 System Support

Establish support objectives for initial and full operational capability. Discuss interfacing systems, transportation and facilities, and standardization and interoperability. Describe the support approach including configuration management, repair, scheduled maintenance, support operations, software support, and user support (such as training and help desk).

5.1 Maintenance

Identify the types of maintenance to be performed and who will perform the maintenance. Describe methods for upgrades and technology insertions. Also address post-development software support requirements.

5.2 Supply

Describe the approach to supplying field operators and maintenance technicians with necessary tools, spares, diagnostic equipment, and manuals.

5.3 Support Equipment

Define the standard support equipment to be used by the system. Discuss any need for special test equipment or software development environment

5.4 Training

Describe how the training will ensure that users are certified as capable of operating and using the proposed system.

5.5 Transportation and Facilities

Describe how the system will be transported to the field, identifying any lift constraints. Identify facilities needed for staging and training.

6 Force Structure

Estimate the number of systems or subsystems needed, including spares and training units. Identify organizations and units that will employ the systems being developed and procured, estimating the number of users in each organization or unit.

7 Schedule

To the degree that schedule is a requirement, define target dates for system availability. If a distinction is made between Initial Capability and Full Operational Capability, clarify the difference between the two in terms of system capability and/or numbers of fielded systems.

8 System Affordability

Identify a threshold/objective target price to the user at full-rate production. If price is a KPP, include it in the section on KPPs above.

9 Signatures

Sponsor's Acquisition Program Manager [print and sign] Date

Sponsor's Representative [print and sign] Date

S&T Project Manager [print and sign] Date

S&T Division Head [print and sign] Date

10 Appendixes

11 Glossary

Example Only

OPERATIONAL REQUIREMENTS DOCUMENT

National Emergency Response Interoperability Framework and Resilient Communication System of Systems

Example Only
Contents

1. GENERAL DESCRIPTION OF OPERATIONAL CAPABILITY.....	44
1.1. Capability Gap	44
1.2. Overall Mission Area Description	46
1.3. The Description of Resilient Portable Communications Responder Kits	46
1.4. Supporting Analysis.....	49
1.5. Mission the Proposed System Will Accomplish	50
1.6. Operational and Support Concept	51
1.6.1. Concept of Operations	51
1.6.2. Support Concept	52
2. THREAT.....	52
3. EXISTING SYSTEM SHORTFALLS	54
4. CAPABILITIES REQUIRED	56
4.1. Operational Performance Parameters	56
4.2. Key Performance Parameters (KPPs).....	58
4.3 System Performance.....	60
4.3.1 Mission Scenarios	61
4.3.2 System Performance Parameters	64
4.3.3 Interoperability	65
4.3.4 Human Interface Requirements	70
4.3.5 Logistics and Readiness	70
4.3.6 Other System Characteristics.....	71
5. SYSTEM SUPPORT	71
5.1 Maintenance.....	71
5.2 Supply	71
5.3 Support Equipment	72
5.4 Training	72
5.5 Transportation and Facilities	72
6. FORCE STRUCTURE	72
7. SCHEDULE.....	73
8. SYSTEM AFFORDABILITY.....	73
9. SIGNATURES.....	74
10. APPENDIXES	75
11. GLOSSARY	75

1 General Description of Operational Capability for a National Emergency Response Interoperability Framework and Resilient Communication System of Systems

1.1 Capability Gap

Interoperability and compatibility of First Responder communication systems is a mandate of the National Incident Management System (NIMS). However, as of 2008, the only interoperability systems widely in use are expensive and complicated proprietary voice-over-radio systems. These aptly described “patchwork” interoperability systems are unable to scale without additional, costly equipment coupled with costly on-site support provided by highly trained technicians. This current mode of operations is not feasible in the critical first minutes and hours of an incident response.

The vast majority of Emergency Responders are limited in their ability to communicate and collaborate with each other. They are unable to communicate with command, support teams and other responding organizations present at an incident scene. In 2008, almost 7 years after the tragic lessons learned by 9/11, the overwhelming majority of Emergency Response Organizations (ERO) does not have the basic capability for any of their team members to establish communications at an incident site. They have to wait hours for large trucks and/or trailers with very expensive¹ and complicated communications equipment delivered to the site. In the case of a catastrophic incident causing a scorched earth² environment, it may take days to get the necessary equipment and communication support personnel to the incident site.

It is not only the complexity and cost of existing systems that inhibit NIMS compliance; most systems often render previous technology investments obsolete or require a need for costly upgrades to legacy systems proving impractical or unaffordable. A system is required that creates a communications framework enabling the ability to allow not only interoperability of disparate systems, but also the ability to interconnect legacy systems and new systems.

Another major capability gap is in providing an affordable solution for the interoperability and interconnection of communication systems that support IPv4 routing with those systems that answer the Department of Defense mandate for IPv6 compliance. The cost of phasing out an IPv4 system (which is prevalent in the vast majority of state and local ERO’s, Non-Government Organizations and private sector security) is beyond realistic budgetary feasibility and would take years to accomplish.

Yet, closing this gap is mandatory. The NIMS mandate for interoperability is unattainable without a cost-effective, easy-to-implement system that provides a framework for the interoperability of data and video between responders and EROs. Data is as critical as voice communications within an incident site. If noise levels inhibit voice communications or silent communications are necessary, instant messaging is an effective tool. Video from an inexpensive webcam on a responder’s laptop may make a critical difference by providing a visual assessment to the ERO. Maps and other files needed at the incident site must get to the response team without the need to deliver files physically via courier, currently the most widely-used solution⁵.

Example Only

Existing interoperable voice, data and video communications require fixed private networks or access to the Internet via a Virtual Private Network (VPN) requiring authentication servers and server-based network management systems. This requirement for access to remote servers creates an insurmountable capability gap for interoperable communications among responders in the hours or days they must wait for communications trucks and/or trailers to arrive at the incident scene. This ORD requires a system that provides peer-to-peer interoperability between responders and EROs without the requirement for remote servers or dedicated networks. The requirement is for secure peer-to-peer communication between any responder using any type of voice, video or data communication device and any other responder or ERO without requiring the receiving communication to be of similar device type or dedicated network. Responders at an incident site must be able to establish incident area peer-to-peer communications within minutes of responding and interoperate with EROs both at the incident site and/or remotely across readily available disparate communications networks without the need for third-party services or servers.

Even more problematic is the fact that most EROs still depend on vulnerable radio or cellular infrastructure to support expensive communication and command vehicles. Network failures caused by destruction of critical infrastructure, such as radio towers, landlines and network control centers, represent a major challenge for the public and private sectors. If they do have systems, the majority is not portable enough for easy transport to the incident scene by a first responder; or is so complicated, extensive training is required to operate the system. Very few EROs currently have portable systems whose capabilities allow a responder to establish interoperable voice, data and video communications at the incident site without technical support in ten to twenty minutes. All EROs require this capability.

Dramatically illustrated in the aftermath of the 2004-2005 hurricane season, which resulted in catastrophic damage across the Gulf States, is the ultimate example of the capability at hand. Vast areas realized devastating damage to their communications infrastructure. There was no communications resiliency. The available response recovery solutions were inadequate or failed altogether, leaving many areas where lives were at risk without communications for days.

Many critical infrastructure facilities of importance to the security of the region did not have effective communications for weeks.³ Belle Chase Naval Air Station, critical for the staging of over 30,000-rescue operations south of New Orleans, did not have reliable voice communications for nearly 96 hours after the landfall of Hurricane Katrina. With a system that meets the requirements of this ORD, the Coast Guard Rescue Operations in New Orleans would have had telephone capability and data communications within 10 to 20 minutes of beginning the emergency response. This communication could have been established by anyone at the staging area regardless of whether they had training in deploying communication networks or not.

Almost all communication systems in 2008 still require some type of fixed infrastructure in order to work and the presence of qualified technicians or engineers is required. Yet many disaster situations result in no useable infrastructure to support either local area or wide area communications.

According to an **Associated Press report in 2005**, “Downed telephone lines and damaged cellular towers left emergency crews confused and isolated in the aftermath of Hurricane

Example Only

Katrina.” The report, quoting experts, said communications systems eroded as the waters rose and only got worse.

“We had no way to communicate except by line of sight. Our radios were not operable, most landlines and cell phones were useless and our communications centers were under water. When help arrived, we could not communicate with them either.” **Juliette Saussy, director of Emergency Medical Service of New Orleans, told regulators.**

“Some three million telephone lines were knocked out as the violent storm hit the Gulf Coast on August 29, 2005. At least 38 911-call centers went down, and more than 1,000 cellular towers were out of service. As many as 20,000 calls failed to go through the day after the storm, and about 100 TV and radio stations were knocked off the air...” **FCC Chairman, Kevin Martin said.**

There must be a framework for enabling communications, interoperability and collaboration that is affordable. The biggest gap in 2008 is that existing solutions are too expensive for most EROs and funding for staffing communication technicians to operate these solutions reduces the ability of most EROs to equip and staff for other vital capabilities necessary for mission effectiveness. Billions of dollars in grants are provided for solutions that will not meet the NIMS requirements. This ORD requires, not only that the technology work, but that it is affordable.

The local incidents as well as the wide area natural disasters within the past seven years clearly identify the capability gap to enable First Responders to communicate, interoperate and collaborate with each other, their command, and their support teams or with other organizations present at an incident scene within minutes of arriving at an incident site. This ORD provides the system requirements to close this vital gap in the NIMS, saving lives and increasing security.

1.2 Overall Mission Area Description

First Emergency Response Providers (FERP) by definition are the professionals who first arrive at an incident site to provide emergency medical services, security, law enforcement, assessment of the scope of the incident and recommend and coordinate an extended response if required. The mission area covered by this ORD is to outline the capabilities needed to enable FERPs to communicate and collaborate with each other, their command and interoperate with mutual aid, support teams and other responding organizations within minutes of arriving at an incident site. This ORD will also address the capabilities needed to provide interoperable voice and data systems to command in control of the incident; dynamically managing the incident as the response grows and scaling communications as required; increasing collaboration and extending the chain of command across jurisdictions. Finally, this ORD will identify the requirements of the proposed system capabilities and provide a communications framework for the creation of a dynamic, interoperable system of systems.

1.3 The Description of Resilient Portable Communications Responder Kits that Create a System of Systems.

The primary system solution that closes the capability gap and accomplishes the mission of this ORD is actually a system of systems (SoS). The SoS must meet three primary requirements. First, the SoS must be dynamic, enabling interoperability between any combinations of different communication device types; converge any type or number of disparate networks on-demand at any incident site. The SoS also fosters dynamic communications with EROs, elected officials whose

Example Only

districts are affected by the incident, supporting emergency operations centers (EOC), medical facilities, NGOs, military bases and private sector security involved in the area of the event. There cannot be any operational restrictions on the number of or combination of systems available to support the incident response. The requirement is the EROs and FERPs use the same software-based framework that is freely distributable at the incident site and can be loaded on or accessed by any device in minutes.

In order to create a dynamically interoperable SoS, the SoS must be based on software that converges network protocol types and provides network presence awareness. The SoS is required to enable data interoperability among any combinations of ad hoc, terrestrial data, telephony or satellite networks that are immediately available to the FERP or will be introduced to the SoS by other FERPs or EROs as the response develops.

The second primary requirement that must be in place to meet the mission of this ORD is human portable resilient communication systems that can provide connectivity to the interoperability framework. These systems will be in a kit form that has everything a FERP needs, to be hand-carried to the incident site, transported by car, helicopter or small watercraft. The kit must be able to provide voice, video and data communication peer-to-peer among FERPs at the incident site as well as capability across any available network. If normal network infrastructure is unavailable, the kit will contain a broadband satellite system to insure connectivity beyond the incident site. The Resilient Portable Communications Kit (RPCK) will be easy to setup and in operation in 10 to 20 minutes by any FERP. The kit will require zero technical support to setup. The RPCK must seamlessly participate in an expanding system of systems. The kit will be available in multiple form factors providing EROs the flexibility to have kits carried by hand in cases, mounted in vehicles, installed in mobile EOCs or any other type of response apparatus. If an ERO needs to support large-scale recovery operations, the RPCK will be modifiable to meet the requirement of the ERO.

The communication capabilities of the RPCK require:

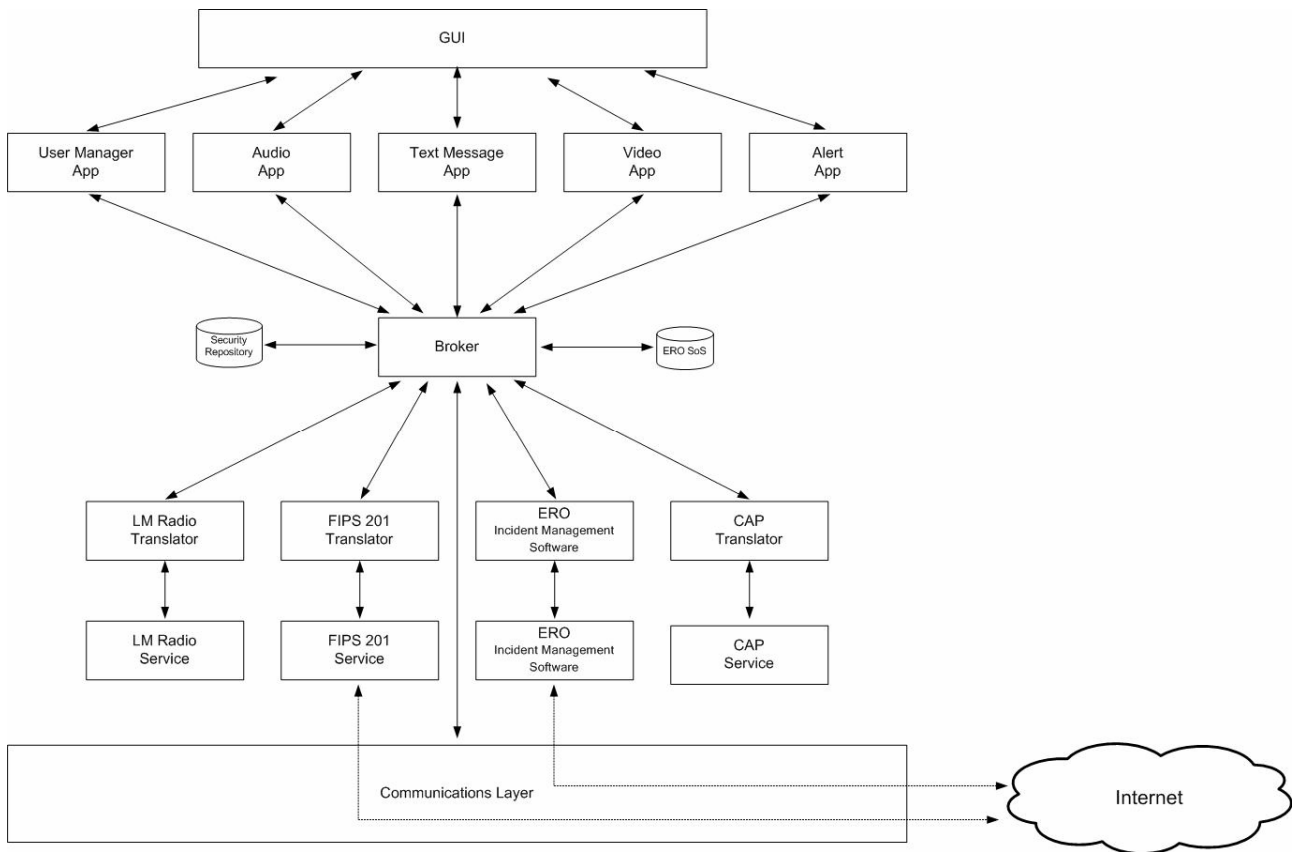
- the ability to operate via both AC and DC power without requiring filtering. It will directly connect with any 12-volt battery, vehicle cigarette lighter adaptor, generator, tactical solar array or tactical fuel cell.
- a full featured VoIP PBX with at least 5 handsets (wired or wireless) with the ability to scale the support of VoIP handsets for every FERP at the incident site.
- wired Ethernet connectivity for a minimum of 4 external devices.
- wireless access to the network for any 802.11-enabled COTS computer at the incident site. The system's wireless coverage will be scalable simply by deploying software definable wireless routers operating on AC or DC power deployable by the FERP.
- network management software converging data, telephony and video protocols while interconnecting seamlessly and without configuration with IPv4 and/or IPv6 networks and devices.
- IPv6 and IPv4 network routing with a software firewall as well as allowing external firewalls and VPNs to be used if required.
- simple operating instructions with color-coded connections allowing any FERP to deploy the network without prior exposure or training to the RPCK.
- the capability to add IP-based devices and peripherals as needed to support an extended response or recovery operation.

Example Only

- the ability to interconnect with any Land Mobile Radio Network (LMR) or cellular “push to talk” (CPT) phone patchwork interoperability system, enabling LMR or CPT devices to interoperate with any other type of device on the SoS, such as a laptop computer. This ability allows EROs utilizing IP-based devices (laptop, PDA, desktop computer) to have voice communications with LMR or CPT devices
- interoperability support with cellular systems.

The third primary requirement is the kit must be affordable and scalable. The SoS fails if the FERP does not carry resilient communications to the incident. EROs will need multiple Rocks. If the kits are too expensive they will not be available where they are needed most as an integral part of any FERP’s support equipment. The RPKC should be affordable for DHS to rapidly fund the distribution of enough kits across the United States, enabling the deployment of a resilient SoS, which in turn creates a National Communication Resiliency Network (NCRN). Even if parts, or all, of the national power and communications infrastructure are compromised or destroyed, the NCRN would survive.

The following diagram details the architecture needed to create the framework of a SoS:



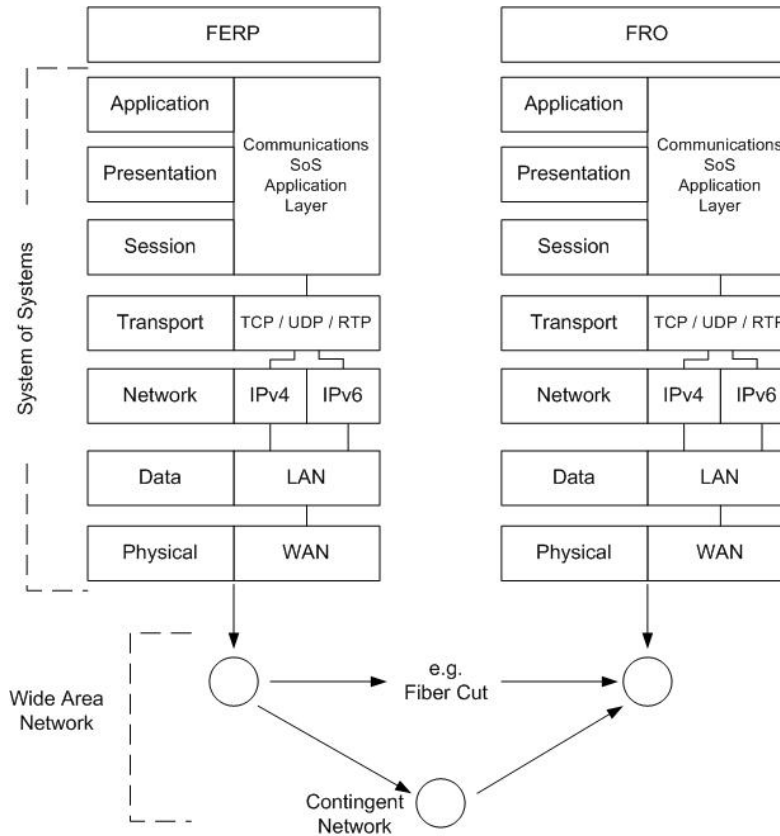
The kits are required to interconnect with any available IPv4 or IPv6 data network that the FERP has permission to use; providing Wide Area Network (WAN) connectivity without requiring any configuration or modifications by the FERP. By enabling the IPv6 capability, the system provides the ERO the ability to create secure collaboration with supporting agencies anywhere in the world,

Example Only

on-demand. The following diagram details the capability of creating secure peer-to-peer collaboration on-demand without the need of a server.

1.4 Supporting Analysis

The following diagram is the position of components on the OSI stack necessary to support interoperability.



The contingent network in the diagram above is any available WAN connection. If a WAN connection is not available at the incident site, the RPCK will include a small broadband satellite system, with active service.

Example Only

1.5 Mission the Proposed System Will Accomplish

February 28, 2003, President George W. Bush issued Homeland Security Presidential Directive 5 (HSPD-5) which in mandating the National Incident Management System (NIMS) calls for the creation of a system that enables,

“Federal, State and Local governments to work effectively and efficiently together to prepare for, respond to and recover from domestic incidents, regardless of cause, size or complexity. To provide for interoperability and compatibility among Federal, State and Local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system, multiagency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications; and certification; and the collection, tracking and reporting of information and incident resources.”

The proposed SoS and RPKC would enable the accomplishment of this directive. If FERPs and EROs cannot communicate, they fail. The proposed system creates the communication resiliency necessary for an 'interoperable and compatible response' to an incident.

Specifically the proposed system will accomplish this mission by:

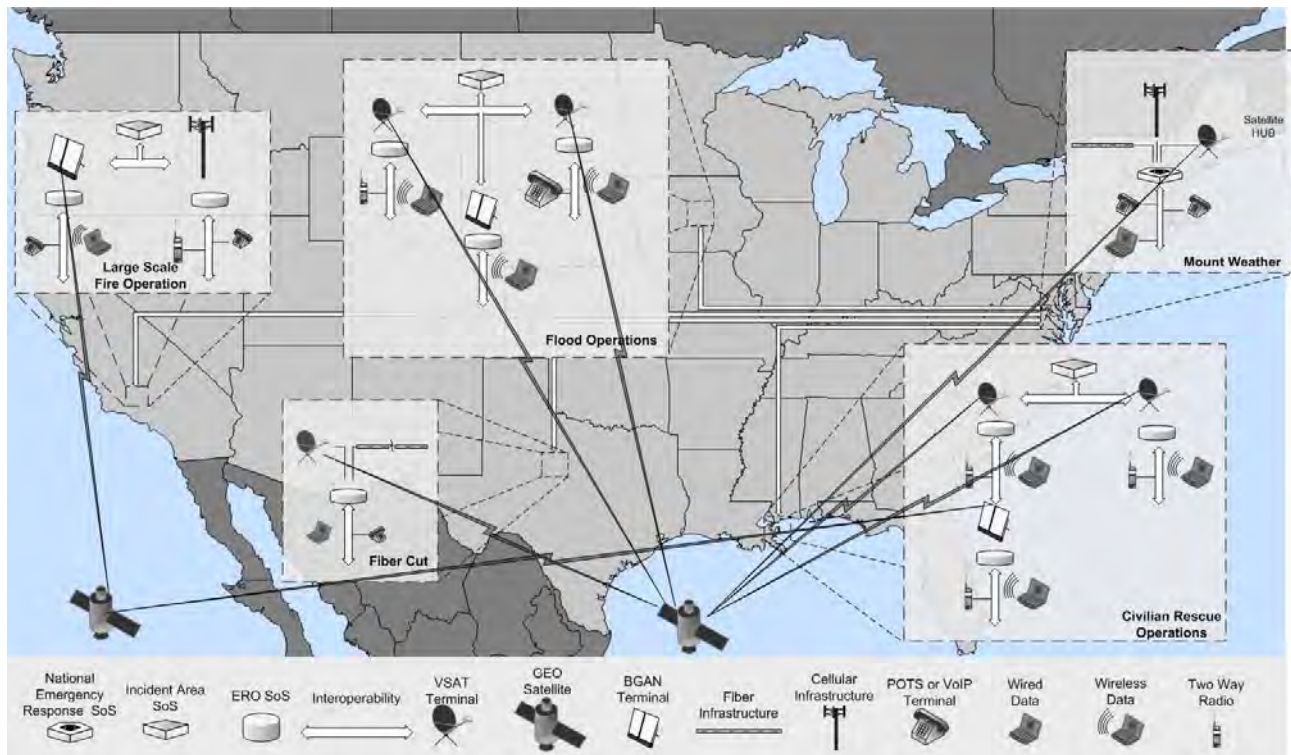
- providing a communication framework that creates dynamically interoperable communications on-demand.
- providing any FERP the capability to communicate at an incident site with other responders and with anyone else who has data or telephony capability anywhere in the country with what the FERP brings to the incident site, there is no need for additional equipment.
- enabling any responder, even if it is the first time the FERP has used the kit, to set up the system in 10 to 20 minutes.
- interoperating with other systems, creating a system of systems for voice, data and video interoperability.
- providing the ability to log communications among FERPs for reporting purposes.
- interconnecting command systems in a multi-agency response across disparate networks on-demand.
- creating visibility among responders to know what resources are available and coordinate the use of those resources.
- enabling the creation of 'ad hoc' incident site, area, regional and national communication networks as needed within minutes.
- providing peer-to-peer communications that enable instant alerts, warnings and advisories that can be viewed and responded from anywhere in the country.

Example Only

1.6 Operational and Support Concept

1.6.1 Concept of Operations

The RPCK and a SoS framework can establish communications anywhere and anytime without any other support. These systems will be a part of the FERP team's basic response tools. The system creates a system of systems with other systems and will interoperate with any other IP-based network. If FERP vehicles in every locality in the country carried the RPCK /SoS system or used the software that provides the system capabilities for legacy systems, in effect, the NCRN is created that provides communication capability even in the aftermath of a large scale infrastructure disaster. The diagram below illustrates the NCRN.



The NCRN will be available to as many FERPs and EROs as possible on a 24x7 basis. The system creates the communication resiliency and provides the capabilities to accomplish the mission only if the SoS is available to the FERP teams and their commanders. Every EOC, fire station, police station, hospital emergency room, private security force at critical infrastructure sites should have a RPCK in order to create a system of systems on-demand. In addition, key response vehicles, apparatus and command vehicles will also have systems in order to be apart of the system of systems. Finally, civilian and political leaders who are integral to the NIMS should also travel with the RPCK to guarantee their availability to collaborate by having personal communication resiliency.

Sites and agencies not affected by the loss of communication capabilities, but who still need to be a part of the SoS can simply do so by running the proposed system software on their existing systems. This ability to run SoS software on any network from any location will provide the capability of a virtual on-demand NCRN, resilient by design. The SoS communication framework is agnostic of

Example Only

device type or network type. The SoS system framework simply requires a MAC or IP address within an IPv4 or IPv6 network.

Billions of dollars has been spent on interoperability since the NIMS mandate, but today there is no capability for interoperability of voice, video and data that can be used on a local, state, regional and national basis immediately following an incident. The proposed RPCK/SoS will provide that capability for far less than the cost of alternative systems that do not have the capability of meeting the mandate. Implementation of a program that would use the system is called for. Meeting this requirement saves hundreds of millions of taxpayer dollars while also being rolled out nationally within three short years.

1.6.2 Support Concept

The very nature of the SoS means providing connectivity when and where it is needed. A staff of network convergence engineers would support the system around the clock. The support engineer must have the ability to troubleshoot problems in real-time. The support engineer would have the ability to run remote diagnostics on any supported system. Because one of the major requirements of the ORD is hardware components be minimized when possible by providing network functionality with software. The majority of support issues would more than likely be related to the convergence software running the RPCK or the framework software running the SoS.

Software updates will be pushed to all systems in a planned and coordinated manner. Because the SoS is a peer-to-peer framework, updates will automatically be logged to the support database with an acknowledgement of a successful update. If updates are required at the incident site, the support engineer would have the ability to remotely update the RPCK at the incident.

If there are hardware failures with the RPCK, replacement systems and parts will be staged at regional logistic depots, which would guarantee a maximum delivery time of 8 hours to the ERO. Spare parts should be included with each RPCK for repairs that can be made by the FERP.

Live interactive webinars will be held daily on a regional basis allowing any FERP to not only receive training, but also ask for advice and share ideas with other FERPs. These webinars will be coordinated and monitored by a national support staff. Because every RPCK would provide peer-to-peer video capability, enhanced support would be provided to any FERP when needed.

2 Threat

If FERPs and EROs cannot communicate, they cannot respond effectively. Lives have been lost because communications systems were not resilient or could not interoperate with other systems at the incident. Rescue operations cannot be coordinated; assets requested or deployed all while valuable time is lost without critical communications capability.

On a local level incident response, too many missions are compromised because under-funded EROs cannot afford easy-to-use resilient communication systems. The systems sold to them are too expensive and require costly support. Complex systems requiring this type of support take resources away from other critical roles.

In most cases, as communications systems funding becomes available, EROs do not possess the knowledge or experience to adequately obtain a system that addresses all the communication risks

Example Only

they will face in a disaster. There are no standards published that give them guidance on possible solutions that will meet the demands necessary to implement this ORD. Instead, they rely on existing relationships with vendors or salespeople, who themselves are not skilled or adept in disaster recovery communications. These resources work for very large companies whose business model relies on proprietary technology that does not allow other manufacturers' products to integrate. Often times EROs find that what they get is not what they thought they were buying. There are dozens of anecdotal stories of EROs spending millions to deploy systems that do not accomplish the intended mission and when they complain they are informed they will need to spend millions more to actually get the system to do what they need, if indeed the system can do what they need.

On a state and regional level where interoperability exists, only certain types of radio systems have this ability. These systems depend on an infrastructure with no resiliency. Major budget dollars spent on incident management software and services by EROs to manage incidents on a regional or state basis will not work if they do not have connectivity to the Internet. Alert and warning systems have become a major business since the Virginia Tech tragedy, but they all depend on networks that provide no resiliency. If power fails, campus communications fail. You cannot send a SMS alert and have any guarantee the message was received if you are depending on a highly vulnerable cellular network. If you send an emergency email, there is no way to guarantee that the multiple e-mail servers required for the delivery of the email will be available and able to deliver the increased amounts of email generated due to an event. Not only are EROs creating plans that will fail without resilient and an interoperable communication framework, they are spending hundreds of millions of dollars building a false sense of readiness.

There currently is no interoperable resilient national communication solution across federal, state and local EROs. Solutions that will take decades, costing billions of dollars and do not provide resilient interoperability are a major threat to homeland security. Big budget telecommunications projects follow the failed philosophy of "you throw enough money at a problem it will be fixed", thus leading EROs to ignore the existing vulnerabilities that could be addressed by less costly and more practical solutions. Too many telecommunications professionals are still pushing 20th century technologies to address 21st century problems. A response to a pandemic, major terrorist strike at key infrastructure, cyber attack on telecommunication centers, super regional earthquakes and catastrophic oil shortages planned to cripple the US economy or any other scenario with national impact will fail because current communications infrastructure will be compromised or worse yet, destroyed. Without communications, EROs are blind, deaf and mute to any coordinated national response. There is no capability to create a national "ad hoc" communications network for a coordinated national response. This inability leaves NIMS vulnerable to failing on a catastrophic level.

Finally, the greatest threat is ignoring the plurality of our system of government. Incident response always starts at the local level; expenditures must happen at the local level. It is impractical to implement a federally mandated one-size-fits-all system. William Waugh of Georgia State University in Atlanta points out in his paper "*Terrorism, Homeland Security and the National Emergency Management Network*"

"On September 11, 2001, officials and agencies that are part of the national emergency management system orchestrated the responses to the collapse of the World Trade Center towers and the fires at the Pentagon. The efforts of local, state, and federal emergency

Example Only

agencies were augmented by nonprofit organizations, private firms, and organized and unorganized volunteers. The system reacted much as it would have for a major earthquake or similar disaster. In the rush to create federal and state offices to deal with the threat of terrorism and, ultimately, to create a Department of Homeland Security, the very foundation of the nation's capacity to deal with large-scale disasters has been largely ignored. Although the human and material resources that the emergency management network provides may again be critical in a terrorist-spawned catastrophe, the new Homeland Security system may not be capable of utilizing those resources effectively. The values of transparency, cooperation, and collaboration that have come to characterize emergency management over the past decade seem to be supplanted in the new command-and-control-oriented Homeland Security system. If that occurs, when the resources of the national emergency management system are needed most, the capacity to utilize the system may be severely damaged and cultural interoperability will be a serious problem.”

Avoiding this problem lies in a communication system that is based on the concepts of the SoS called for by this ORD. All of the efforts of the National Emergency Management Network (NEMN) is wasted without a NCRN. Ham radios alone will not coordinate the management of a national response effort. EROs and FERPs need resilient voice and data communication capability that will interoperate with other EROs and FERPs.

3 Existing System Shortfalls

Why do current systems fall short of providing the capability to meet the NIMS requirements?

“To provide for interoperability and compatibility among Federal State and Local capabilities, the NIMS will include a core set of concepts, principles, terminology, and technologies covering the incident command system, multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications; and certification; and the collection, tracking and reporting of information and incident resources.”

Specifically, current systems fall short in these areas:

- Most systems are not resilient. Systems that depend on a fixed infrastructure, dedicated networks and proprietary technology are not reliable in a response to a major disaster or infrastructure failure. Most systems take days if not weeks to restore when they fail. Without communications, NIMS plans fail.
- The requirements published for NIMS compliance by EROs lack a communications framework that simplifies the process of implementing a system that meets the requirement for interoperability and compatibility. Most EROs lack the technical resources to filter through the plethora of available systems. In many cases, communications specialists who are making these decisions are only experienced in analog radio systems or telephony and are being forced to make IP networking decisions in which their lack of knowledge leads them to spend their budget on systems that only provide part of the capability they need. EROs need options that work within a

Example Only

communications framework that will guarantee interoperability and compatibility with any agency or ERO.

- Systems are too expensive. The ERO buys a system that is limited by budget or grant realities. This result is limited capability. They have what they can afford, not what they need. Every ERO and FERP need full resilient communications capability.
- Systems are too complicated. One major provider of systems that any ERO would deem reliable is selling a solution that requires three (3) certified technicians to operate. The ERO has a powerful system that will cost more in five years to operate than it cost to purchase. A FERP will not have the needed communication capability if the technician cannot get to the incident scene. This could take hours in most cases and in the case of a major disaster, days.
- Many systems rely on proprietary technology that can only integrate with like devices. The major providers of communication systems provide systems based on proprietary technology that drives up the price for the ERO to not only acquire and support, but also make it difficult and expensive to interoperate with other EROs. In some scenarios, voice, video and data interoperability between different proprietary systems is not feasible.
- Many systems will fail to provide resilient communication because they are so cumbersome they require dedicated power and transportation, rendering them useless to the FERP in the first critical minutes of a response. Semi-trailers cannot travel over roads blocked by fallen trees and downed power lines. Due to the flooding, responding to Katrina meant having to fly systems and technicians in by helicopter or small planes, taking days to provide communication capabilities for rescue operations. If the systems are simple to use and FERP-portable, they could and should go to the incident site with the FERP.
- Since there is no current framework to create a system of systems today, even the grant process for funding systems is slowed down. Without a framework, it is a daunting challenge for a multi-agency grant process to verify what is being bought by the ERO is necessary and will meet the mission requirements. With a SoS, it becomes feasible to require systems be compliant with the framework, making purchasing decisions and grant processes easier.
- Most ERO systems networks are IPv4 and not IPv6 compliant. The majority of FERPs would not even notice the difference, but a system that is not IPv6 compliant is more difficult to secure in trying to support interoperability. These security concerns by themselves can cause any mutual response to fall short of the requirement for interoperability and compatibility.
- Current systems also fall short because, due to a lack of an interoperability framework supporting systems being apart of a system of systems, it is problematic if not impossible to allow EROs not only to interoperate with other EROs and FEMA, but NGOs, military and private sector security as well. Without a communications framework supporting

Example Only

communications across organizations, a mutual-aid response will likely fall short on what is needed for an effective response and rapid recovery.

4 Capabilities Required

4.1 Operational Performance Parameters

The SoS and RPCK must meet the NIMS mandate. To do so the RPCK, at a minimum must be able to:

- converge multiple protocols and networks to provide interconnectivity to any IPv4 or IPv6 network or optimally a system that will interconnect to IPv4 and IPv6 networks wired or wireless, and terrestrial or satellite (O/T)
- support IPv6 connectivity and be capable of routing to an IPv4 LAN. (O/T)
- to run two or more RPCKs at the same incident site (T) to run two or more RPCKs at multiple sites across a large area and support collaboration of every RPCK or IP network being used in the response. (O)
- operate on either AC or DC power (T), directly connect to any 12-volt battery, vehicle cigarette lighter, generator, tactical solar array or tactical fuel cell. (O)
- support interoperable voice, video and data applications at the incident site (T), the ability to support secure interoperable voice, video and data from the incident site with any other location in the country (O).
- provide two form factors, one portable and one that can be mounted in a mobile transport in less than one hour (T), multiple form factors enabling the ability to put a RPCK anywhere. (O)
- be carried by a FERP to an incident on foot, by small watercraft, car or SUV, helicopter or small plane (T) or, the RPCK is small enough to fit in a bag or case that the FERP is using to carry other gear into the incident (O).
- mount in fire apparatus or emergency response vehicle (T) or, small enough to fit in any ERO network rack or any mode of transportation available in the response. (O)
- setup in 20 minutes by the FERP (T) in less than ten minutes. (O)
- require no more than six steps to setup (T) no more than three steps to setup. (O)
- provide VoIP calling anywhere in the United States (T) anywhere in the world. (O)
- provide a software VoIP PBX that supports at least three phone calls at one time using a single toll-free DID (T) or able to support thirty phone calls at one time using a single toll-free DID. (O)
- support extension-to-extension dialing over the incident area (T) or support extension dialing across a WAN. (O)
- create a LAN for the incident site (T) or create a “no setup required” LAN for the incident site with software providing secure IPv4 and IPv6 routing and the ability to support organizational security requirements. (O)
- interconnect with any available network providing Internet connectivity (T) or the ability to connect to multiple networks and rollover to a backup network when the primary fails or load balance between the two. (O)
- provide 10mb network connectivity between users on the LAN (T) or 54mb network connectivity between users on the LAN. (O)

Example Only

- support interoperable peer-to-peer networking (T) support peer-to-peer video, audio and data connectivity. (O)
- provide a minimum 400mw 802.11 a/b/g wireless access point that can support non-line-of-sight wireless access to the incident LAN from up to 100 yards (T) or a minimum 400mw 802.11 a/b/g wireless access point that can support the same access from up to one mile. (O)
- support up to twenty-five users on the network at one time (T) or support up to one hundred users on the network at one time per RPCK. (O)
- provide one VoIP handset (T) or five VoIP handsets with the option of adding up to twenty-five handsets per RPCK. (O)
- support any IP-over-satellite network access (T) or have the ability to provide satellite service for the RPCK without having to increase the size of the RPCK. (O)
- provide complete instructions for setup and trouble shooting (T) or complete color-coded instructions with pictures that a FERP with an elementary education can setup. (O)
- be affordable enough to purchase and maintain (T) or affordable enough for the ERO to have RPCKs at all supporting sites with enough RPCKs to support every FERP responding to the incident. (O)
- meet COTS requirements or optimally DHS should purchase specified systems in quantity and distribute as equipment grants to NIMS compliant EROs.

The SoS at a minimum must:

- create a system of systems at an incident site simple enough for a FERP to setup in 10 to 20 minutes or optimally extend the system of systems to any system in the country, if the system has access to the Internet or mutually accessible dedicated network. Nothing more should be required other than entering the location code of the SoS.
- create a communications framework for interconnecting disparate local area data networks, video networks and radio networks and enable automatic interoperability between all interconnected networks at the incident site or optimally securely interconnect disparate networks anywhere in the country creating a WAN on-demand.
- support the interoperability of peer-to-peer communications of voice, video and data or optimally support peer-to-peer and one-to-many and many-to-many connectivity of all users within the SoS.
- provide a framework for collaboration or optimally a framework for collaboration that can provide application functionality by writing an XML document.
- support presence management and optimally will include a self aware application that several times a minute updates the SoS user list enabling dynamic collaboration and peer-to-peer communication.
- support multiple applications or optimally multiple applications and services, including multiple security services.
- operate at level 4 of the IP communication layer and optimally as much functionality as possible should operate at layer 5, 6 and 7.
- Support the Federal efforts to provide extended alerting:
 - Commercial Mobile Alert System (CMAS)
 - Common Alerting Protocol (CAP)
 - existing broadcast alert services.
- Provide a mechanism for Trusted Identity Management:

Example Only

- National Incident Management System (NIMS) requirements (SP 800-73, SP 800-78, SP 800-79, IR 6887)
- Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standard (FIPS) 201 compliance and support.
- First Responder Identification Credential (FRAC) support
- Public Law 110-53 compliance .

4.2 Key Performance Parameters (KPPs)

The key performance parameters for the SoS and the RPCK are:

- Resiliency - interoperable communications must be able to establish voice and data communications within 15 minutes from the time of arrival at the incident site. The system must provide required communications capability even if all communications infrastructure is compromised or destroyed. Redundant communication must be provided with the RPCK. If the VoIP services are not working, the FERP should be able to have peer-to-peer voice capability with anyone on the SoS. If conditions are not favorable for audio communications, the FERP should be able to send private and public instant messages or alerts and advisories using the SoS software.
- Accessibility - Communications must be established by a FERP without the need for technical support. No configuration of the software should be required to setup the RPCK. The system will be connected to the best available network and connected to an AC or DC power with phone and Internet services available to all FERPs.
- Portability – The FERP must have a portable solution they can carry with them to the incident to assure they will have communications capability immediately upon arrival. RPCKs must be man portable and operate independent of large vehicles and/or trailers.
- Interoperability - The SoS provides full interoperable voice, video and data communications among FERPS and supporting agencies and EROs regardless of communication device types. The interoperability must be dynamic. Dynamic interoperability is the ability to connect any user across any network and have the ability to connect any IP communication device with any other IP communication device. The interoperability must be at level 4 or 5 of the communication layer enabling the SoS to connect any network and run on any IP device. The SoS should also enable interoperability between interoperable radio and telephone switching systems and any data user of the SoS.
- Expandability - The SoS must not have any limitation on the number of users it can support. The number of interconnected networks cannot be limited. The RPCK must be scalable either by linking multiple RPCKs together or by running the SoS on a larger Resilient Communication Command System (RCCS). A RCCS should be able to support hundreds of users exactly as a RPCK supports dozens of users. The RCCS must also be tactical and transportable, but the need for greater scalability will limit the method of transportation to an SUV or pick-up truck. Except the RCCS should not only offer the same features and functionality as a RPCK, but also be as easy to setup and come in a kit form. Because of the greater processing power of a RCCS, the area of coverage will increase, providing greater flexibility.

Example Only

- Visibility - The SoS must be able to allow span of control and mutual assessment and collaboration at and beyond the incident area site. The software interface must support a span of control over the users allowing for grouping users into manageable groups and sub-groups without compromising security. The ability to group should be as simple as entering a code that will direct the user to their group, while allowing incident command the ability to see all resources. Peer-to-peer voice, video and data communication must allow users on demand the ability to have private one-on-one communication or private group conversations, while at the same time having incident wide communications.
- Transparency - The SoS must not only enable the interoperability of voice, video and data communications, but it must also interconnect and support other systems and networks providing alert, warnings and advisories. The SoS software will enable alerts and advisories between any FERP or ERO without needing anything but the SoS software. The alerts and advisory capability will expand to provide public advisories.
- Flexibility - The RPCK must provide a full featured software PBX that is configurable from an easy-to-use GUI interface providing QoS and options to meet the ERO and FERP requirements. The PBX should provide a toll-free DID and support hundreds of extensions if needed. The PBX will have defined calling features available for configuration by the ERO. The RPCK must support as many simultaneous calls as the backhaul will allow. The SoS should also support both IPv4 and IPv6 networking and the RPCK should provide IPv6 capability to EROs who only have IPv4 capability.
- Usability - The RPCK and SoS must work with both AC and DC power, be network agnostic and able to work in any type of weather or climate that the FERP is operating in. The RPCK should require no special environmental conditions. The RPCK must converge the network protocols involved in providing voice, video and data so that network configurations are automatically provided to the user. The FERP should be able to connect color-coded cable, power the system up and have full communication capability.
- Adaptability - The SoS communication framework must be built using XML to allow for the rapid implementation of services and development or integration of applications used for collaboration. The FERP must be able to create a system of systems, enabling scalability, interconnectivity and rapid data convergence among all responders in minutes, for all responding mutual aid agencies, remote support and chain of command. This capability will not require dedicated technical resources to maintain. The SoS and RPCK must function in any environment without need of other systems if they are not available, but seamlessly interconnect to those systems without requiring the FERP to do anything. The RPCK will turn any vehicle into a forward command post for areas that have been cut-off or are a HAZMET site. The system will go anywhere in the country and work without modifications or additional configurations.
- Affordability - The SoS is affordable to the ERO. The software enabling peer-to-peer interoperability will be freely distributed with the ERO only paying for the delivery medium. The cost of the communications framework software should decrease with the number of groups within the ERO's span of control and should be available as a software service if the ERO has limited technical resources for organizational installation and system

Example Only

administration. The RPCK must be COTS compliant and provide volume-pricing incentives.

4.3 System Performance.

There are many types of disasters in the United States, but the most common emergencies are:

Chemical Emergencies

Dam Failure

Earthquake

Fire or Wildfire

Flood

Hazardous Material

Heat

Hurricane

Landslide

Nuclear Power Plant

Emergency

Pandemics

Terrorism

Thunderstorm

Tornado

Tsunami

Volcano

Wildfire

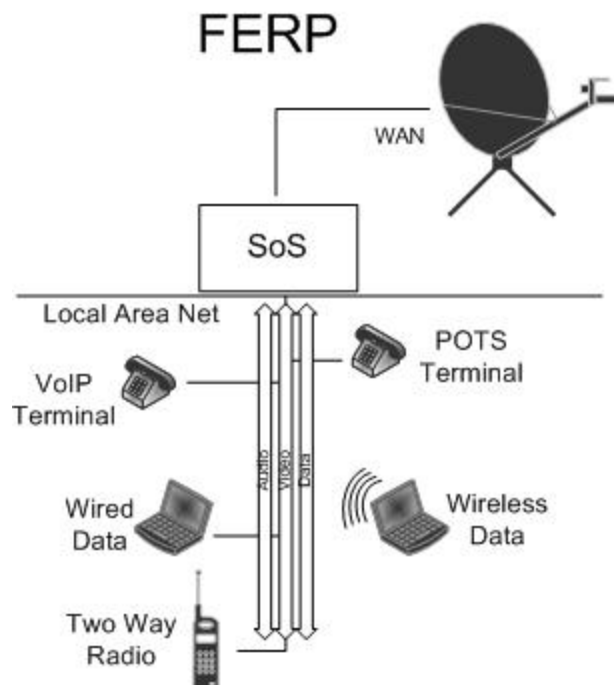
Winter Storm

Example Only

4.3.1 Mission Scenarios

Preparation and/or planning for these scenarios are paramount to enable recovery. The first and foremost consideration must be the lives of any potential victims or personnel within the immediate area of the incident site. Secondly, no situation, no matter how small, should ever be viewed in any other term than worst case scenario. If emergency responders are prepared for the worst possible situation, they inevitably will increase their odds for success. Those who fail to plan and fail to prepare are our greatest liabilities.

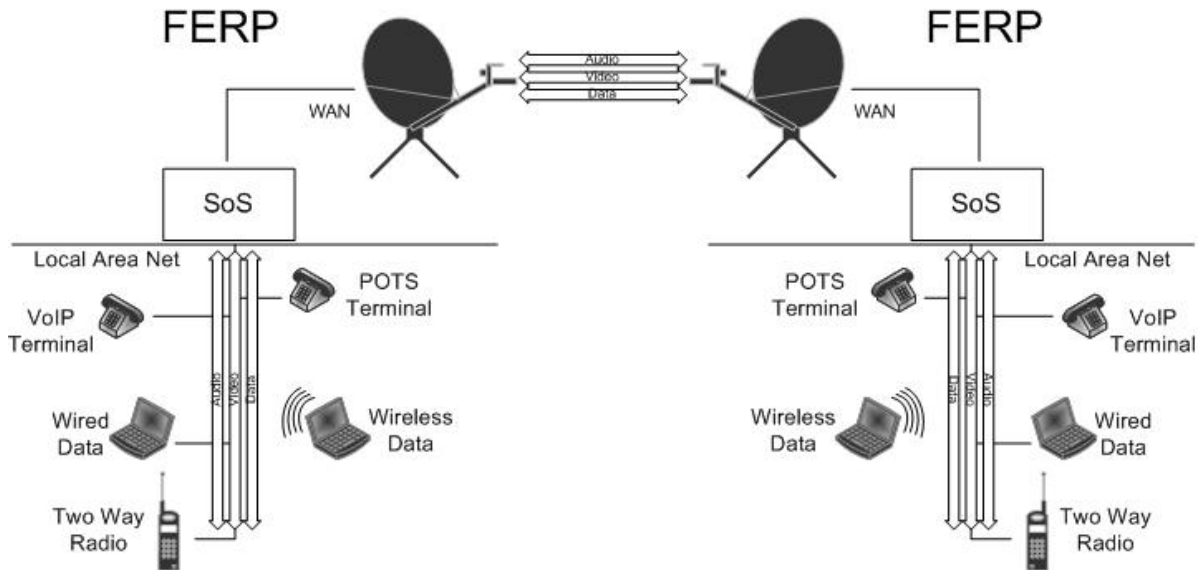
The most frightening and destructive phenomena's of nature (e.g. Hurricane, Tornado, Earthquake, Tsunami, Wild Fires, or Flooding) strike suddenly, violently, and many times in the event of an earthquake or tornado they occur without warning. If an earthquake or tornado occurs in a populated area, it may cause many deaths, injuries, and extensive property damage. There are no guarantees for safety following a disaster, identifying potential hazards ahead of time and advance planning can save lives and significantly reduce injuries and property damage. In the event of a disaster, EROs are required to do an assessment of the damage prior to allowing safety personnel and restoration groups into the incident area. Most likely, this would require communications in a scorched earth environment. FERPs would be required to setup and deploy the SoS in the disaster region and communicate to other reporting agencies to coordinate relief and aid.



In the event of a Man-Made Disaster (e.g. Terrorist or Enemy-Nation Attack) the ERO would require a number of FERP teams respond and report. The needs now are to have interoperability with these team members to include establishing two-way radio communications, data transmissions to and from multiple agencies as well as establishing an Incident Area Command Center (IACC) with full voice telephony communications mandated. If the immediate responsibility of the ERO is to assess the damages by physically entering the disaster area providing an

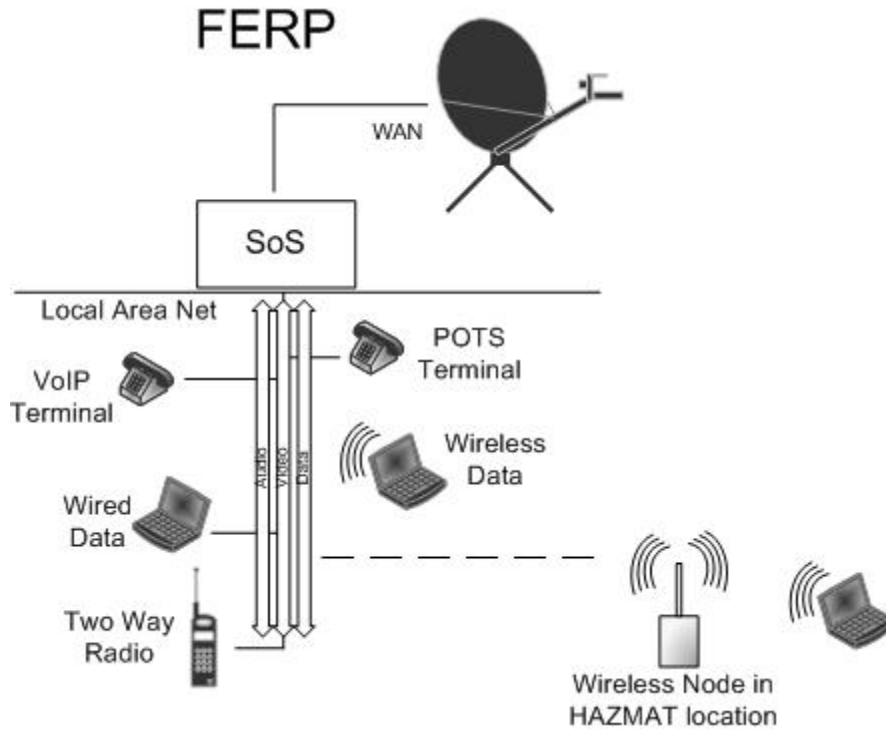
Example Only

assessment to the IACC in order to organize and manage the critical next steps of the rescue, video transmission may be required to ascertain the damages and environmental impact.



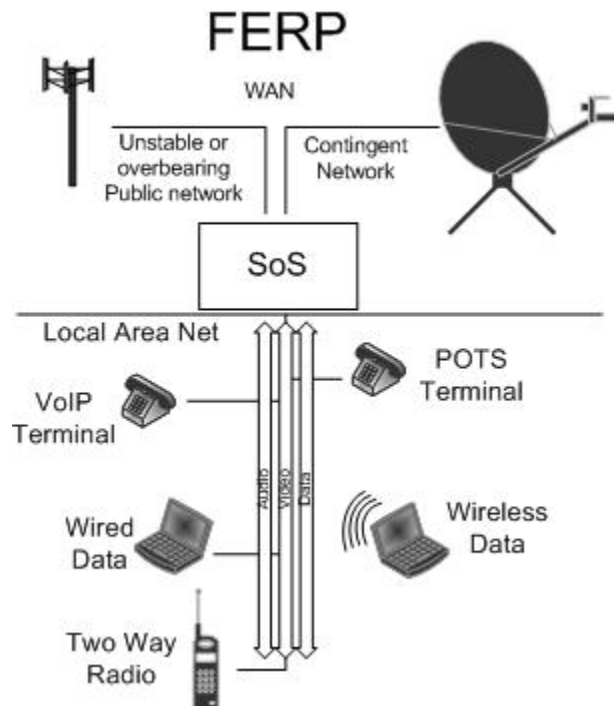
In all cases of the aforementioned disasters, all EROs need to assess the damage within the incident area, establishing communication to and from the incident site, enabling them to relay information of assessments to decision making authorities that enables them to conclude on the critical decisions for recovery. This would require the ERO to have minimal setup steps in deploying communications since the focus must be the disaster site. The SoS must be able to quickly deploy in different scenarios and adapt to different topologies of networks and environments seamlessly.

Example Only



Within 10 to 20 minutes of the FERPs' arrival at the incident area, IACC should be able to move into rescue operations. The system must now move to providing LAN and WAN capability, allowing responding personnel and agencies the ability to interoperate immediately.

Example Only



Not all responses are for emergency operations, some exceptions are large-scale events (e.g. Republican or Democratic National Convention, Super Bowl, National Sports Events, Concerts, Demonstrations or Political Rallies). These types of events can often cripple existing communication layers with an influx of traffic generated at the event site. The ERO must have the ability to overcome these obstacles easily and seamlessly. The FERP must have the ability to support two-way communications as well as telephony communications. In addition, the FERP must have the ability to send video data to and from the event site. Typically, in these types of situations, FERP members often work with civilian security and/or corporate personnel where interoperability is just a word in the dictionary. Many agencies are responsible for security at large scale events where tens of thousands of people attend. In many cases, multiple agencies, public and private are "working" the event in some manner. All require a system that establishes a LAN and WAN for all to utilize quickly and easily. In addition, this system must be able to utilize any current network infrastructure or establish its own infrastructure immediately.

4.3.2 System Performance Parameters

KPPs for the RPCKs

- Resilient communication established in 10 to 20 minutes.
- No technical support is required for any FERP to set up system.
- Portability, the common form factor should weigh less than 40lbs and be small enough to be carried on commercial airline and stored in an overhead compartment.
- Same functionality in different form factors.
- Very low power consumption, target 30 watts typical.

Example Only

- Complies with Part 15 of the FCC Rules.
- Extended-temperature operation up to +54°C (130°F).
- The enclosure must meet or exceed:
 - FED-STD-101C, Method 5007.1, Paragraph 6.3, Procedure A, Level A Tests are superseded and concurrent with ASTM B 4169, DC-18, Assurance Level I, Schedule A.
 - MIL-STD-810F, method 506.4, Procedure II of 4.1.2. FED-STD-101C Method 5009.1, Sec 6.7.1 Tests are superseded and concurrent with ASTM B 4169, DC-18, Assurance Level I, and Schedule H.
 - ATA 300, Category I, "General Requirements for Category I and II Reusable Containers".
 - Resilient to salt water spray: MIL-STD 810E Method 509.3.
 - Immersion MIL-STD-810F, method 512.4.
 - Qualified to MIL-STD-810 environmental standards.
 - Qualified to MIL-STD 810E Method 516.4. High shock/vibration exist.
 - Qualified to meet Ingress protection (IP67) while in use.
- Consist of at least 2-port WAN connections with fail over and load balancing.
- Provide an easy-to-use administration control GUI or HMI.
- Consist of at least a 4-port Fast Ethernet switch.
- Support auto-MDI-MDIX network installations, along with support for auto-crossover, auto-polarity, auto-negotiation, and bridge loop prevention.
- Allow for computing devices to be networked together using 10BaseT or 100BaseTX LAN connections.
- Field programmable, port-based VLAN functionality.
- Allow any combination of LAN ports to be connected together in subnets for use in a small secure or non-secure network.
- IEEE 802.3 and IEEE 802.3u compliant.
- Fully independent media access controllers (MACs).
- Embedded frame buffer memory.
- High-speed address look-up engine.
- Qualified to MIL-STD-810 environmental standards.
- Equipped with system status, warning, error indicators.
- Network cable complies with Category 6 standards, providing performance of up to 250 MHz.
- IEEE 802.11a/b/g/n standards (2412-2462MHz) (FCC), (5475-5725MHz) (CE), (5745-5825MHz) (FCC).
- Encryption standard must compile with 802.11i with AES-CCM & TKIP Encryption, 802.1x, 64/128/152bit WEP.
- Wireless data transfer speed up to target of 300Mbps.
- Wireless nodes peer-to-peer exceed a target of 1 km in range in line of sight environments.
- Port forwarding / tunneling allowing an external user to reach a port on a private IP address (inside the LAN) from the outside WAN connection.

Example Only

- Administration of the system must support Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) and an additional encryption/authentication layer between the HTTP and TCP.
- VoIP wired terminals support multi-line usage with up to 11 line indicators (expandable to 100 lines).
- VoIP wired terminals must support dual 10/100Mbps Ethernet ports.
- VoIP wired terminals must support basic enterprise call features (e.g. caller ID display or block, call waiting, hold, mute, speaker, transfer (blind or attended), forward, and 3-way conferencing.)
- Interconnection of Radio-over-IP (RoIP) interfaces allowing LMR radio to broadcast over SIP network.
- Connection of analog telephones or POTS terminals.
- Call types required in the RPCK or RCCS PBX.
- Activity Detection - Activity detect call feature, which provides an integrated voice terminal user a visual indication of voice activity of a particular terminal.
- Alternates / Fail-over Trunk - Automatic trunking fail-over if a primary voice trunk is determined busy, the system will switch to the next available trunk, this operation must be seamless to the terminal.
- Announcement on Hold (AoH) - Allow callers to listen to a recorded announcement/s to callers on hold or to a predefined extension. The system shall allow for one or more audio channels to be programmed to distribute audio information that is pertinent to the operation.
- Assigned Access - It shall be possible for selected dial terminals to have an assigned access (by class of service) to any combination of the following: individual nets, public address systems, radio trunks, and PSTN connections. Terminals assigned such access shall be able to obtain the desired connection by keying the appropriate number from the Address Numbering Plan, and terminals that attempt to complete a call to a destination to which access has not been assigned will receive an unavailable tone.
- Automated Attendant (AA) - The PBX shall allow callers to be automatically transferred to a user's extension without the intervention of a live receptionist. (e.g. select 1 for EOC, 2 for Field Director.)
- Blacklists - The PBX must have the capability of using a list of persons or organizations that have incurred disapproval or suspicion and therefore the call is rejected by the system.
- Call Details - The PBX shall make record and a log of all calls made including:
 - source number, destination number, call duration, date, and time.
- Call Forward - The PBX shall support a telephone call forward capability, for:
 - the user of a particular extension can chose to automatically forward calls to another desired extension or phone if their extension is busy.
 - the user of a particular extension can chose to automatically forward calls to another extension if not answered after a defined number of rings.
- Call Groups - The PBX shall support a telephone call groups' capability, for:
 - rotary hunting (where an incoming call is automatically rerouted to another terminal in a call group if the first terminal is busy, unavailable, or is not answered during the ring time out period.
 - call pickup within a call group (where any terminal in a call group can pick up a ringing call to a group member, by dialing a designated call pickup number).

Example Only

- Call Monitoring - A call monitor capability shall be supported to allow supervisors or trusted users to listen or tap into an active call with out alerting the other parties of the monitoring.
- Call Queuing - Allows multiple calls to be placed in a queue and answered by the next available call group or extension.
- Call Recording - The PBX shall support recording audio of a phone conversation for later playback or retrieval.
- Call Transfer, Hold - Once a call is connected, it shall be possible to place the call on "Hold" "Transfer" by pressing the feature code.
- The PBX must have the ability to blind transfer a call to another extension without the need to wait for the other extension to pick up.
- The PBX must have the ability to transfer a call to another extension without the need for the other extension to pick up before the call is transferred.
- The PBX must allow a call to be placed on hold. A call hold capability shall be available to all PBX subscribers who are involved in a two party call.

- Caller ID:
 - The specific terminals will display the caller's phone number on the phones screen.
 - Remote phone must send caller's ID.
 - The specific terminal will display the phone number of a second caller whilst talking to the first caller.
 - The PBX must have the ability for an administrator to change or correct the outgoing caller ID information.
- Conference Bridging - It shall be possible to host a conference bridge or room that multiple parties at multiple locations using different phone types can access. All conference bridges will have the ability to be password protected by the administrator choice. (e.g. conference calls on a local extension, remote fixed line, mobile and VoIP connection all in one conference.)
- Extensions Numbering - The PBX shall have a true flexible numbering plan feature, whereby any number from "0" to "9999" may be assigned to stations or feature codes.
- Hot-line Trunk - The PBX shall have the ability to assign designated trunks to ring designated extensions.
- Interactive Directory Listing (IDL) - IDL allows the inbound callers to lookup a person's extension by their name.
- Paging - All terminals will have the ability to 'dial direct' to an overhead speaker and or capable terminal that can be grouped or zoned for announcement or an alert to be made.
- Protocol Conversion - This allows the interconnection of disparate phone networks: (e.g. connect a Telstra call to a VoIP call.)
- Standard protocols supported include: TDM, SIP, H.323, LAX, SCCP.
- Radio Device Connection:
 - The PBX must allow the interconnection of analog terminals (e.g. Two Way Radio, Land Mobile Radio, and other like devices)
- Remote Call Pickup - This allows a call to be picked up at a remote terminal location.

Example Only

- Remote Office Support - Ability to connect phones located in a remote office to the office system as local extensions.
- Speed Dialing - Speed dial numbers shall be programmable at both the local level (speed dialing numbers that are applied to a unique terminal) and at the global level (speed dialing numbers that are applied to all terminals). Each local level speed calling list is unique to a specific terminal while the global level is available to all configured terminals.
- Three-Way Calling - Connect three people into a mini conference call.
- Voice-Mail - The PBX must have the ability to record a message from a caller when you are away from your desk. This includes ability to deliver the voice-mail message via email as well as the standard flashing light on your terminal (this feature is terminal specific).
- Satellite services when they are needed.

KPPs for Satellite Services for the RPKC

- VSAT data terminal must have the capability for Star and SCPC configurations.
- VSAT data terminal shall support at least 4 public IP addresses.
- VSAT data terminal shall support an 8 Port 10/100 Ethernet Switch.
- VSAT data terminal shall support Ku-band.
- VSAT data terminal shall support auto antenna acquisition with one button push operation.
- VSAT data terminal shall support TCP/IP throughput of transmit of 18 Mbps and receive 4.2 Mbps.
- BGAN data terminal shall support TCP/IP throughput of transmit of 464 kbps and receive 448 kbps.
- BGAN data terminal shall support audible tone signal strength for manual acquisition.
- BGAN data terminal must meet IP-54 rating (dust and spray proof in all directions).

KPPs for SoS Framework and Software

- Provide for modular system development and composition.
- Provide a method for brokering transactions amongst the composed subsystems.
- Provide translators that act as proxies for services, translating requests/responses into and out of a common, shared format (our XML-based language).
- Provide a method for definition of composition of services.
- Provide for communications among/between asymmetric clients.
- Respond to other well-known communications protocols for discrete info (including, for example, Jabber, et. al)
- Be able to render audio and video supplied in various formats.
- Be able to capture audio and video in some number of oft-supported formats.
- Provide a method for publishing availability/capabilities to other possible clients.
- Provide for authentication of credentials and access to identity information.
- Provide for transport of content in cases where peer-to-peer is not possible due to underlying network configuration.
- Provide for ad hoc network creation where indicated.
- Provide for store and forward of data where required (in, for example, cases where a client is not available at the time of original sending).

Example Only

- Provide a method of finding clients with known characteristics.
- Provide a method for decoupling content itself from the method for transporting said content to other clients.
- Provide for data transport.
- Provide for control/throttling of data transfer (particularly streamed data transfer) to ensure the viability of the local network as a whole.
- Support the Federal efforts to provide extended alerting:
 - Commercial Mobile Alert System (CMAS).
 - Common Alerting Protocol (CAP).
 - existing broadcast alert services.
- Provide a mechanism for Trusted Identity Management.
 - National Incident Management System (NIMS) requirements (SP 800-73, SP 800-78, SP 800-79, IR 6887).
 - Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standard (FIPS) 201 compliance and support.
 - First Responder Identification Credential (FRAC) support.
 - Public Law 110-53 compliance.
 -

4.3.3 Interoperability

Interoperability provided by software that creates a communication framework enables any IP device or system to create a system of systems allowing interconnectivity between any IPv4 or IPv6 user device and multiple IPv4 or IPv6 networks. Any FERP can communicate using voice, video or share data with any other FERP; limited only by the capability of their device (i.e. a LMR would be limited to voice communications). The FERP can communicate with their ERO and can collaborate with other agencies and FROs, NGO, military response teams or private sector security that may be responding to the incident. If responding organizations do not have the software prior to the incident, the SoS software that is included with every RPCK can be freely distributed from any FERP to anyone who needs it. This allows interoperability to be dynamic, changing to meet the communication needs as the response grows and evolves.

Example Only

The only requirement for interoperability is that the FERPs terminal or device has an IP or MAC address. If the use of analog devices are part of the EROs response plan the analog network can be given an IP or MAC address by connecting one of the analog terminals using the analog network be connected to a patchwork interoperability switch that in turn is a part of the SoS.

4.3.4 Human Interface Requirements

Based on a communications framework required by this ORD, the strength of a system of systems is based software that will run on any operating system, which will run on an IPv4 or IPv6 networks. There are no special human interface requirements other than knowing how to use a common phone, a LMR or computer. If the FERP can access and use day-to-day computer applications used by the ERO, then they will be able to run the SoS software. It is easier than sending an email. The FERP can use devices and terminals they already use.

The RPCK standard form factor will weigh less than 40lbs, allowing any FERP to hand carry the kit if necessary. The SoS and RPCK should require no specialized personnel at the incident site. Any FERP should be able to set up a RPCK in 10 to 20 minutes even if they have no experience or training. No matter how well designed the system is, systems do require support due to user, hardware or software malfunction. If for any reason support should be required due to equipment failure, the user must be able to use the troubleshooting guide included with the system. Around-the-clock telephone and online support will be available from the RPCK provider. The human interface requirement for this system requires the FERP to be able to read simple instructions.

4.3.5 Logistics and Readiness

The SoS will be up and utilized constantly by EROs. It can provide inter-agency interoperability on a daily basis and be in operation when an incident occurs. As the FERP arrives at the incident site, interoperability and collaboration are immediate just by the FERP turning on the devices they are using; the FERP connects automatically to the SoS.

In order to facilitate interoperability with EROs and FERPs that do not have the SoS software, the software must be available to every FERP on a USB thumb-drive that can be used to freely install on any computer required to join the SoS. The installation software should also be available to load on ERO servers so that the software can be freely downloaded if necessary. The SoS software should also be downloadable from approved websites with proper security clearance. Installation of the software must be quick, simple and intuitive. No training should be necessary for any FERP to install the software and connect to the SoS.

If the device is only able to run on an IPv4 network, free VPN software must be available for installation. Installing and using the VPN should require no configuration. If a VPN is needed it should be as simple as clicking on ‘install VPN’ and the VPN must automatically install, configure and connect the FERP to the SoS via the VPN.

If software updates are released for the SoS or RPCK, a release method of freely upgrading will be implemented.

Example Only

At least one RPCK should be available to every ERO in the country. Because a requirement for the RPCK is that it be a self-contained kit, distribution of new kits, additional kits, accessories such as additional VoIP handsets, cameras, headsets, cables, satellite systems should be managed under a contract with a national technology logistics company. Logistics must be handled by an organization, which specializes in delivering network technology efficiently to the public/private sector. Efficient distribution and parts should be stored in strategically located sites in order to guarantee delivery to the ERO in less than 8 hours. A just-in-time inventory method should be used to avoid using public funds to stockpile systems. A purchasing system should be instituted to guarantee EROs the ability, once a state of emergency is declared, to order additional systems, parts and accessories immediately.

4.3.6 Other System Characteristics

The SoS and RPCK will be simple to use and affordable. VoIP services will be provided with a flat rate annual contract for unlimited calls. Every RPCK will have an available satellite option for resiliency; the cost of constant satellite services will be affordable. DHS should negotiate flat rate contracts with providers for on-demand satellite service when the RPCK is deployed. Every system should always be on and able to support a phone call to the national support center requesting that additional bandwidth be provided for the duration of the incident. Without a national plan, the cost of satellite services may be more than the cost and maintenance of the kit.

5 System Support

5.1 Maintenance

A maintenance agreement should be in place on every SoS system and RPCK.

The SoS will run around the clock, if issues arise, users should contact the support desk. The support will be available unceasingly for SoS. If updates to the SoS software are needed, the update will be sent directly to the user by the support desk and will be downloadable from a support website.

The RPCK must be used regularly in everyday operations or be required to be tested twice a month to be confident that there are no problems with the kit's performance. The day-and-night support center must have the ability to run remote diagnostics on any kit and if possible repair the system remotely. If a kit has a component failure that cannot be immediately fixed at the users' location with the assistance of the support desk, a loaner will be shipped to the ERO immediately. The ERO will ship the "down" system to the repair depot. Under the support maintenance agreement the loaner system is provided at no charge until their repair kit is returned and tested by the ERO. A ratio of loaners available to kits in service will be 1 to 30.

5.2 Supply

The installation software will also be available on ERO servers so that the software can be downloaded from the ERO server if necessary. The SoS software should also be downloadable from approved, secure websites with proper authorization. Installation of the software must be quick, simple and intuitive. No training should be necessary for any FERP to install the software and connect to the SoS.

Example Only

Because a requirement of the RPCK is self-containment, distribution of new kits, additional kits, loaner kits should be available if a RPCK fails. Accessories such as additional VoIP handsets, cameras, headsets, cables, satellite systems should be managed under a contract with a national technology logistics company that specializes in delivering network technology efficiently to the private/public sector. Efficient distribution requires parts be stored in strategically located depots in order to guarantee delivery to the ERO in less than 8 hours. A just-in-time inventory method is required to avoid using public funds to stockpile systems. A purchasing system is required to guarantee EROs the ability, once a state of emergency is declared, to order additional systems, parts and accessories immediately.

5.3 Support Equipment

The RPCK will include any equipment necessary for testing and the system must be available to be tested remotely by support if need. The remote diagnostics will require nothing more than the customer's approval.

5.4 Training

The SoS and RPCK will be simple enough that user training is not required. However, in order to maximize the power of the SoS and to fully understand what the RPCK is capable of, webinars will be held everyday on a regional basis covering topics that will improve the effective use of the SoS and RPCK. An online group forum will be available for FERPs to share ideas and ask questions of other FERPs. This service will be a feature of the SoS software.

5.5 Transportation and Facilities

The SoS is software and does not require transportation or storage. The RPCK by design must be small enough to store in the trunk of a car or in a closet in the FERPs office or duty station. It will be able to be stored anywhere with a temperature between minus ten degrees Celsius and fifty degrees Celsius. The RPCK will require no special transportation; however, it must be available in a form factor that can be mounted in any vehicle, making that vehicle a mobile resilient communication center. It also will be able to be used anywhere at anytime without any special installation being required and easily be transportable as carry-on luggage on any commercial airline.

6 Force Structure

Many homeland security applications rely on resilient communications; there can be no SoS without communications systems to connect to. In order to implement a national SoS providing national interoperability, enough RPCKs must be distributed across the country to provide resilient communication in enough locations to guarantee a national emergency communication network can be created from a system of systems. It would take 200,000 RPCKs to provide at least one system to each of the following:

Example Only

Potential system users	Approximate Number
Law enforcement agencies in the United States	17,000
Fire departments in the United States	30,000
Incorporated cities in the United States	80,000
Counties and or Parish Governments in the United States	3,000
School Districts and Colleges in the United States	20,000
Emergency Operation Centers in the United States	15,000
Ports of entry in the United States	240
Critical Infrastructure and Key Assets in the United States	33,000
Hospitals in the United States	5,500

These numbers do not reflect the number of court houses whether Federal, State, District or Local, the number of jails and or prisons, total number of Federal Government agencies buildings or personnel in the United States, the number High Schools, Middle Schools or Elementary Schools in the United States. The numbers also do not reflect the number of substations and offices within a particular category. If a RPCK was distributed to each of the 53,000 fire stations alone, the infrastructure for a national resilient communications network would be in place.

The SoS will be distributed to every FERP (as many as one million copies in the first six months) in the country as soon as possible, even without a kit the SoS can be created and as long as communication infrastructure is sound, a local, regional, state and national interoperability network will be created enabling collaboration and cooperation.

7 Schedule

The SoS should be rolled out in phases. Year one should establish SoS groups in the most vital areas creating a national framework of senior FERPs, EROs and supporting agencies with a nation-wide roll-out completed in less than four years.

8 System Affordability

The total price for core components to meet the mission described in the ORD shall be less than \$20,000 (in high volume production).

9 Signatures

Sponsor's Acquisition Program Manager [print and sign] Date

Sponsor's Representative [print and sign] Date

S&T Project Manager [print and sign] Date

S&T Division Head [print and sign] Date

10 Appendixes

1. In this document, the terms "product" and "system" are synonymous. The word "system" is used to refer to either.
2. The word expensive as it relates to emergency response communications not only means the acquisition costs of expensive hardware and software, but the costs of ongoing maintenance, training and support costs that many times exceed the cost of the actual hardware and software.
3. The term "scorched earth" here means an incident scene where normal communication infrastructure need for voice, data and/or video communication has been severely compromised destroyed or does not exist.
4. Stennis Space Center was without communication infrastructure for over 2 weeks after Hurricane Katrina made land fall.
5. An example of what is meant by 'pony express', In responding to the disaster created by Hurricane Charley in August of 2004, 17 FROs responding to provide mutual aid to a devastated Hardee County Florida, for days had to rely on passing notes between command posts and having responders drive 45 miles to relay communications to areas not affected by the destruction of the communication infrastructure in southwestern and central Florida.

11 Glossary

Resilient	Recovering readily from injury, adversity, or the like while returning to the original form.
System of Systems	A collection of task-oriented or dedicated systems that pool their resources and capabilities together to obtain a new, more complex, 'meta-system' which offers more functionality and performance than simply the sum of the constituent systems.
Dynamic Interoperability	A property referring to the ability of diverse systems and organizations to work together (inter-operate) characterized by continuous change, activity, or progress.
IPv4	<p>Internet Protocol version 4 (IPv4) is the fourth iteration of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. IPv4 is the dominant network layer protocol on the Internet and apart from IPv6 it is the only standard internetwork-layer protocol used on the Internet.</p> <p>IPv4 is a data-oriented protocol to be used on a packet switched internetwork (e.g., Ethernet). It is a best effort protocol in that it does not guarantee delivery. It does not make any guarantees on the</p>

Example Only

correctness of the data; this may result in duplicated packets or packets delivered out of order. These aspects are addressed by an upper layer protocol (e.g. TCP, and partly by UDP).

IPv6

Internet Protocol version 6 (IPv6) is a network layer for packet-switched internetworks. It is designated as the successor of IPv4, the current version of the Internet Protocol, for general use on the Internet.

The main change brought by IPv6 is a much larger address space that allows greater flexibility in assigning addresses.

The large number of addresses allows a hierarchical allocation of addresses that make routing and renumbering simpler. With IPv4, complex CIDR techniques were developed to make the best possible use of a restricted address space. Renumbering, when changing providers, can be a major effort with IPv4. With IPv6, however, renumbering becomes largely automatic, because the host identifiers are decoupled from the network provider identifier.

COTS

Commercial off the Shelf

ERO

Emergency Response Organization

FERP

First Emergency Response Provider

RPCK

Resilient Portable Communications Kit

RCCS

Resilient Communication Command System

NCRN

National Communication Resiliency Network

GUI

Graphical User Interface

QoS

Quality of Service

IACC

Incident Area Command Center

OPERATIONAL REQUIREMENTS DOCUMENT

Persistent Intelligence, Surveillance and Reconnaissance Family of Systems Services

Contents

1. GENERAL DESCRIPTION OF OPERATIONAL CAPABILITY	81
1.1. Capability Gap.....	81
1.2. Overall Mission Area Description.....	83
1.3. Description of the Proposed Product or System	83
1.4. Supporting Analysis	83
1.5. Mission the Proposed System Will Accomplish	84
1.6. Operational and Support Concept.....	85
1.6.1. Concept of Operations	85
1.6.2. Support Concept	86
2. THREAT.....	86
3. EXISTING SYSTEM SHORTFALLS	87
4. CAPABILITIES REQUIRED	87
4.1. Operational Performance Parameters.....	87
4.1.1. Deployed Ground Control Station (GCS) Employment:	87
4.1.2. Remote Split Operations Employment:	87
4.1.3. Ground Control Stations.....	87
4.1.4. Secure GCS	88
4.1.5. Displays.....	88
4.1.6. Aircrew/DHS Situational Awareness	88
4.1.7. Digital Video Interfaces	89
4.2. Key Performance Parameters (KPPs)	89
4.2.1. LRGCS.....	89
4.2.2. BLOS Communications for Multiple Aircraft Control	89
4.2.3. Computer Resources	89
4.2.4. Computer Software	90
4.2.5. Interfaces	90
4.2.6. Operational Flight Program (OFP)	90
4.2.7. Mission Planning.....	90
4.2.8 Mission Data	90
4.2.9. Certification	91
4.2.10. Airworthiness Certification.....	91
4.2.11. Airspace Access.....	91

Example Only

4.2.12. Sense-and-Avoid Requirement General	91
4.2.13. Aircrew Warning and Collision Avoidance	91
4.2.14. Field of Regard.....	91
4.2.15. Lost Link Procedures	92
4.2.16. Emergency Situations	92
4.2.17. Ground Operations.....	92
4.2.18. Takeoff and Landing	92
4.2.19. In-flight Operations.....	92
4.2.20. Cautions and Warnings.....	92
4.2.21. Data links	92
4.2.22. Multi-band LOS Datalink	92
4.2.23. Tactical Video Streaming and Imagery Data link	93
4.2.24. Single Frame Imagery Dissemination	93
4.2.25. Voice Communications	93
4.2.26. Aircraft Radio Communications.....	93
4.2.27. GCS Radio Communications	93
4.2.28. GCS Intercom	93
4.2.29. Navigation	94
4.2.30. Surveillance.....	94
4.2.31. Global Air Traffic Management (GATM) Requirements	94
4.2.32. Propulsion system.....	94
4.2.33. Weather Hazards	94
4.2.34. Flight Data Recorder	94
4.2.35. Lost-link Performance	95
Payload Characteristics.	95
4.2.36. Mission Kits	95
4.2.37. Sensor/Payload Capabilities	95
4.2.38. Electro Optical/Infrared Sensor(s).....	95
4.2.39. Sensor Bore-sighting.....	95
4.2.40. Automatic Search Pattern/Automatic Cuing.....	95
4.3 System Performance.	96
4.3.1 Mission Scenarios	96
4.3.2 System Performance Parameters	96
4.3.3 Interoperability.....	97

Example Only

4.3.4 Human Interface Requirements	97
4.3.5 Logistics and Readiness	98
5. SYSTEM SUPPORT	98
5.1 Maintenance	98
5.2 Supply	99
5.3 Support Equipment.....	99
5.4 Training.....	99
5.5 Transportation and Facilities	100
6. FORCE STRUCTURE	100
7. SCHEDULE	100
8. SYSTEM AFFORDABILITY	100
SIGNATURES.....	101

1 General Description of Operational Capability

The Department of Homeland Security (DHS) requires the capability to commercially lease reusable, medium altitude Intelligence, Surveillance, and Reconnaissance family of systems to augment Customs and Border Patrol (CBP), United States Coast Guard (USCG), Immigration and Customs Enforcement (ICE), and the Federal Emergency Management Agency (FEMA) in support of their mission areas. The leasing of this family of systems should be low cost compared to DHS acquisition, operations and maintenance of MQ-9 Predator B unmanned aircraft, have high reliability, maintainability and availability, be easily transportable, and provide full connectivity at all levels of command and control. This family of systems lease includes tactical unmanned aircraft systems (UAS), medium altitude long endurance (MALE) UAS, and the command and control connectivity to provide all appropriate DHS nodes full motion video, voice, and data transmission and reception at all echelons. Each UAS is packaged as a “fly away kit” which can be transported to any required border region in support of CBP, and moved as necessary in support of USCG, ICE, and FEMA. The required C2 connectivity is also self-contained and can be transported to the appropriate location as required to support the missions. These “kits” are designed to be scalable, and tailorable to support DHS needs.

1.1 Capability Gap

CBP is actively engaged in the Secure Border Initiative to attain the ability to gain operational control of our nation’s borders by providing 24-hour, year-round surveillance capabilities that will help deter illegal entry attempts into the United States, and enable USBP agents to detect, analyze, and rapidly respond to illegal cross border activity. The MQ-9 Predator B Unmanned Aircraft System (UAS) augments Customs and Border Protection Air and Marine (CBP A&M) assets supporting ground interdiction agents on the Southwest Border. CBP A&M is engaged in the Department of Homeland Security’s (DHS) mission to prevent terrorist attacks within the United States, reduce its vulnerability to terrorism, minimize damage from attacks that might occur, and streamline recovery efforts. CBP A&M accomplishes this mission through an integrated and coordinated air and marine force engaged in the detection, interdiction, and prevention of acts of terrorism arising from unlawful movement of people or illegal drugs and other contraband. However, this capability is resource constrained and is assumed to be so for the foreseeable future. Currently, CBP A&M operates 4 MQ-9 UAS in support of southwest, southeast, and northern border regions, in addition to over 260 manned aircraft throughout these three border regions. A persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems can readily augment CBP A&M and provide both enhanced capability and improved persistence at a lower cost per flight hour. The family of systems immediately provides a turnkey, “power by the hour” ability to apply additional UAS into an area of interest, increasing sensor dwell time, reducing revisit rates, and accomplishes this at a much lower cost compared to using manned aircraft.

The capabilities described in this ORD also support the DHS objective of Maritime Domain Awareness (MDA) which is the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or

Example Only

environment of the United States. MDA is the integration of Global Maritime Intelligence and Global Maritime Situational Awareness. Global Maritime Intelligence is the product of legacy, as well as changing intelligence capabilities, policies and operational relationships used to integrate all available data, information, and intelligence in order to identify, locate, and track potential maritime threats. A persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems enhances MDA by providing increased numbers of sensors, superior persistence, at a lower cost than manned alternatives.

The United States Coast Guard is a military, multi-mission, maritime service within the Department of Homeland Security and one of the nation's five armed services. Its core roles are to protect the public, the environment, and U.S. economic and security interests in any maritime region in which those interests may be at risk, including international waters and America's coasts, ports, and inland waterways. USCG protects America's maritime borders from all intrusions by: (a) halting the flow of illegal drugs, aliens, and contraband into the United States through maritime routes; (b) preventing illegal fishing; and (c) suppressing violations of federal law in the maritime arena.

USCG Unmanned Aerial Vehicles (UAVs) can provide persistent wide area surveillance at both strategic and tactical levels. Access to sensor coverage and data provided by UAVs may reduce some operational requirements for conventional aircraft, by extending the mission reach of Coast Guard operational units. UAVs will contribute to a range of missions, including maritime border protection; law and treaty enforcement; and search & rescue. To date, the USCG has not acquired any UAV systems, but instead is collaborating with CBP to provide an interim unmanned capability using a portion of their MQ-9 assets, stretching thinner a four vehicle fleet. A persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems can fill this critical gap, by providing dedicated systems to support USCG that can ensure dedicated capacity to support USCG missions.

The primary mission of the **Federal Emergency Management Agency** is to reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters, by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation. A persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems could provide dedicated UAS assets to assist FEMA in damage assessment, search and rescue, and Chemical-Biological-Nuclear-Radiological and Explosive (CBRNE) consequence management.

U.S. Immigration and Customs Enforcement (ICE), the largest investigative arm of the Department of Homeland Security (DHS), is responsible for eliminating vulnerabilities in the nation's border, and with economic, transportation and infrastructure security. ICE intelligence professionals process information from a variety of sources to provide assessments of patterns, trends and new developments in a wide range of law enforcement areas. Intelligence focuses on data and information related to the movement of people, money and materials into, within and out of the United States, to provide

Example Only

accurate and timely reporting to ICE leadership and field agents in support of enforcement operations. A persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems could provide dedicated UAS assets to assist ICE in support of their mission.

1.2 Overall Mission Area Description

This ORD supports the following Office of the Secretary of Homeland Security Mission Areas: Land Surveillance and Reconnaissance, Maritime Surveillance and Reconnaissance, information sharing, and command and control.

1.3 Description of the Proposed Product or System

The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems will build on the capabilities existing in the CBP, USCG, FEMA and ICE and provide significant, additive capability to DHS. It provides a loitering and persistent capability not previously available to personnel at all echelons, from the border patrol agent monitoring the southern US border, first responders, Coast Guardsmen, all the way up to the President of the United States. Each persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems will have a baseline payload of sensors that offer multi-spectral acquisition capability. The system will be flexible enough to add additional combinations of payloads and the capability to carry interchangeable, but compatible, payloads for flexibility. The ISR family of systems aircraft and mission payloads will be remotely operated throughout the range of DHS operations. The system will collect and process information that can then be reported or further exploited to accomplish the intelligence functions of indications and warning, support to appropriate DHS agencies and departments requiring surveillance and reconnaissance services. The ISR family of systems includes a variety of commercial off the shelf (COTS) remotely piloted aircraft (RPA) systems, associated payload(s), data link(s), ground station(s), communications and dissemination systems, logistics support packages, and an ability to accomplish the following functions: Command and Control (C2) of multiple air vehicles and payloads; compliance with all appropriate communications architectures that permit interoperability with any other system that complies with standard formats for data and direct dissemination via the data link. Additional exploitation system capability can also be added, at the discretion of DHS.

1.4 Supporting Analysis

This ORD supports Homeland Security Presidential Directive (HSPD):

HSPD – 2: Combating Terrorism through Immigration Policies to prevent aliens who engage in or support terrorist activity from entering the United States

HSPD – 4: National Strategy to Combat Weapons of Mass Destruction which applies new technologies, increased emphasis on intelligence collection and analysis, strengthens alliance relationships, and establishes new partnerships with former adversaries to counter this threat in all of its dimensions

Example Only

HSPD – 5: Management of Domestic Incidents. The ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system

HSPD – 13: Maritime Security Policy. Establishes policy guidelines to enhance national and homeland security by protecting U.S. maritime interests

HSPD – 19: Combating Terrorist Use of Explosives in the United States. The prevention and detection of, protection against, and response to terrorist use of explosives in the United States.

This ORD supports DHS S&T continuing need to develop the means for greater first responder participation in the definition of capability gaps in order to ensure their high priority needs are met. DHS customers' critical needs take the form of Enabling Homeland Capabilities (EHCs), consisting of technologies that can be developed, matured, delivered, and commercialized or validated as a standard within a 3-year period. This ORD directly addresses the following EHCs:

Border Security

DHS S&T Leads: Customs & Border Protection and Immigration & Custom Enforcement

- Detection, tracking, and classifying of all threats along the terrestrial and maritime border including numerous topographies such as rugged terrain, concealing foliage, water obstacles, mountains, and other environmental constraints

Infrastructure Protection

DHS S&T Lead: Office of Infrastructure Protection

- Advanced, automated, and affordable monitoring and surveillance technologies

Interoperability

DHS S&T Leads: Federal Emergency Management Agency and Office of Emergency Communications

- Standardize, pilot, and evaluate emergent wireless broadband data technologies and applications
- Provide seamless access to voice and data networks, using a unified communications device

1.5 Mission the Proposed System Will Accomplish

The missions that the persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems will accomplish include, but are not limited to:

- Border Security
- Port Security
- Natural Disaster Response

Example Only

- Search and Rescue
- Man-Made Disaster Response
- Special Security Event Support

1.6 Operational and Support Concept

1.6.1 Concept of Operations

The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems will function as a stable of dynamically re-taskable assets, able to combine all elements of the ISR process. It will leverage existing COTS capabilities to increase mission effectiveness and create synergies for DHS. The family of systems will rapidly flex between Intelligence, Surveillance, Reconnaissance, search and rescue, and disaster response where appropriate.

The family of systems will operate primarily at medium altitudes, but will also contain capability for short range, low altitude operations in supporting DHS. It will seamlessly integrate with existing DHS assets from CBP, USCG, FEMA, and ICE as well as other government agencies as DHS shall direct. The family of systems will extend the department's eyes in the area of operations and provide the ability to immediately transition to a different role when appropriate. Command and control (C2) through all echelons will enable the family of systems to rapidly transition within the ISR collector, communications relay, and search and rescue roles.

The family of systems will integrate with existing DHS agency C2 concepts and organizations and existing tactics, techniques, and procedures: operational control will be exercised through the appropriate DHS agency, and the platforms will deconflict using normal air traffic control and airspace control measures, such as a temporary flight restriction (TFR). Its persistence and ability to communicate with C2 nodes and other DHS assets render the ability to accomplish critical DHS missions under adverse surface weather conditions. The family of systems will use off-board data, robust sensors, and automatic cueing to detect persons in areas of interest. Immediate, automated processing of data will derive actionable coordinates to assist other DHS assets to accomplish their respective missions. Improved communications/data links and situational awareness displays will ensure full area of interest integration at all DHS command and control echelons. A modular architecture permits tailored mission flexibility, where the family of systems acts as the platform to employ specialized sensor payloads, such as communication relay.

The family of systems will offer DHS personnel and planners a low-cost, persistent capability to perform a wide variety of DHS missions augmenting existing assets in achieving desired outcomes. It will seamlessly integrate with manned and unmanned platforms on the ground, in the air, and in space. Digital, open-ended, machine-level interfaces will leverage information technology to rapidly and accurately locate, identify, and act on critical emerging items of interest and facilitate the timely flow of actionable information to all echelons of command. The family of systems is scalable, and tailorable to meet DHS means. The family of systems will be available to DHS as a leased service using a "power by the hour" concept.

Example Only

1.6.2 Support Concept

Logistics support will be managed by the family of systems service provider and shall be integrated into the existing commercial support structure. The family of systems must have a maintenance concept that provides for high reliability, maintainability, and availability at the minimum cost. The service provider will perform all maintenance with a focus on maximizing rapid transportation, minimizing repair turnaround times, and minimizing payload reconfiguration times. Standard test and ground support equipment, petroleum, oil, lubricants, line replaceable units (LRU), and repair parts will be used. Peculiar support equipment, manning, training, unique aviation fuel and facility requirements will be minimized. The service provider will be responsible for technical data, training, and procedures. The logistics support concept should maximize system availability, flexibility and self-sufficiency. Stages of various levels of contractor support may be required prior to Initial Operational Capability for each increment to provide supply and maintenance technical support during the build up phase. For operations in sensitive environments, DHS users must have easy and reliable sustainment capability for both austere operations and airfield operations.

Supply support will be accomplished by the service provider (Threshold). Contractor supply data systems must provide DHS users total asset visibility throughout the supply chain and meet the protocols for, and interface with any DHS or other government agency supply data system (Threshold). The service provider will provide personnel to support operations from existing DHS facilities, and deployable contractor manpower positions, if required. Supply/resupply methods will not require additional reporting procedures. To the extent possible, parts should be properly configured with current software and delivered with all proper seals, gaskets, pneumatic, and electronic interface connections installed so they may be directly connected in accordance with the appropriate technical orders. The service provider is responsible for shipping mission critical parts originating from the contractor facility to any location supporting DHS operations. Required parameters for United States deliveries: 48 hours (Threshold) from supply system requisition to delivery of parts to aircraft, 24 hours desired (Objective).

2 Threat

The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems will face a wide array of threats during operations ranging from humanitarian operations like disaster relief, to low-intensity operations like supporting CBP, to high-intensity operations like response to a terrorist attack. As an attritable asset, the family of systems may execute missions in higher risk scenarios (e.g., CBRNE exposure) than a corresponding manned platform. Possible threats to the family of systems range from small arms (e.g., looters/rioters) to surface-to-air missiles (SAM) including man portable air defenses (e.g., terrorists), fixed-wing and rotary-wing aircraft, directed energy weapons (to include lasers and radio frequency weapons), nuclear, biological, and chemical (NBC) weapons, and information warfare. The most severe threat to the proposed family of systems will be a combination of these diverse systems, with the degree of severity being mission scenario dependent. In addition, terrorism and sabotage are also threats at all operating locations. Ground control stations are subject to the same

Example Only

threats as other assets at the location they are operating from but could be a higher priority for a surgical attack depending upon other collocated assets.

3 Existing System Shortfalls

Of all of the DHS agencies addressed by this ORD, CBP is the most advanced with four MQ-9 UAVs, building to an eventual fleet of 20 aircraft supporting both the southern and northern border. However, in the event horizon for this ORD, there remain critical gaps in ISR coverage that could be filled by utilizing the persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems capability.

The USCG is now partnering with CBP to investigate using MQ-9 UAVs in support of maritime ISR in the southeast region of the United States. Even with this assist from CBP, USCG currently has no deployable ISR assets for their fleet. The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems can close this critical gap.

Likewise, FEMA must rely on other government agencies to supply ISR support in response to natural or man-made disasters. The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems would provide FEMA an in-house disaster response capability.

Finally, ICE would benefit from the use of the persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems supporting intelligence collection on high profile criminals and terrorists in support of their mission.

4 Capabilities Required

4.1 Operational Performance Parameters

The system must support flexible employment options and must support DHS operations basing (Threshold).

4.1.1 Deployed Ground Control Station (GCS) Employment:

A complete persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems consists of a GCS and/or Launch and Recovery GCS (LRGCS), four aircraft, data link, and support equipment (SE) collocated at a DHS operating location (Threshold).

4.1.2 Remote Split Operations Employment:

The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems uses a GCS or a LRGCS deployed at a DHS operating location, launches an aircraft and hands it off to a GCS located in or outside the area of interest Beyond Line Of Sight from the launching GCS/LRGCS (Threshold).

4.1.3 Ground Control Stations

The GCS is either mobile to support forward operating locations or at a fixed facility to support remote split operations. A mobile GCS is containerized for deployability. A fixed facility GCS consists of identical capability in a permanent facility. For the persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems it must

Example Only

(1) have the capability to perform mission planning, (2) provide a means for manual and/or autonomous control of aircraft and payloads, (3) allow personnel to launch, recover, and monitor aircraft, payloads, system communications status, and current and forecast weather along entire route and vicinity for duration of flight, (4) receive payload sensor data, (5) display all-source threats to the aircraft, (6) display Common Operational Picture, and (7) provide support functions. The ground station must perform these functions as required, prior to, and during, each family of systems mission.

A deployed system must support 24 hours per day, seven days per week operations for 30 days (Threshold). Ground stations, except LRGCS, must be able to control two aircraft simultaneously (one full mission and one ground operations, takeoff, enroute navigation and landing) to support continuous area of interest coverage (Threshold). Multiple full air vehicle control of at least four aircraft is desired (Objective). The GCS must provide redundancy for vehicle control (Threshold). Workstations for all other functions listed above must be reconfigurable (Objective).

The GCS will receive, process, format and perform quality control of sensor data, sensor auxiliary data, and platform navigation data from at least one (Threshold), four (Objective) aircraft for dissemination/exploitation. The mobile ground stations and associated equipment must be operable and supportable from forward deployed and austere locations (Threshold). The ground station must be able to record and store collected data (Threshold), in a commercial off-the-shelf (COTS) digital random-access format/media (Objective).

To support system miniaturization and maximize operational flexibility/deploy-ability, the GCS shall be designed with modular/reconfigurable systems (Threshold), using open-architecture operating systems (Threshold). Full air vehicle and/or sensor command and control capability shall be incorporated into a ruggedized, briefcase-sized computer (Objective), and designed to work in a distributed command and control environment (Objective).

4.1.4 Secure GCS

GCS equipment and interfaces must be certified for DHS secure operations and data transmissions. System and interfaces will be certified for collateral level (SECRET (Threshold) and TS (Objective)).

4.1.5 Displays

Information required to safely perform ground and flight/mission operations will be displayed in a heads-up display (HUD) (Threshold). Information required to operate equipment/ system shall be displayed in logical menus with minimal layers and capability for single action return to the top-level menu (Threshold). Any single menu action which could result in the probability of causing harm to ground personnel or loss of the aircraft will require a warning display and a confirmatory step before execution (Threshold)

4.1.6 Aircrew/DHS Situational Awareness

The aircrew requires near-real-time situational awareness displays in the GCS that fuse mapping, charting, geodetic information, aircraft position, sensor pointing information,

Example Only

and weather. Situational awareness data must be fused into a common display (Threshold). In addition, aircrew situational awareness should be maximized by providing flight indicators and warnings using multiple sensory cues (e.g., visual, aural and tactile) (Objective). The system shall provide an aural warning when the aircraft is nearing flight conditions that exceed normal operating parameters (Objective).

4.1.7 Digital Video Interfaces

The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems should use standard digital interfaces and National Geospatial-Intelligence Agency (NGA)-compliant digital video formats (News Industry Text Format and Joint Photographic Experts Group) to maximize interoperability and imagery quality. Use GCS-based encoder and Key Length Variable (KLV) system to convert analog video outputs to Moving Picture Experts Group (MPEG)-2 and KLV private data stream (PDS) prior to disseminating to users (Threshold). Eliminate all analog-to-digital conversions by compressing digital video directly from sensors into MPEG-2 data stream, add KLV PDS to stream prior to dissemination (Objective). All of the system's data that will be exchanged or has the potential to be exchanged, shall be tagged, as required, in accordance with the standard for tagged data items (e.g. Extensible Markup Language (XML), the current JTA standard), and tags shall be registered.

4.2 Key Performance Parameters (KPPs)

4.2.1 LRGCS

The LRGCS will be capable of servicing, systems checks, maintaining, launching, and recovering aircraft under LOS control for handoff to a mobile or fixed GCS. (Threshold) It will be designed for minimal physical and logistics footprint and reduced support requirements (Threshold) and provide the ability to perform functional system checks on aircraft satellite communications systems. (Objective)

The GCS and LRGCS will provide sufficient cues to allow the pilot to safely takeoff, navigate under Instrument Flight Rule conditions to published weather minimums, and land (Threshold).

4.2.2 BLOS Communications for Multiple Aircraft Control

The ground communications terminal supporting BLOS operations shall allow one (1) to four (4) GCS connections and support for four (4) simultaneous aircraft orbits with appropriate number of hot spares (Threshold) and one (1) to eight (8) GCS connections and eight (8) simultaneous orbits with appropriate number of hot spares (Objective).

4.2.3 Computer Resources

Computer resources will consist of all hardware and software necessary to fulfill mission requirements including that associated with aircraft avionics systems, mission planning systems, weapon planning, support equipment, and data collection equipment. Software shall use a structured programming language and open-system approach (Threshold). All software shall provide enhanced system performance, maintainability, interoperability, portability, reliability, and user friendly operation. Computer hardware resources (storage, interconnecting data bus, memory, and processor) must have a 100%

Example Only

reserve over that used or experienced during the most demanding processing and storage operations (Threshold) with a goal of 200% (Objective). Storage requirement includes the entire worldwide navigation database (Threshold). Reserve resource capability shall be computed by sub-system and shall not be a system-wide average. Hardware and software must ensure data integrity is maintained (Threshold).

4.2.4 Computer Software

The software will be developed in a modular manner to promote rapid and low-risk system upgrades (Objective). Software will be releasable to other DHS contractors for under government purpose rights or restricted use in the development of associated training, planning or data exploitation systems (Threshold). All software maintenance shall be compatible with the existing DHS computer software support structure, including maintenance data collection and other information systems planned for use (Objective). Software shall be designed for reusability in the training devices, by incorporating “hooks” to support trainer-unique functionality (Objective).

4.2.5 Interfaces

External/internal system interfaces must be fully documented and defined to facilitate evolutionary growth through modular replacement of hardware and/or software (Threshold), and to satisfy requirements for interoperability with existing or projected capabilities (Objective).

4.2.6 Operational Flight Program (OFP)

OFP software changes shall be loaded and verified by service provider maintenance using standard PC based laptop computers (Threshold). Aircraft software loading/verifying will be accomplished via a standard interface (Threshold). Loading and verifying of OFP must be accomplished within 30 minutes (Threshold) 15 minutes (Objective).

Operational software version information for all Computer Software Components shall be displayed upon operator request (Threshold).

4.2.7 Mission Planning

The system will support the use of a DHS approved Mission Planning System architecture, standards and interfaces (Threshold). The capability shall consist of an automated system to provide responsive, flexible, user-friendly and accurate integration of payload and platform mission planning, including threat avoidance along the route for the flight duration (Threshold). The system must allow for pre-flight loading and in-flight updates of mission data (Threshold). System will display digital, geo-referenced current and forecast weather overlaid on GCS situational displays (Objective). The capability for sensor collection planning requirements and display of collection points on sensor operator display is required (Threshold). The ability to designate a collection objective on sensor operator display and automatically slave a designated sensor to that point in wide field-of-view is required (Threshold), in narrow field-of-view (Objective).

4.2.8 Mission Data

Personnel must be able to load and verify mission/navigation data via a data transfer system (Threshold). Aircraft and fixed/mobile GCSs data systems must be certified to

Example Only

store classified data at DHS direction (Threshold). If required by DHS, the aircrew shall have the ability to selectively zeroize data with/without power on the equipment (Threshold). The aircrew shall have the capability to zeroize all classified data (with the exception of the flight data recorder) with a single safeguarded action (Objective).

4.2.9 Certification

The aircraft system requires certifications to allow United States-wide system employment.

4.2.10 Airworthiness Certification

The aircraft system must be certified as airworthy when operated in accordance with its technical order (Threshold, KPP).

4.2.11 Airspace Access

The aircraft system must be able to operate in appropriate Federal Aviation Administration (FAA) airspace (Threshold). The aircraft system must be able to operate in appropriate classes of airspace worldwide with no additional coordination requirements than inhabited aircraft (i.e., file-and-fly) (Objective).

4.2.12 Sense-and-Avoid Requirement General

The overall performance of the sense-and-avoid system shall be such that the probability of colliding with another aircraft is comparable to that for other aircraft of similar size, weight, and performance. The measure of total system performance shall depend on, but not be limited to, such aspects as onboard sensors, air traffic control, concept of operations, and reliability. Furthermore, the system shall possess the capability to detect both participating and non-participating aircraft day and night (weather permitting), determine if a potential collision hazard exists, notify the operator of the hazard, and either provide a suggested conflict resolution for pilot action or maneuver autonomously to avoid the other aircraft (Objective).

4.2.13 Aircrew Warning and Collision Avoidance

The sense-and-avoid system shall notify the operator through some combination of visual and audible warnings when an aircraft is projected to pass within 500 feet (Threshold). The warnings shall allow sufficient time for the operator or onboard autonomous system to maneuver the aircraft to avoid conflicting traffic by 500 feet (Threshold). If the aircraft does not receive a pilot/operator command input to resolve an imminent collision hazard (defined as aircraft projected to pass within 500 feet of one another), it shall maneuver autonomously to avoid the conflicting traffic by at least 500 feet (Objective). The autonomous maneuver capability will warn the pilot/operator about the pending maneuver and incorporate an override capability, time and conditions permitting (Objective).

4.2.14 Field of Regard

The field of regard of the onboard sensor system shall be at least 110 degrees horizontal from the nose, 15 degrees vertical with respect to the flight path angle, and be able to detect conflicting air traffic during all expected maneuvers (Threshold).

Example Only

4.2.15 Lost Link Procedures

If the aircraft loses its command and control (C2) link(s), it shall have the capability to maneuver autonomously to avoid traffic and then return to its previous altitude and course once the avoidance maneuver is complete (Threshold). If the aircraft maneuvers to avoid traffic while lost link, it shall notify the aircrew of this fact upon re-establishment of the link (Threshold).

4.2.16 Emergency Situations

A reliable sense and avoid system will operate under emergency power situations (e.g., engine-out glide, battery only, etc.) (Objective).

4.2.17 Ground Operations

The system must be able to operate from airfields with other aircraft (Threshold). The aircraft must be able to operate at up to 8,000 ft density altitude with a 50-ft obstacle from prepared airfields with runways 5,000 ft by 75 ft (Threshold), 3,000 feet by 75 feet (Objective) and taxiway widths of 50 feet (Threshold). The system must also be capable of launching and recovering on unimproved areas. (Threshold)

4.2.18 Takeoff and Landing

The air vehicle must be able to takeoff and land using pilot control via the LOS link (Threshold) and allow for automated takeoffs and landings via BLOS datalink (Objective). Crosswind limitation for takeoff and landing not less than 16 knots (Threshold) to 20 knots (Objective) on a dry runway. The aircraft must be capable of takeoff and landing on wet runways (Threshold).

4.2.19 In-flight Operations

The system must operate at flight altitudes of 10,000 (Threshold), 30,000 (Objective) feet Mean Sea Level. The aircraft must be able to operate in Visual Meteorological Conditions (Threshold). The aircraft should have the capability to be equipped with a system to track vehicle position to aid in locating a downed vehicle (Objective).

4.2.20 Cautions and Warnings

Methodology for displaying system warnings, cautions, and alarms must be appropriate to the gravity of the situation (Threshold). Screen displays of system warnings, cautions, and alarms must be consistent between workstations (Threshold).

4.2.21 Data links

Software Communications Architecture (SCA) is desired for all data links (Objective).

4.2.22 Multi-band LOS Datalink

The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems requires multi-band capability to effectively support DHS operations. Field-installable, modular kits are required to allow swapping out existing LOS transceivers and antennas for data link-compliant terminals (Threshold). Integrated multi-band ground and aircraft transceivers and antennas are required (Objective).

Example Only

4.2.23 Tactical Video Streaming and Imagery Data link

The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems requires the capability to simultaneously broadcast sensor video to multiple aircraft or ground users within LOS of the aircraft (Threshold). The system shall simultaneously broadcast to multiple users over data link or other appropriate standard interface (Objective).

4.2.24 Single Frame Imagery Dissemination

Capability to allow aircrew to create a still frame image of the current sensor video frame and transmit it over LOS link to aircraft and ground users via a data single format is required (Threshold).

4.2.25 Voice Communications

SCA is required for all radios (Objective).

All aircraft and ground radios must be compatible with VHF Air Traffic Control (ATC) 8.33 kHz and 25 kHz Channel Spacing (Threshold).

4.2.26 Aircraft Radio Communications

The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems aircrew must be able to simultaneously monitor and communicate with multiple C2 nodes, aircraft, and appropriate DHS personnel using voice communications during all missions. Radios must be compatible with existing nets (FM, VHF, UHF, Maritime, and/or SATCOM) and transmission security techniques. Radios must be able to monitor the appropriate guard band.

4.2.27 GCS Radio Communications

Aircrew requires access to VHF/UHF networks within GCS LOS and:

Aircrew shall be able to transmit and receive audio for all radio channels/networks through the GCS intercom system (Threshold).

Aircrew shall be able to control the radio channel and mode from the existing operator seats (Threshold), with control integrated in the pull down menu system (Objective).

4.2.28 GCS Intercom

The system requires an integrated intercom system.

Aircrew shall be able to access all radio and telephone communications systems through a single headset/intercom system (Threshold).

The intercom system shall allow extending the intercom stations to co-located fixed or deployable ops cells (Threshold).

Intercom shall be extendable to up to 300 feet (Threshold) or 2 km (Objective).

Crew chiefs should connect on intercom nets using wireless headsets (Objective).

Example Only

The aircrew shall have the ability to define access rights for each intercom station to include radio transmit, receive/monitor only, and membership in private nets (Threshold).

4.2.29 Navigation

Basic Area Navigation shall be compliant with FAA Advisory Circular AC 90-96 (Threshold). Required Navigation Performance (RNP-1) (Threshold), RNP-0.3 (Objective).

4.2.30 Surveillance

Automatic Dependent Surveillance-Broadcast (Objective). Reduced Vertical Separation Minimum compliant avionics (Threshold). Mode S Level 2 (Threshold).

4.2.31 Global Air Traffic Management (GATM) Requirements

The persistent Intelligence, Surveillance, and Reconnaissance (ISR) family of systems must be certified to applicable civil communication, navigation, surveillance, and air traffic management performance standards to ensure access to controlled airspace (Threshold).

4.2.32 Propulsion system

The engine design must be compatible with airframe design to maximize access for on-equipment maintenance and inspections (Threshold). Unassisted ground start capability and in-flight restart capability is required (Threshold). A heavy fuel compatible engine is required (Objective).

4.2.33 Weather Hazards

The system must be equipped to detect and avoid weather hazards (e.g., thunderstorms, lightning, etc.) and the data must be provided to the ground station so operators may take action as required (Threshold). The ground station must have a terminal area weather radar display (Objective). Operators require real-time measurements from the aircraft of ambient temperature, wind speed/direction (Threshold). The system must be able to support ground, launch and recovery operations in extreme temperature conditions (-40 F to +110F) (Threshold) (-40 F to +150 F) (Objective). While sustained aircraft operations in icing or turbulence are not envisioned, the aircraft must have the capability to detect and transition through a 5,000 ft layer of light icing and/or moderate turbulence (Threshold); and transition through a 5,000 ft layer of moderate icing and sustained moderate turbulence (Objective). The aircraft and payloads design should mitigate performance degradation caused by extended, moderate exposure to environments containing sand, dust or rain (Objective).

4.2.34 Flight Data Recorder

The system must provide the capability to continuously record flight data with an operable data link (Threshold). The aircraft must incorporate a crash-survivable data recorder to continuously record the last 30 minutes of flight data during lost link conditions (Objective).

Example Only

4.2.35 Lost-link Performance

In the event of loss of data link, the aircraft must execute a preplanned, user-programmable mission profile to facilitate restoration of the data link and minimize collateral damage if link cannot be reestablished. (Threshold). The aircraft must have the capability to support automatic landing if link cannot be reestablished (Threshold).

4.3 Payload Characteristics.

4.3.1 Mission Kits

Mission kits will consist of defined equipment, sensors, and personnel required to meet specific DHS requirements and will be identified as such.

4.3.2 Sensor/Payload Capabilities

System shall be designed to allow rapid payload reconfiguration (Objective). Payloads should be hardened against laser attack (Objective).

4.3.3 Electro Optical/Infrared Sensor(s)

The sensors will have full-motion video and be capable of:
In daylight conditions, providing color, motion video with a National Imagery Interpretability Rating Scale (NIIRS) rating of 5.0 at 30,000 feet slant range (Threshold, KPP) and 8.2 at 60,000 feet slant range (Objective).

Multiple focal lengths to provide wider area surveillance at a reduced NIIRS (Threshold).

In low-light/night conditions, producing video images at a NIIRS rating of 4.0 at 30,000 feet slant range (Threshold, KPP) and NIIRS 8.2 at 45,000 feet slant range (Objective).

The sensor(s) shall be able to detect and display the location of laser target markers and Search and Rescue signaling devices (Threshold).

The system must have an eye-safe, near-infrared, multimode target marker (Threshold).

The sensor(s) will maintain an auto-track on a designated object within the design gimbal tracking limits for minimum of 60 seconds (Threshold) for 60 seconds on a moving target (Objective); on a designated object for as long as the aircraft position allows the sensor to maintain the object/target in its field of view (Objective).

Sensor operator shall be able to discontinue auto-track at will (Threshold).

4.3.4 Sensor Bore-sighting

Sensors providing three-dimensional geolocation information will be capable of manual bore-sighting (Threshold); auto-bore-sight (Objective).

4.3.5 Automatic Search Pattern/Automatic Cuing

The sensor must be able to automatically search an area with an operator selectable pattern appropriate to the item of interest type and location (raster, star, spiral, etc.) and

Example Only

cue potential items of interest (Objective). The operator should be able to manually designate displayed returns as items of interest (Objective). The operator should be able to manually break the lock on a particular item of interest; the sensor should then resume the search, locking on the next available item of interest (Objective). The system should be selectively capable of automatically cross-cueing all sensors to an item of interest within the sensor’s field-of-view, provide resolution of 5 meters or less. The system should have a capability to overlay/integrate/ fuse data over other sensor data (Objective). The system will be capable of item of interest classification, recognition, and identification (Objective).

4.4 System Performance.

4.4.1 Mission Scenarios



4.4.2 System Performance Parameters

Key Performance Parameter	Development Threshold	Development Objective
The aircraft system must be certified as airworthy	Certification complete	
Datalinks for all command, control, and dissemination networks	Compliant Datalinks	NSA Compliant, DISA Certified
The aircraft must have a minimum total endurance of 10 hours plus appropriate fuel reserves	10 hours	24 hours
Provide full motion video with a NIIRS rating at 30,000 feet slant range of:	Daylight color video 5.0 NIIRS, low light/night 4.0 NIIRS	Daylight color 5.5 at 60,000 feet slant range, low light/night 5.5 at 45,000 feet slant range
Employment of EO/IR Sensor Suite	Successful	
The system must be capable of being transported by C-130 (Military) or civilian aircraft (e.g., FED EX) by either palletized or roll-on/roll-off capability	Demonstrated capability	
All activity interfaces, services, policy-enforcement controls, and data-sharing of the appropriate interoperability profiles will be satisfied to the requirements of the specific integrated architecture products (including data correctness, data	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements	100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing*

Example Only

availability and data processing), and information assurance accreditation, specified in the threshold (T) and objective (O) values.	designated as enterprise-level or critical in the integrated architecture.	requirements in the integrated architecture.
--	--	--

System Performance Parameter Attributes:

Attribute	Development Threshold	Development Objective
System must support 24/7 operations for 30 days	24/7 operations for 30 days	
Heads-up display	Approved	
Situational awareness data	Fused into a common display	Bi-directional into the network
LOS Communications for Multiple Aircraft Control	4 simultaneous aircraft	8 simultaneous aircraft
Loading and verifying of OFP	30 minutes	15 minutes
Operational altitude MSL	10,000	30,000
Daylight video NIIRS rating	5.0 @ 30,000 ft slant range	5.5 @ 60,000 ft slant range
Low-light/night video NIIRS rating	4.0 @ 30,000 ft slant range	5.5 @ 45,000 ft slant range

4.4.3 Interoperability

The system requires an ISR Interoperability Architecture certified standard interfaces to applicable C4ISR architectures as required by DHS. Using the Joint Interoperability Test Command (JITC) Interoperability System Certification ensures that the persistent ISR family of systems contains interfaces, protocols and data standards that conform to information technology standards found in other government agencies to maximize interoperability. Critical components such as routers and switches internal to the system will be capable of providing their status to appropriate external networks (Threshold).

4.4.4 Human Interface Requirements

All system components must be ergonomic in design to eliminate personal injury of individuals operating and maintaining the system. In addition, it must be user friendly to allow ease of operation and maintenance, and must be designed to eliminate all family of systems component damage during operation, disassembly, repair, and assembly.

Example Only

4.4.5 Logistics and Readiness

High reliability, ease of maintenance and supportability are the persistent ISR family of systems requirements.

Overall	Threshold	Objective
Full Mission Capability	80%	90%
Mission Capability	90%	95%
Not Mission Capable for Maintenance	≤8%	<5%
Not Mission Capable for Supply – Overall	≤ 10%	≤ 5%
Abort Rate	<10%	<5%
Mean Time Between Maintenance Planned	Hourly- 50 hours Calendar-30 days	Hourly- 100 hours Calendar-60 days
Mean Time Between Critical Failure	500 hours	1000 hours
Mean Repair Time	<90 min	<60 min
Effective Time On Station	85%	>95%

5 System Support

Initial Operational Capability (IOC) Definition. IOC declaration is based on the system meeting the required assets available date and the service provider successfully completing a realistic trial period that demonstrates it can perform its assigned DHS mission(s). IOC declaration is meant to be event-driven and not schedule-driven. IOC is declared when the service provider demonstrates its ability to perform its assigned DHS mission(s) with the new or upgraded systems. The service provider must be sufficiently satisfied with system performance, quantities received, level of proficiency, and support capability to declare the assets initially operational and capable of performing the assigned DHS mission. IOC is declared six months after DHS leases at least one persistent ISR family of systems kit in support of one DHS agency. FOC declaration is based on all family of systems kits required by DHS to support all agencies identified by this ORD.

5.1 Maintenance

A maintenance training system will be comprised of, but not limited to, training devices, courseware, hardware, software, facilities, and personnel. The Training System will support the organizational maintenance structures and the following training categories: Initial Skills, Continuation, and Conversion/Activation Training (Threshold). Maintenance personnel will require initial skills training and continuous career field training to support mission roles. Familiarization training may be developed in the Computer Based Training (CBT) format. Training devices shall replicate the functionality of the aircraft, GCS, beyond line-of-sight communications, and associated equipment and be designed for concurrent upgrades to accurately simulate current fielded

Example Only

systems (Threshold). Devices shall support a continuous upgrade knowledge level training with troubleshooting, fault isolation, repair, and remove/replace type tasks that extend beyond the initial skills level (Threshold).

5.2 Supply

Spares Support Packages. Deployed operations will be supported through the use of spare support packages. Spare support packages will include sufficient quantities to support a full family of systems deployment in support of DHS missions for 30-days (24/7 operations) without re-supply (Threshold).

Provisioning Strategy. Sufficient spare parts must be planned, budgeted, and procured to minimize down time. Provisioning will ensure all parts upgrades and/or replacements are properly documented for installation and training prior to operational employment. Each system will require initial spares at system delivery as determined by DHS (Threshold) and a 30-day spares support package for deployed operations (Threshold).

5.3 Support Equipment

SE maintenance and calibration will be minimized. Appropriate technical documentation will be required for procured SE. The system and its SE must use standard fittings and connections (Threshold). All required SE must be operated in the same ground environment, as the system (Threshold). The quantities, characteristics, and functions of this SE will not restrict operational employment of the system in support of DHS missions. All required peculiar SE will be fielded with the delivered system for all levels of maintenance and in sufficient quantities to support the operational mission (Threshold).

Requirements for flight-line test equipment will be held to an absolute minimum and will be of minimum size, weight, and complexity needed to verify system operational status and fault isolation. The calibration of peculiar SE must be accomplished at required calibration intervals of not less than 180 days (Threshold). SE shall be selected using the following preference hierarchy (most desirable first); existing government furnished equipment, COTS, modified COTS, and newly designed SE to satisfy multiple system requirements. Any SE new to the family of systems inventory shall be delivered with complete logistics support (Threshold).

5.4 Training

The training system (e.g., syllabi, unit training devices, and training devices) must provide qualified mission operators and task certified maintainers across the training continuum. The syllabi, part task trainers, and training devices will be defined to reflect operator, maintenance, and communications personnel training needs. Training devices and part task trainers will replicate the operational equipment, controls, and displays as necessary for DHS mission accomplishment. For operations, aircrew training devices will be considered a prime source of initial, mission, and continuation follow-on training in lieu of actual aircraft flights. Training devices should integrate the effects of threats and weather on the systems. The training plan must ensure service provider personnel are trained and available to operate and maintain the system prior to IOC. Operations and

Example Only

maintenance will use an agreed to portion of the family of systems fleet to support formal training. Maintenance training shall focus on producing qualified technicians to maintain new systems, and shall include system operation and familiarization, system and subsystem theory of operation, interfaces with existing aircraft systems, troubleshooting, and task accomplishment required to support all organizational-level maintenance. Initial training and any required materials (courseware, lesson plans, charts, and diagrams) shall be procured by the service provider at least 30 days prior to accepting delivery of each new system component (Threshold). In order to allow competitive procurement of training systems, relevant interface, flight, mission, and maintenance data shall be available completely (Threshold).

5.5 Transportation and Facilities

The system design must minimize deployment footprint, be mobile, deployable, and transportable by standard means to include road, and air transportable by military, Civil Reserve Air Fleet (CRAF) or civilian aircraft. The system must be capable of being transported by C-130 (or equivalent) aircraft by either palletized or roll-on/roll-off capability (Threshold, KPP). Aircraft, GCS/LRGCS, data link and support equipment stowed for transport must suffer no internal or external damage or degradation of performance as a result of being transported by or as a result of being loaded or unloaded onto trucks or aircraft by forklift, crane, hoist, or winch, (Threshold). The design should minimize the system's deployment footprint, including basic equipment, training, operations, maintenance, and support equipment. If any portion of the system will not be used for daily flying operations, provisions should be made for long-term storage of components. The system must have the capability, under normal conditions, to tear down and prepare for movement in less than 24 hours by service provider personnel (Threshold). The system must be capable of set-up by service provider personnel and operation (one aircraft prepared for launch and one as a ready spare) within 24 hours after arrival at a deployed location (Threshold). The system must be capable of full-up operations within 36 hours after arrival (Threshold).

6 Force Structure

The solution should be usable by CBP, TSA, USSS, USCG and FEMA, as well as first responders and critical infrastructure/key resources potential users.

7 Schedule

The solution shall be available for lease within one year of the completion of this ORD.

8 System Affordability

Total lease price shall be less than \$25/square mile/day with all maintenance, spares, etc. borne by the supplier.

9 Signatures

Sponsor's Acquisition Program Manager [print and sign] Date

Sponsor's Representative [print and sign] Date

S&T Project Manager [print and sign] Date

S&T Division Head [print and sign] Date

Example Only

Operational Requirements Document (ORD)

Interoperable Communications Switch

Table of Contents

1 GENERAL DESCRIPTION OF OPERATIONAL CAPABILITY	105
1.1 Capability Gap.....	105
1.2 Overall Mission Area Description.....	105
1.3 Description of the Proposed System	106
1.4 Supporting Analysis	107
1.5 Mission the Proposed System Will Accomplish	107
1.6 Operational and Support Concept.....	108
1.6.1 Concept of Operations	108
1.6.2 Support Concept	109
2 THREAT.....	109
3 EXISTING SYSTEM SHORTFALLS	109
4 CAPABILITIES REQUIRED	110
4.1 Operational Performance Parameters.....	110
4.2 Key Performance Parameters (KPPs)	124
4.2.1 Connectivity.....	124
4.3 System Performance.	124
4.3.1 Mission Scenarios.....	124
4.3.2 System Performance Parameters.....	125
4.3.3 Interoperability.....	125
4.3.4 Human Interface Requirements	125
4.3.5 Logistics and Readiness	126
4.3.6 Other System Characteristics	127
5 SYSTEM SUPPORT	127
5.1 Maintenance	127
5.2 Supply	128
5.3 Support Equipment.....	128
5.4 Training.....	128
5.5 Transportation and Facilities	128
6 FORCE STRUCTURE	129
7 SCHEDULE	129
8 SYSTEM AFFORDABILITY	129
9 APPENDIXES.....	130

LIST OF FIGURES

Figure 1.3-1 The Critical Functions and Interfaces of the Interoperability Switching System provide First Responders Interoperability with each other and the rest of the world.....	107
Figure 1.6-1 An Interoperability Switch-Based Facility Communications System Provides Networked Communications Between any Number of Agencies and Personnel.....	108

List of Tables

Table 4.1-1 Matrix for Required Types of Terminal Calls Operations and Services	113
---	-----

1 General Description of Operational Capability

As a goal, first responders would like to be able to speak to anyone at any time in any place. With the ubiquitous cell phone, that vision seems to be nearly a reality. There is a natural desire to extend this near reality to the far more complex environments of mobile platforms, remote locations (middle of the ocean, out in the desert, atop mountains), and scenes of destruction (earthquakes, explosions, fires).

While the inability to complete a cell phone call successfully may be an annoyance in a personal situation, the inability to communicate can have deadly consequences in a public safety situation. It is therefore critical that those responsible for communications in these organizations plan ahead for contingencies, set realistic expectations, acquire necessary equipment, and conduct training on a periodic basis.

Regarding expectations, it is realistic to pre-engineer multiple solutions to specific interoperability challenges that can be relied upon in an emergency. It is not realistic to think that on-the-fly personnel can expect to successfully interoperate between communications media that have not been previously analyzed and engineered for interoperability. There are numerous challenges to successful interoperability. The right combination of equipment, knowledge, and training will lead to mission critical interoperability when it's needed most. Wishful thinking and ignoring the complexities will, in contrast, provide a false sense of security and lead to failure.

The problems and issues associated with different radio systems not being able to communicate with each other have been known to first responders for many years. The communications problems surrounding the terrorist attacks on September 11, 2001 significantly raised the visibility of this issue and have led to numerous and varied attempts to improve communications interoperability amongst first responders.

1.1 Capability Gap

One primary method of resolving communications interoperability is having all involved parties using the same, or at least interoperable, radios, whether they are cellular, portable, fixed or mounted. Since many first responders have already invested significantly in their current radio systems, acquiring new radios is often not a practical solution. This leads to the second means of resolving interoperability issues, the use of a gateway or switching type of device or system that can quickly and easily connect two or more otherwise non-interoperable radio systems. This system would allow multiple first responders to talk to each other either directly or via radio nets, all while using their existing radios, cell phones, or telephones.

1.2 Overall Mission Area Description

The mission area covered by this ORD is all public safety related events where first responders must communicate with other first responders using communications media such as radios and telephones that are not normally interoperable. This includes different

Example Only

agencies and types of first responders (police, fire, EMTs, etc.) and first responders from different jurisdictions and/or locations (city, county, state, federal, etc.)

1.3 Description of the Proposed System

Responders in the field need access to a switching system with the capability to integrate voice communications of all types in a special evolution or command and control type environment such as an Emergency Operations Center. The proposed interoperability switching system will provide the user the ability to provide advanced Private branch Exchange like capabilities between handsets connected through PSTN, IP, local radio systems (e.g. Land Mobile Radio (UHF or VHF)), commercial wireless (cellular/PCS and satellite) and other standard interface systems. The switching system shall include a full range of switching functions for telephony, radio circuits, simultaneous plain and P-25 encrypted circuits, progressive radio and telephone conferencing and netting, extensive administrative support for configuration planning and event and call logging, and a wide variety of system interfaces. It will support a wide range of commercial voice terminals (analog and digital), radios, wireless systems (such as IP-DECT), integrated voice communication terminals, assignable loudspeakers, and virtually any other analog or digital voice source. The switching system will be able to provide interoperability on a much broader scale than simply tying together radio nets. The switching infrastructure must be able to bring all the types of voice communications needed by each user together in a single voice terminal. For some, a telephone is sufficient; for others, a multi-purpose integrated terminal that can handle both radio and telephone calls is appropriate.

The switching system shall be capable of connecting to all types, brands and styles of first responder land-mobile radios in a fixed or mobile communications center. The system will be the hub that connects or networks different types of radios (even radios on different frequency bands) and at the same time allows the local users at the communications center to join multiple radio networks and communicate over telephones, intercom and landlines, all at the same time. Figure 1.3-1 shows the critical functions and interfaces of such a system that will allow first responders, and anyone else associated with a particular emergency operations or communications center, to communicate with one another while using different systems.

Example Only

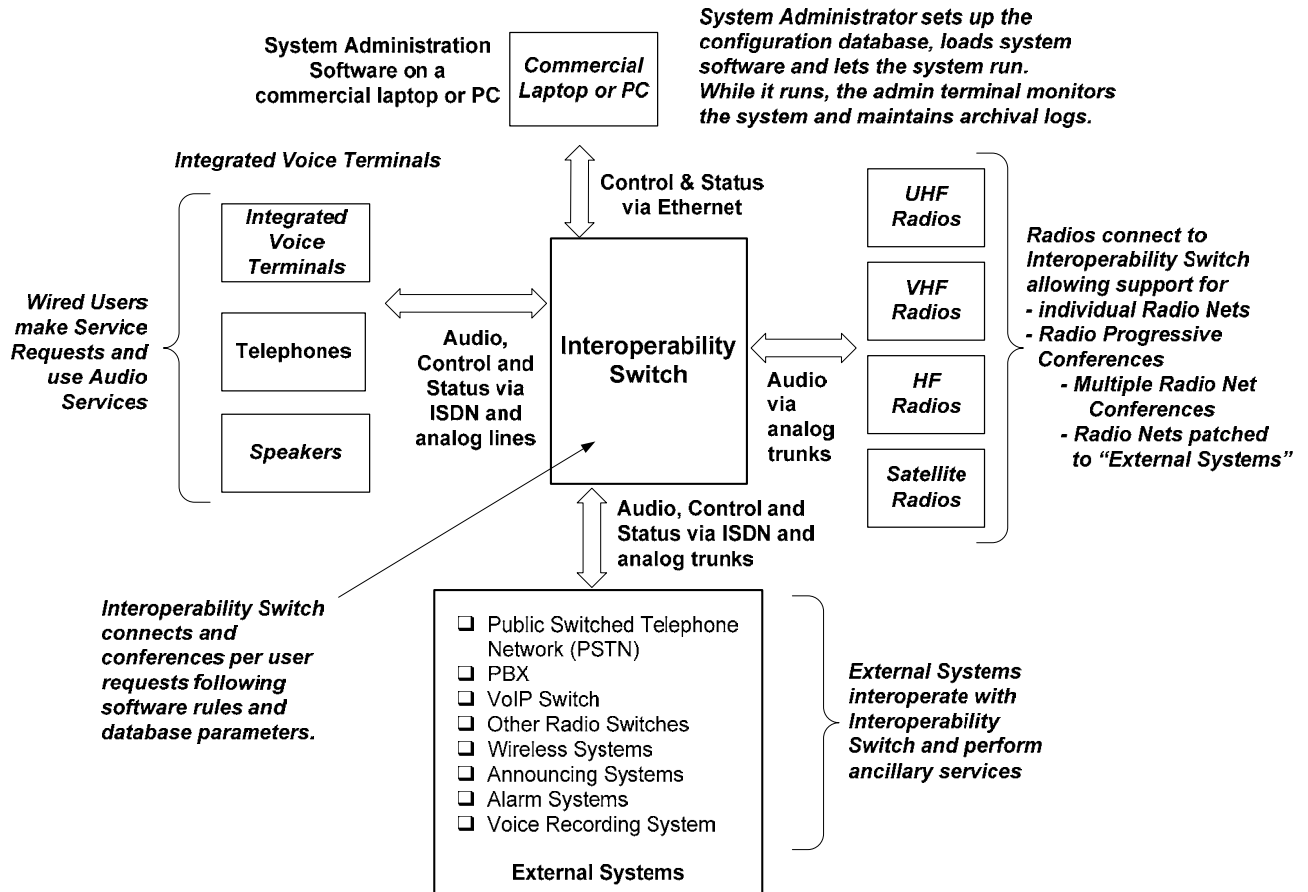


Figure 1.3-1 The critical functions and interfaces of an interoperability switching system to provide first responders interoperability with each other and the rest of the world

1.4 Supporting Analysis

This ORD is supported by analysis done by DHS S&T.

1.5 Mission the Proposed System Will Accomplish

The proposed system will be able to connect and network different and various types of radios, wireless systems, integrated voice terminals, telephones and other communications media such as PBXs, VoIP Switches and the Public Switched Telephone Network (PSTN). Integrated voice terminals are defined as devices that can handle several functions, such as radio calls, telephony, and intercom simultaneously. The proposed system will provide a means for users (first responders and those that need to talk to them) with different communications devices and media to seamlessly communicate and interoperate with one another.

Example Only

1.6 Operational and Support Concept.

1.6.1 Concept of Operations

The Interoperability Switch will enable first responders to communicate with each other and with communications center personnel using different types of radios, cell phones, telephones and other communications means. This system will integrate voice communications so that police, fire, EMT personnel of all types and from all jurisdictions will be able to easily talk to each other using whatever means of communications they have. Figure 1.6-1 shows the concept of first responders using various devices all connected to the Interoperability Switch by either wire or wireless, being able to communicate with one another. This communications can be either conferenced, networked (netted) or point to point. The proposed system will typically be located in a fixed communications or command center such as an Emergency Operations Center (EOC) but will also be sized to be able to be located in a mobile station if needed.

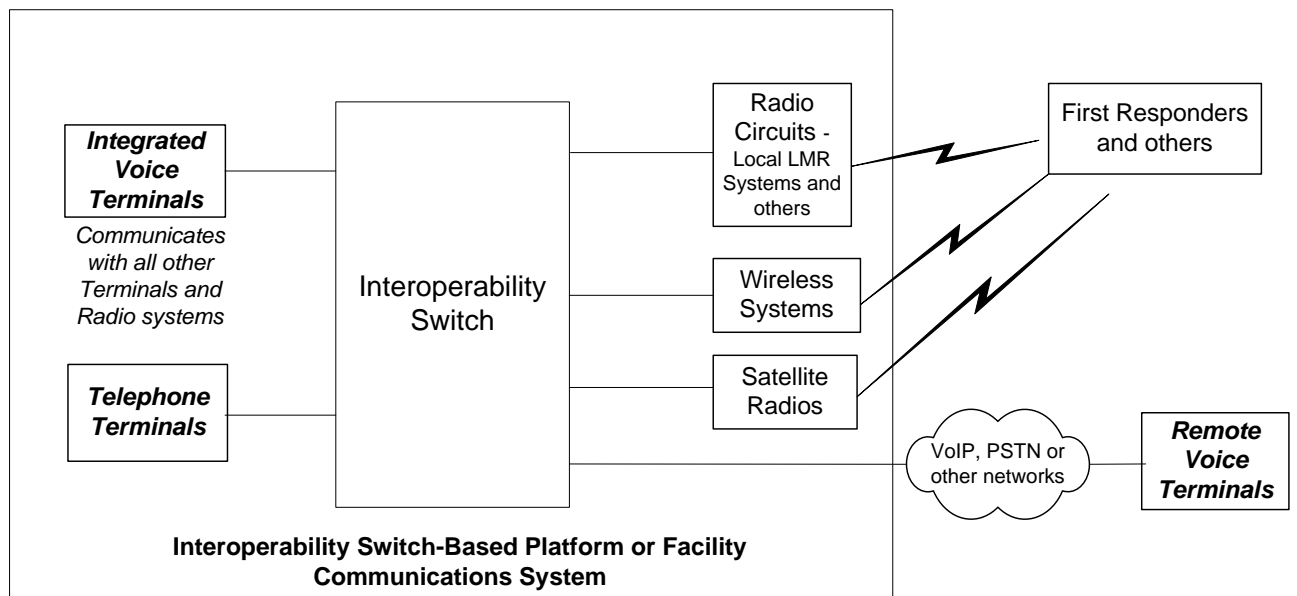


Figure 1.6-1 An Interoperability Switch-Based Facility Communications System Provides Networked Communications Between any Number of Agencies and Personnel

The proposed system will provide the following operational capabilities:

1. Enable all agencies and entities to keep their existing radios and other voice terminals, yet integrate them together in a System-of-Systems.
2. Provide the ability for communications operators to quickly and seamlessly connect or disconnect any number of First Responders with a few button pushes (no laptop needed).
3. Deliver calls without blocking.

Example Only

4. Enable managers, and other authorized users, to monitor as many communication channels or circuits as they require (or can personally handle) to achieve maximum situational awareness.
5. Interface with security and encryption, if required, to provide transmission security, and easily control who can hear which conversations.

1.6.2 Support Concept

The proposed system shall be maintainable either by the equipment provider or by personnel trained to maintain the system.

The design of the proposed system shall support easy installation by the equipment provider or other trained personnel. Some knowledge of the (fixed or mobile) emergency operation center's interfaces (such as radios, telephones and power) will be required in order to plan and do the installation.

Maintenance requirements for the system shall be minimal. Each unit shall include basic self-test mechanisms to indicate proper operation. System design shall allow for easy replacement of a defective Line Replaceable Unit (LRU) by a new unit with no need for user level repair maintenance. Defective LRUs will be returned to the manufacturer for disposition.

Spare parts will be made available by the equipment provider if not available as a commercial off the shelf (COTS) item.

Training shall be provided by the equipment provider to either a system trainer (via a train-the-trainers session) or to the users and operators at the installed site at a time convenient to the users and operators.

2 Threat

The proposed system counters any threat potentially caused or exacerbated by first responders not being able to communicate with one another. In critical situations, the inability of responders to be able to communicate with one another or with command and control authorities could cause loss of life. The interoperability provided by this system will eliminate communications breakdown or failure as a source of issues when dealing with the threat or situation.

3 Existing System Shortfalls

Existing systems that provide interoperability have the following weaknesses:

The number of devices and nets supported is inadequate to serve as a radio switch for all but the very smallest of applications.

No support is provided for integrated voice terminals. Integrated voice terminals greatly improve the mission effectiveness of users through:

Example Only

Allowing multiple circuits (radio or telephony) to be monitored simultaneously while supporting one channel in active mode.

Provision of dynamic key text and color to make communications intuitive and responsive to the specific needs of the user.

Supporting advanced interaction with remotely controllable radio terminals. Such interaction requires an intelligent switch.

Allowing a member of a conference (using an integrated voice terminal - IVT) to monitor the terminal traffic and dynamically manage the conference by adding members or dropping others out of the conference as circumstances warrant.

No support is provided for secure voice circuits. Even if secure conferences are not attempted (with multiple radios and encryption devices), these applications do require the switching system to support secure radio circuits at the same time that plain radio circuits are operating. This imposes requirements on the switching equipment that the current systems do not support.

While the Human-Machine Interface (HMI) for current systems may be adequate for the duration of a specific interoperability net, it is not acceptable for a general radio switch.

The HMI for a current system is accomplished using a laptop. Thus, the management of any conference requires someone to use a central gateway laptop for conference setup and management. This requires personnel resources that will not be necessary when each conference can be managed at the voice terminal of the leader of the conference.

The ideal managers of specific conferences are likely to be different individuals depending upon the mission served by the conference. Thus, a central laptop is much less effective for HMI than allowing integrated voice terminals to serve the conference managers as needed operationally.

4 Capabilities Required

4.1 Operational Performance Parameters

The proposed system shall provide required voice and control signal connections to support terminal-to-terminal calls, terminal to net calls, external system calls to terminals and nets, and combinations of these.

The proposed system shall provide a “non-blocking” architecture such that calls cannot be blocked because of switch limitations.

The proposed system shall support ISDN and POTS lines and trunks, and provide for non-blocking traffic flow among all switch port connections, for up to 2000 subscribers (configuration dependent).

Example Only

The proposed system shall be able to provide connections for three classes of terminal devices:

- Direct BRI S/T line connections for user terminals such as integrated voice terminals and ISDN phones;
- Direct POTS connections for POTS and Analog phones and connections;
- Network Termination (NT) adapters for converting between the BRI S/T lines and special analog interface connections such as Radios and PA systems.

The proposed system shall provide a Primary Rate Interface (PRI) trunk connection for interfacing to Private Branch Exchange (PBX) systems and Radio Communication Systems (RCS).

The proposed system shall be capable of providing redundancies to ensure protection against single-point failures.

The proposed system shall support full-duplex connections, conferencing, self-test operations, and both Plain (unencrypted) and secure modes of operation between designated terminals and systems.

The proposed system shall be created such that users from outside the EOC's area of responsibility are able to communicate with local first responders.

Digital Terminals

The proposed system shall support digital/ISDN terminal direct dial service to other dial terminals and direct dial access (when properly class marked) to nets and external systems that interface with the Interoperability Switch.

Specific Interoperability Switch features available for use by digital terminals will be limited only by the physical configuration of the terminal and the accesses or class marks available to it.

Digital/ISDN terminals shall provide an interface to an associated Interoperability Switch in accordance with industry standard digital BRI S/T characteristics and requirements, and to standard accessory connections associated with the terminal (e.g., handsets, headsets, speaker extensions).

Integrated voice terminals (IVT) are multi-functional ISDN terminals that will have Push-to-Talk capability and can therefore make radio calls in addition to making standard telephone and intercom calls.

The Interoperability Switch shall provide the power for the ISDN terminals.

Analog Terminals

The Interoperability Switch shall support analog POTS (Plain Old Telephone Service) services that operate with a standard Loop Start signaling interface, for connections to

Example Only

POTS terminals, associated FAX machines and external connections that appear to the POTS interface as a terminal.

Analog POTS terminals shall provide an interface to an associated Interoperability Switch in accordance with the requirements of industry standard EIA/TIA-464B, and to standard accessory connections for the terminal (e.g., handsets).

The Interoperability Switch shall provide the power for the analog terminals.

System Features

The proposed switching system shall provide the connection paths for the voice and control signals transmitted and received by dial terminals and net terminals. The types of call connections that shall be provided are as follows:

- Dial terminal to dial terminal calls: The calling party activates the dial terminal, receives a dial tone or indication and presses or selects (keys) the appropriate buttons on the terminal for the desired service
- Dial terminal to Net terminal calls: The calling party initiates the call and keys the terminal for the desired service. If the dialed number or single button access represents a net, the calling party will be connected to the net.
- Designated terminal to External System interface connections (such as PBXs, VoIP Switches or the PSTN)

The proposed system shall provide and support the services and features shown in Table 4.1-1. The paragraphs that follow the table define the service requirements in additional detail.

Example Only

Table 4.1-1 Matrix for Required Types of Terminal Calls Operations and Services

	CALL OPERATION OR SERVICE	TERMINAL APPLICABILITY		
		Integrated Voice Terminal	ISDN COTS Terminal	POTS or Analog Terminal
1	Call Hold	X	X	X
2	Call Transfer	X	X	X
3	Abbreviated Addressing	X	X	X
4	Progressive Conferencing	X	X	X
5	Preset Conferencing	X	X	X
6	Meet-me Net	X	X	X
7	Privacy/Auto Override	X	X	X
8	Call Forwarding	X	X	X
9	Call Waiting	X	X	X
10	Assigned Access	X	X	X
11	Access Restriction	X	X	X
12	Alternates	X	X	X
13	Plain or Secure Calls	Either	Plain	Plain
14	Call Monitor (Simultaneous)	X	-	-
15	Push To Talk	X	X	X
16	Intercom Announcing	X	-	-
17	Intercom Hotline	X	-	-
18	Emergency Reporting	X	X	X
19	Speed Calling Lists	X	X	X
20	Call Groups	X	X	X
21	Discriminating Ringing	X	X	X
22	Caller ID	-	X	
23	Activity Detection	X	-	-
24	Analog connection	X	X	X
25	PA Announcing System connection	X	X	X
26	Alarm System Connection	X	-	-
27	Radio Net access	X	X	X
28	Radio Progressive Conferencing	X	X*	X*
29	Assignable Speaker	X	-	-
30	Voice Recorder – Record	X	-	-
31	Voice Recorder – Playback	X	-	-

X Required

- Not Required

* Does not need to initiate a Radio Progressive Conference, but can be added by an Integrated Voice Terminal

System Call Processing Requirements

The following subparagraphs of this section provide a brief description of Call Processing types and services for the Interoperability Switch (shown in Table 4.1-1).

Call Types

Call Hold

Example Only

Call Hold places an engaged call on hold to allow a subscriber to consult a third party. A Call Hold capability shall be available to all Interoperability Switch subscribers who are involved in a two party call.

Call Transfer

Call Transfer provides a capability to transfer a received call to another terminal, and also permit three-party calls.

A Call Transfer capability shall be available to all Interoperability Switch subscribers who are involved in a two party call.

Call Transfer shall refer to both a "Blind Transfer" (transferring party hangs up before the transfer is answered) and an "Active Transfer" (transferring party waits for the transfer to be answered before completing the transfer). Active Transfer is also known as a transfer with introduction.

Call Transfers to PSTN Lines, Nets, Conferences, and Multi-party calls shall not be allowed.

Additionally, Call Transfers from Nets and Conferences shall not be allowed.

Subscribers currently connected to nets or in conferences shall not have the capability of call transfer.

Abbreviated Addressing (Speed Dialing)

Abbreviated Addressing / Speed Dialing permits designated dial terminals the capability to use abbreviated addresses for dialing. Entering a designated abbreviated addressing code into a terminal keyboard (typically two digits preceded by an "asterisk") shall initiate a call from the dial terminal.

Speed Dial Numbers shall be programmable at both the Local level (Speed Dialing numbers that are applied to a unique terminal) and at the Global level (Speed Dialing numbers that are applied to all terminals). Each Local Level Speed Calling List is unique to a specific terminal while the Global Level is available to all configured terminals.

The system administration terminal software (SAT) shall allow for the configuration of up to 10 Local Level Speed dial numbers per terminal, and the SAT shall allow for the configuration of up to 80 (T) Global Level Speed dial numbers.

Each integrated voice terminal shall provide the ability to program up to 20 (T)/25 (O) pre-programmable dial keys or buttons, local to the integrated voice terminal, that are to be used for speed dial. Additionally most ISDN telephone terminals provide the ability to program speed dial keys available on the terminals.

Privacy/Automatic Override

It shall be possible to assign a Privacy Override capability so that the "busy" condition of a called dial terminal, and Call Waiting if applicable, can be overridden by someone with

Example Only

the proper authority. This feature will allow selected users to exercise preemption capabilities to cut into or override terminals being used for calls with lower precedence levels. Two methods shall be available for initiating Privacy Override in designated terminals:

- a. After receiving dial tone, the subscriber depresses the # key and then keys in the called terminal directory number; or
- b. After keying the called terminal directory number and receiving busy, the subscriber depresses the # key within three seconds after receiving busy tone.

A one-second override tone shall be placed on the existing connection, such that all members of the connection hear the tone, before connecting the override call.

An Overridden terminal with the Call Waiting capability that is active on one call appearance shall have the previously active call placed on hold.

Call Forwarding

Dial Terminals designated or class marked for Call Forwarding shall be able to have all incoming calls routed to another dial terminal, through subscriber implementation.

Three types of Call Forwarding shall be available:

- a) Unconditional, where calls will be automatically rerouted;
- b) Call Forwarding Busy, which reroutes an incoming call only if the called terminal is busy;
- c) Call Forwarding No Reply, which reroutes an incoming call if there is no answer within a specified amount of time.

To implement Call Forwarding, the subscriber shall dial a configurable special service code appropriate to the type of Call Forwarding, followed by the four-digit number of the terminal to which the calls are to be forwarded.

Upon the completion of a terminal Call Forwarding to a valid terminal, the subscriber shall be notified with a confirmation tone.

To cancel Call Forwarding on a terminal, the subscriber shall dial the configurable special service code assigned for cancelling Call Forwarding.

Call Waiting

A Call Waiting capability shall be available for designated terminals that provide a visual and/or audible indication at a terminal engaged in an established call, to alert it that an incoming call is awaiting connection. A single user action at the designated terminal shall place the engaged call on hold and connect to the waiting call.

Assigned Access

It shall be possible for selected dial terminals to have an assigned access (by class of service) to any combination of the following: individual nets, Public Address systems, Radio trunks, and PSTN connections.

Example Only

Terminals assigned such access shall be able to obtain the desired connection by keying the appropriate number from the Address Numbering Plan, and terminals that attempt to complete a call to a destination to which access has not been assigned will receive an unavailable tone.

Access/Class Mark Restrictions

It shall be possible to assign Access Restriction (Class Mark) categories to all Interoperability Switch line connections, circuits and terminals for the purpose of controlling intercommunications to or between them. Class Marks (CM) provide a means for software to control user accesses and privileges (such as Call Waiting, Call Forward, and Override).

An assigned or default Class Mark shall apply for each terminal, circuit or call feature so that if the CM appears within the Class of Service (COS) restricted category for a calling party (CLG) terminal, the CLG terminal will be prevented from connecting to the called terminal, circuit or call feature. COS and CM assignments for individual terminals will be provided from the SAT (via the Switch).

Alternates

It shall be possible to designate three alternate terminals to be tested in the event that the primary terminal is busy, unavailable or idle, for a minimum of 16 (T) / 32 (O) dial terminals.

If the primary terminal is busy or unavailable when called, the alternate terminals shall be checked in order and the first idle alternate rung.

If an idle alternate is rung and not answered before the ring period timeout, the next alternate terminal shall be rung.

If the last alternate is idle and not answered a calling ISDN terminal will be placed on-hook while a POTS terminal shall receive unavailable tone.

If the dialed terminal and all alternates are busy, the calling party shall receive busy tone.

If the dialed terminal and all alternates are busy and the caller chooses to override within 3 seconds of receiving busy tone, the dialed terminal shall be overridden.

Call Groups

The Interoperability Switch shall support a telephone Call Groups' capability, for:

- a) Rotary hunting (where an incoming call is automatically rerouted to another terminal in a Call group if the first terminal is busy, unavailable, or is not answered during the ring time out period.
- b) Call pickup within a Call Group (where any terminal in a Call group can pick up a ringing call to a group member, by dialing a designated call pickup

Example Only

number), for at least 16 (T) / 32 (O) groups with a minimum of 16 (T) / 20 (O) subscriber members per group.

Plain or Secure Calls

Controls for integrated voice terminals only shall be provided to permit calls in both plain and secure modes of operation.

When a circuit transitions to secure mode all plain-only ports connected to the secure circuit shall have their audio reception blocked until the circuit transitions back to plain mode.

Transmission of plain-only ports shall still occur to the secure circuit. The Interoperability Switch will be responsible for security by configuring, connecting, tracking, and disconnecting circuits. When an incompatible security connection is attempted, the integrated voice terminal shall display a security mismatch with a security mode indication on the display.

An integrated voice terminal shall not have the capability to change the security mode of a call while its PTT is depressed or while the PTT of a terminal connected to the circuit is depressed.

When a Radio Net is switched to secure mode, all Plain-Only terminals in the net shall:

- Be disconnected from the net.
- Receive a Security Mismatch (Unavailable) tone.

If a Plain Only terminal attempts to override a terminal with at least one Call Appearance in a Secure Radio Net, the following shall occur:

- The override is unsuccessful and there is no disturbance to the net.
- The Plain Only terminal gets Unavailable tone.

Call Monitor

A Call Monitor capability shall be supported with integrated voice terminals that permit an integrated voice terminal with an existing call connection to accept or originate a new call connection without disconnecting the existing call. The first key or button pressed in accepting or originating a call will move an existing call into the monitor mode, where it is held and monitored while the user participates in the new call.

The first key pressed in accepting or originating a call shall move the existing call into the monitor mode on the ISDN Bearer 2 channel.

The integrated voice terminal shall be able to monitor calls on the Bearer 2 channel while the user participates in an active call on the Bearer 1 channel.

Discriminating Ringing

The Interoperability Switch shall support a Discriminating Ringing capability, by providing a user selected discriminating ringing for calls originating within the system,

Example Only

originating outside the system (PSTN), or from interface connections (e.g. wireless system).

Caller ID

The Interoperability Switch shall provide a calling line identification capability (Caller ID) on all ISDN terminals equipped with a user display (reference ANSI T1.625 as a guide).

Activity Detection

The Interoperability Switch shall provide an Activity Detect call feature which provides an integrated voice terminal user a visual indication of voice activity on a monitor channel.

The operator shall be provided the ability to toggle this feature on and off from the integrated voice terminal.

When enabled, only the integrated voice terminal keys or buttons that are occupied with calls in monitor mode (illuminated amber) shall blink when audio is being received on the channel associated with the key. This makes it possible for the user to be active in one call while knowing exactly where the monitor audio in the speaker is originating.

When this feature is disabled, monitor calls shall remain solid amber even when audio is being received.

Conferences and Nets

Progressive Conference

For a subscriber terminal that is properly class marked, it shall be possible to set up a full-duplex Progressive Conference capability, whereby terminals are called to join a conference.

A minimum of 15 (T) / 20 (O) Progressive Conferences in progress or in setup at one time shall be allowed, for 12 (T) / 14 (O) conferees per conference. Setup of a conference will be initiated by a conference originator, and add-on permitted by any conference member with the proper permissions (the members Class of Service is not restricted from performing a Progressive Conference)

Preset Conference (and Command Net Call)

A Preset Conference is a call between a set number of previously designated terminals. At least 15 (T) / 20 (O) Preset Conferences of 12 (T) / 15 terminals each shall be supported.

Dialing the Preset Conference directory number from one of the designated terminals shall ring the other designated terminals.

Example Only

Each designated terminal (of a predefined conference member) shall be added to the Preset Conference if it goes off-hook before the end of the ring period, which shall be programmable up to a maximum of 45 seconds.

Command Net Call is similar to a Preset Conference except that it does not allow automatic Privacy Override.

At least 15 (T) / 20 Command Nets of 12 (T) / 15 terminals each shall be supported.

Meet-Me (Voice) Net

A Meet-me net capability shall be provided, whereby participating terminals are not pre-assigned to the net but will enter it with a single action depression (on a integrated voice terminal) or defined programmable directory number with no additional user action.

Dialing a defined Meet-Me number shall immediately connect a terminal to the Meet-Me net.

Every terminal that dials the meet-me net directory number shall be connected into the net with the ability to disconnect and reconnect without disturbing other net participants.

Each net shall support a capacity of at least 12 (T) / 15 (O) participants.
The minimum simultaneous net capacity shall be at least 15 (T) / 20 (O) nets.

Emergency Nets/Calls

An Emergency Reporting Net capability of up to 3 (T) / 4 (O) nets shall be provided to receive emergency calls from any dial terminal, with one terminal assigned to each emergency net for handling incoming emergency calls on that net, and identified as the Responsible Dial Terminal (RDT).

When a called RDT goes off-hook, it will be connected to its emergency net, and any subsequent calls to the emergency number or associated net number will be connected to the emergency net and be able to converse with other net members.

Emergency reporting shall be possible for each of five 'readiness' conditions, and under each condition of readiness a particular RDT may be designated as responsible for handling emergency calls on one or more Emergency Reporting Nets.

An Emergency Reporting Net shall be identified by up to two emergency telephone numbers (i.e., 2211 and 911) in addition to a net number.

The following call/connection procedures shall be implemented:

Any terminal calling the Emergency number and RDT is not-busy, shall receive a ring-back tone until the RDT operator goes off-hook (or integrated voice terminal equivalent), at which time both parties shall be connected to the corresponding emergency net.

Example Only

Subsequent callers calling the emergency number or the emergency net number shall be connected to the corresponding emergency net and be able to converse with other net members.

If the call to the RDT cannot be completed due to equipment problems or settings, the operator of the calling terminal shall receive an unavailable tone.

If an emergency call is made to the RDT while it is busy on a call to other than its assigned emergency net, all parties on the existing call shall hear a one second emergency tone added to their conversation in progress, and then will be placed on hold while the RDT is automatically connected to the Emergency Net.

The RDT shall be overridden by an emergency net call even if the RDT is currently on a non-overridable call on its non-emergency number. The RDT operator may then retrieve any of the parties on hold.

The RDT shall continue to be connected to the corresponding emergency reporting net even if the calling terminal should go on-hook.

The RDT's connection to the net shall be broken only when the RDT goes on hook or deactivates.

At least 3 (T) / 4 (O) Emergency Nets of 12 (T) / 15 (O) terminal participants each shall be supported.

Address Numbering Plan

An Address Numbering Plan capability will be provided that permits each terminal, net, interface channel or service code to be identified by a discrete four-digit number. The address numbers are used in switch service operations for identification purposes and by the subscriber for service requests.

A numbering plan will typically be divided into two parts: a fixed or reserved set of numbers, and a directory set of numbers.

PTT and Intercom Push-to-Talk (PTT)

A Push-to-Talk (PTT) capability shall be supported for integrated voice terminal connections and radio mode calls.

A Voice Operated Transmission (VOX) PTT shall be implemented for POTS and BRI/ST Interface Boards.

Intercom Announce

Intercom capability shall be supported for integrated voice terminals, as a dedicated non-blocking service feature that establishes a talk-back connection between designated terminal users. In Intercom Announce the calling integrated voice terminal alerts the

Example Only

called subscriber with an audible tone. An integrated voice terminal permits a called party to hear the calling party even if the called integrated voice terminal is busy, and a single action at the called integrated voice terminal establishes a connection in the reverse direction to permit the called party to talk to the calling party.

The initiator of the IC call shall have an immediate half-duplex connection to the monitor channel of the other integrated voice terminals in the IC group. The other integrated voice terminals will hear the originator without any action on their part.

An integrated voice terminal key in the IC ringing state shall beep and continue flashing until answered or the caller disconnects.

IC ringing shall not time out. If not answered, the call shall remain in the ringing state until the calling party disconnects.

Pressing the IC key or button on a called integrated voice terminal shall establish full-duplex audio between the terminal, the initiating terminal and any other integrated voice terminals that have answered.

If other members disconnect, leaving one remaining member, the call shall remain active.

An integrated voice terminal shall have the ability to leave the IC call and re-enter the call by depressing the IC key.

An integrated voice terminal operator who presses the IC key to return to an active IC call shall be immediately connected.

At least 15 (T) / 20 (O) total Intercom circuits of 12 (T) / 15 (O) participants each shall be supported.

Auto Answer

Applicable to ISDN terminals with Auto Answer capability, an incoming ring signal shall automatically activate the terminal if its Mode switch is set to "Auto-Answer," allowing the terminal to ring once and the calling party to start speaking.

The integrated voice terminal shall include a locally enabled Auto-Answer feature, whereby the terminal automatically answers incoming telephone and Intercom Announce calls without any user action required.

External Connection Calls

A capability shall be provided to permit dial terminals that are appropriately class marked to dial a connection to an interfacing external system, as described in the paragraphs that follow (such as to a Public Address (PA) system, Radio net, or access to a PSTN trunk using a dialed access code).

Public Address (PA) and Alarm System Connection

Example Only

A capability shall be provided for connecting to a PA or Alarm system from designated voice terminals, by keying (dialing, with PTT) a designated PA or Alarm system termination number.

8 (T) / 12 (O) total PA or Alarm System Nets of 12 (T) / 15 (O) participants at least each shall be supported.

Radio Net Connection

The Interoperability Switch shall provide a Radio, Analog NT interface capability (application dependent) that permits a secure mode connection via the Switch, from an integrated voice terminal to a site-provided voice radio device. This NT circuit shall present an interface that consists of BRI S/T-to-analog converter circuits and discrete control lines, for an appropriate radio channel connection that has a standardized interface.

15 (T) / 20 (O) total Radio Nets of 12 (T) / 15 (O) participants at least each shall be supported.

PSTN Connection

A capability shall be provided for accessing PSTN trunks from dial terminals and integrated voice terminals that are appropriately class marked, by dialing an access code. The PSTN side shall provide the required dial tone.

Traffic Handling Capabilities

Traffic handling capabilities for the Interoperability Switch will have minimum (threshold) baseline characteristics as specified in the paragraphs that follow:

- a) Traffic Load and Distribution - During the busiest hour the Interoperability Switch shall be capable of handling: a) 0.004 terminal-to-terminal calls originated per dial terminal per second (equates to one new call per terminal every 4 minutes), with an average holding time of 30 seconds; and b) 0.002 line-to-net calls originated per dial terminal per second (approximately one new call every 8 minutes), with an average holding time of two minutes. It is assumed that the percentage of these calls completed within the originating node is equal to 100% divided by the number of nodes, and that the traffic load imbalance between multiple nodes does not exceed 1.5 to 1.
- b) Call Busy Factor Adjustment - A call busy factor of 25 percent is assumed, to reflect the number of dial terminals unable to make or receive calls because the line is occupied with a previously established call.
- c) Call Initiation Delay - The busy hour call initiation delay measured from call initiation to receipt of dial tone shall be less than 3.0 seconds.
- d) Call Completion Delay - The busy hour call completion delay measured from the last digit dialed to ring forward shall be less than 0.5 second for calls at one node, or less than 2.5 seconds for calls between nodes.
- e) Blocking - An Interoperability Switch shall provide a traffic handling capability of less than one call in one thousand lost or blocked (equates to a call

Example Only

not going through) as a result of: an error in the controller, or a false trunk, switch or station signal.

f) Misrouting - For security requirements, the probability of call misrouting (call sent to another terminal) due to an Interoperability Switch error shall be less than one in 10^6 .

Radio Progressive Conference

Scope

The Radio Progressive Conference (RPC) feature provides a means to establish a true two-way conference call between multiple radios, integrated voice terminals, and other terminals.

Operational Concept

This feature enables an integrated voice terminal user to join two or more Radio Nets together to form one large net. As an example, a VHF link from one land-based agency to a helicopter could be joined to a UHF link from the same agency back to other agencies in the area. The extended network would be half-duplex, but participants on the VHF and UHF links can all hear transmissions and transmit on either link. This represents a concatenation of two nets.

In addition, the feature can be used to bring another terminal into a Radio net. For example, the originator may be participating in a Law Enforcement UHF net and decide that someone on another IVT needs to join the conversation. That operator can call the other IVT and then conference that IVT into the Radio Progressive Conference.

The term progressive in the title implies that additional members (Radio Nets or terminals) may be progressively added (or dropped) one at a time. These conferences can also be referred to as ad hoc conferences.

RPC Requirements

The proposed switching system shall provide Radio Progressive Conferencing with 15 (T) / 20 (O) Preset Conferences.

Each preset conference shall support at least 12 (T) / 15 (O) terminals.

The SAT shall have the capability to configure the Radio Progressive Conference feature for any integrated voice terminal.

If a Radio Net or a Terminal is already involved in a Radio Progressive Conference, attempting to conference that Radio Net or Terminal shall result in an unavailable tone at the attempting integrated voice terminal.

Assignable Speaker/Voice Recorder (AS/VR)

The Assignable Speaker/Voice Recorder (AS/VR) feature of the proposed system shall enable a user to assign speakers or a voice recorder to an Interoperability Switch Radio Net, Public Address Net or Voice Net for monitoring and recording purposes.

Example Only

The proposed system shall be able to interface with a public address announcing system using industry standard interfaces.

The proposed system shall be able to interface with an alarm system using industry standard interfaces.

The proposed system shall be able to interface to a voice recording device using industry standard interfaces, for the purposes of recording any of the circuits or calls that are routed through the switch.

The voice recorder's record port shall be able to be connected to a net (via the Interoperability Switch) such that all voice transmission on the net is recorded.

The voice recorder's playback port shall be able to be connected to a net (via the Interoperability Switch) such that multiple integrated voice terminals and dial terminals can listen to the playback audio.

The connection of the speaker and/or the voice recorder to a net (via the Interoperability Switch) shall be configurable from the SAT (offline or online) or from the integrated voice terminal.

4.2 Key Performance Parameters (KPPs)

4.2.1 Connectivity

The Interoperability Switching System shall provide at least:

Connectivity to radios 16 (T) / 32 (O)

Connectivity to integrated voice terminals - 24 (T) / 48 (O)

Connectivity to telephones 16 (T) / 32 (O)

Connectivity to wireless systems - 4 (T) / 8 (O)

Connectivity to public switched telephone networks - 1 (T) / 2 (O)

Connectivity to recording systems - 2 (T) / 3 (O)

4.3 System Performance.

4.3.1 Mission Scenarios

The Interoperability Switching System will typically be located at fixed area or mobile communications centers that handle emergency events such as an Emergency Operation Center (EOC). Systems will be installed and can be up and in operation at all times in

Example Only

order to minimize the time needed to establish communications in the event of an emergency.

4.3.2 System Performance Parameters

The Interoperability Switching System shall provide at least:

*Connectivity to radios 16 (T) / 32 (O)

*Connectivity to integrated voice terminals - 24 (T) / 48 (O)

*Connectivity to telephones 16 (T) / 32 (O)

*Connectivity to wireless systems - 4 (T) / 8 (O)

Connectivity to other switches via a PRI interface - One (T) / Two (O)

*Connectivity to public switched telephone networks - One (T) / Two (O)

Connectivity to public address systems - 2 (T) / 4 (O)

Connectivity to other Interoperability Switches via a trunk - One (T) / Two (O)

*Connectivity to recording systems - 2 (T) / 3 (O)

Connectivity to Voice over IP (VoIP) systems - One (T) / Two (O)

4.3.3 Interoperability

The Interoperability Switch will be able to interface to all radios, wireless systems, integrated voice terminals, telephones, PBXs, VoIP Switches, PA systems, recording devices and other communications media that utilize industry standard interfaces.

4.3.4 Human Interface Requirements

An Integrated Voice Terminal (IVT) will be the primary and most functional Human Machine Interface (HMI) connected to the Interoperability Switch for connecting and establishing radio/wireless and telephone calls, circuits, conferences and nets.

Analog and Digital Telephones (also known as dial terminals) will be additional HMI devices connected to the Interoperability Switch for the purpose of making and receiving calls and connecting to conferences and nets.

A system administration terminal (SAT) will act as the HMI for system configuration data entry, system configuration reports, system status reports and failure interrogation.

The SAT can be either continuously connected to the Interoperability Switch for permanent ongoing system status reporting, or be capable of being placed in offline mode

Example Only

during user absence or for configuration database updating (for a later database transfer to the Switch).

When the SAT is not online, Switch status and failure events shall be stored in the Switch for batch transfer to the SAT when it is returned to online status.

A SAT connection shall be able to interface to a local or networked printer, if part of the configuration, for hardcopy printouts of system status.

The SAT can be any PC which is operable from 115 VAC, is available with back-up battery option, provides printer and Ethernet interface connections, is capable of running Interoperability Switch SAT software under Microsoft Windows®.

The SAT shall provide for Interoperability Switch setup and management and for initiating Switch Built-in-Test (BIT) operations.

The SAT shall provide a status screen displaying the latest status of the Interoperability Switch.

The SAT status screen shall contain the Interoperability Switch Call and Fault Logs.

The SAT shall provide the user a capability to manage the system tests and view the status of the tests.

Accepted industry standards shall be applied as guidance for human engineering design criteria in the design of the proposed system, to achieve safe, reliable and effective performance by operator, supervisor and maintenance personnel, and to minimize personnel skill requirements and training time.

4.3.5 Logistics and Readiness

The proposed system is required to be operational for several days of continuous operation without interruption. No user level maintenance or spare part replacement is required. Spare PWAs should be available in case replacement is required.

Mean Time Between Failures (MTBF) shall be 1,500 hours (T) 1,800 hours (O)

System Availability (A_i) requirement shall be 0.999995 (T), 0.999997 (O) based on the following formula:

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

Example Only

4.3.6 Other System Characteristics

Design drivers are the interfaces and the ability of the proposed Interoperability Switch to interface to all types of radios, wireless systems, telephones, and other communications media.

Cost drivers are the interface cards for the many and varied systems to be connected to the proposed system.

Risk drivers are the ability of the Interoperability Switch to interface with many and varied different systems using readily available off the shelf interface boards without the need of designing or building new boards

5 System Support

5.1 Maintenance

The proposed system shall be designed for unattended operation. Routine, scheduled maintenance will be performed on-line, except for specified infrequent cleaning operations.

Scheduled maintenance checks shall not be required more than once every 24 hours. Scheduled maintenance may include, but not be limited to: air filter cleaning and replacement; battery cleanliness and battery voltage level checks; daily semi-automatic system tests from the SAT; lamp and meter checks; and general cleanliness requirements.

The total 24-hour normal maintenance burden for an operating system, scheduled and unscheduled, shall not average more than two man-hours (T) / one man-hour (O).

Example Only

5.2 Supply

User Manuals will be provided to the operators and maintenance technicians by the equipment provider (vendor) and will include operator procedures, diagnostic testing/SAT use, and replacement procedures.

No special tools or diagnostic equipment will be required for equipment replacement.

5.3 Support Equipment

Standard support equipment for the Interoperability Switch is the system administration terminal (SAT) described in paragraph 4.3.4 HMI which will handle system diagnostic testing. No special test equipment will be required to maintain or operate the unit. The vendor will provide software upgrades as needed/required and will provide software development services to the buyer for new features as requested.

5.4 Training

Training will be provided by the equipment provider to a system trainer (via a train-the-trainers session) and to the users and operators at the installed site at a time convenient to the users and operators. The training curriculum will be designed to ensure users understand and are fully capable of operating and using all features of the system.

Knowledgeable staff members of the equipment provider will also be made available by phone (via a Help Desk type arrangement) should a user or operator need assistance with any part of the proposed system.

5.5 Transportation and Facilities

It is anticipated that this system will most often be used in a fixed station. If the proposed system is to be mobile or used in the field, it will be transportable via truck or van and will be able to be lifted by two or fewer personnel. Sufficient 115V power and cables will be needed to connect the Interoperability Switch to the radios and other equipment necessary to provide connectivity and interoperability commensurate with the event. Any training needed in the field can be provided as on the job training with no special facilities needed.

6 Force Structure

One Interoperability Switch system will typically be required at each Emergency Operating Center (EOC) or similar type communications center. The proposed system will be modular and scale-able (or sizeable) to have enough capacity and interface boards necessary to interface all of the radios, integrated voice terminals, telephones and other communications devices needed by the center personnel to conduct their mission.

Additional systems can be supplied to mobile platforms (vans or trucks) if an EOC or other shore based center is not within communications range of the event.

The high reliability of the system (para. 4.3.5) dictates only a minimum amount of spares needed for interface boards, power supplies and communications devices

7 Schedule

Demonstration of an initial operational capability is required within 3 months (T) / 1 month (O) after executed SECURE Agreement. For the purpose of this effort, initial operational capability is defined as installation and field demonstration of one fully operational Interoperability Switch system to include one SAT and at least two radios, two integrated voice terminals, two telephones, and one other wireless device (such as a cell phone.)

A fully operational system will be required within 9 months (T) / 6 months (O). A fully operational system includes the Interoperability Switch with interface boards, system administration terminal (SAT), and all necessary integrated voice terminals supplied by the proposed system vendor. Radios and other communications devices (telephones, wireless systems) to interface with the Interoperability Switch are typically separate from the Interoperability Switch system and may have different lead times if they are not already available at the site.

8 System Affordability

An Individual unit price cost for such an Interoperable Communications Switch will cost less than \$200K (T) / \$150K (O).

9 Appendixes

List of Acronyms

CM – Class Mark

COS – Class of Service

COTS – Commercial off the Shelf Equipment

EOC – Emergency Operations Center

ISDN – Integrated Services Digital Network

KPP – Key Performance Parameter

MTBF – Mean Time Between Failures

POTS – Plain Old Telephone System

PSTN – Public Switched Telephone Network

RDT – Responsible Dial Terminal

SAT – System Administration Terminal

IVT – Integrated Voice Terminal

Appendix B: Making it Easier to Work with DHS (Article)

Making it Easier to Work with DHS: The Critical Role of Detailed Operational Requirements

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

In today's dynamic homeland security environment, delivering cost-effective products and services that meet well thought-out detailed requirements is a critical objective for the U.S. Department of Homeland Security (DHS). DHS is composed of many organizational elements with an overriding goal: to enable, support and expedite the mission-critical objectives of DHS' seven operating components – Transportation Security Administration (TSA); U.S. Customs and Border Protection (CBP); U.S. Secret Service, (USSS); U.S. Citizenship and Immigration Service (USCIS); U.S. Immigration and Customs Enforcement (ICE); Federal Emergency Management Agency (FEMA); and the U.S. Coast Guard (USCG). These seven operating components work closely with, support and are supported by a large network of first responders at the state, local and tribal levels. DHS must coordinate, drive and prioritize the detailed needs of this diverse group of operating components and supporting elements, whose missions address a wide variety of terrorist and natural threats to our homeland, in order to maximize the effective use of DHS's resources. Ever changing threat dynamics often require new, innovative-technology based solutions in order to prevent or mitigate the potential effects of current and future dangers. The DHS Science and Technology Directorate (DHS S&T) works diligently to understand, document and offer solutions to current and anticipated threats faced by our "customers" (DHS operating components and field agents) and our "customers' customers" (first responders and the eighteen infrastructure industrial sectors such as banking, chemicals and communications, etc.).

Capstone IPTs and Capability Gaps

DHS-S&T, through the Capstone Integrated Product Team (IPT) process¹, ensures that quality, efficacious products are developed in close alignment with customer needs. The Capstone IPT process is the framework that determines that developed capabilities meet operational needs, analyzes gaps in strategic needs and capabilities, determines operational requirements, and develops programs and projects to close capability gaps and expand mission competencies. This process is a DHS customer-led forum through which the identification of functional capability gaps and the prioritization of these gaps

¹ Kikla, Richard V. and Cellucci, Thomas A. "Capstone IPTs: Even in Government the Customer Comes First," April, 2008.

across the Department are formalized. The IPTs oversee the research and development efforts of DHS-S&T and enable the proper allocation of resources to the highest priority needs established by the DHS operating components and first responders.

Capstone IPTs bring together S&T division heads, acquisition partners and end-users (Operating Components, field agents and supporting First Responders – customers of DHS) involved in the Research, Development, Testing and Evaluation (RDT&E) and acquisition activities. Working together, the IPT identifies, evaluates and prioritizes the necessary requirements to complete missions successfully. IPTs also assess the technological and system readiness of products that will ultimately be deployed into the field. Figure 1 shows the organization of a Capstone IPT. The formation of the IPT at an early stage allows key stakeholders to identify and address critical capability gaps. Each Capstone IPT has a DHS operating component chair or co-chairs. The chair/co-chair, representing the end-users of the delivered Enabling Homeland Capabilities (EHCs), or suite of technologies needed to close a capability gap, engage throughout the process to identify, define and prioritize current and future requirements and ensure that planned technology and/or product transitions and acquisition programs, commercialization efforts and standards development are optimally suited to their operational requirements. Operating components, field agents, first responders and other non-captive end-users with an interest in the core functional areas of an IPT are welcome to participate and contribute throughout the Capstone IPT process.

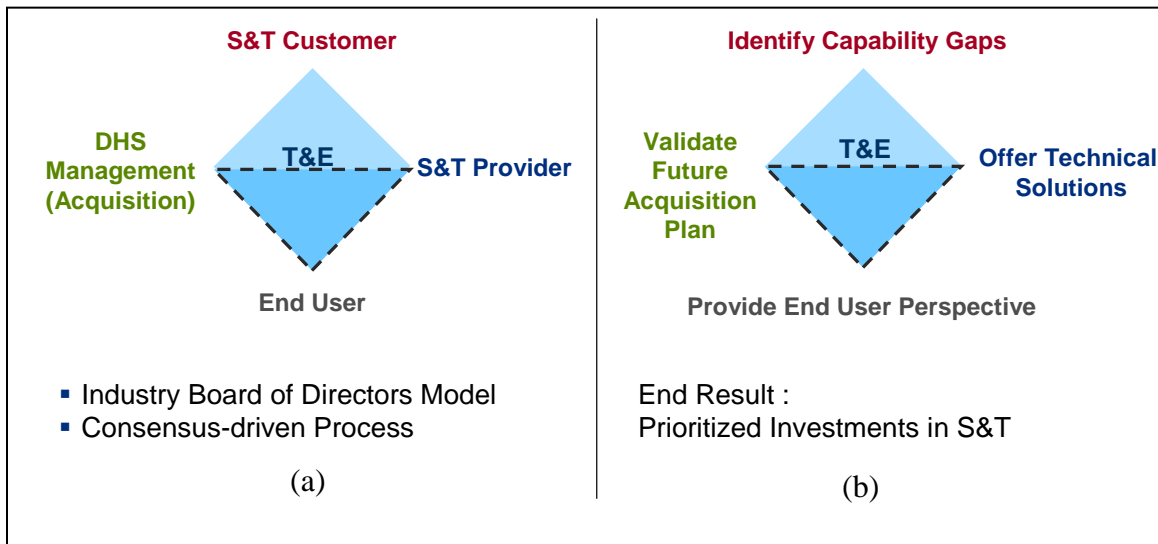


Figure 1 (a) This diagram shows the structure of the Capstone IPT model with (b) the models' output functions carried out by each IPT member.

The Capstone IPTs are structured to focus on functional, department level requirements, articulated as capability gaps, and deal with programmatic and technology issues within the six S&T divisions. Capstone IPTs have been created across twelve major Homeland Security core functional areas: Information Sharing/Management, Cyber Security, People Screening, Border Security, Chemical/Biological Defense,

Maritime Security, Counter-Improvised Explosive Devices, Transportation Security, Incident Management, Interoperability, Cargo Security and Infrastructure Protection. Each Capstone IPT is chaired by senior leadership from a DHS operating component with needs that correspond to a specific functional area. All DHS operating components with an interest in a particular Capstone IPT are invited to send a representative to participate as an IPT member. See Figure 2.

DHS Requirements/Capability Capstone IPTs

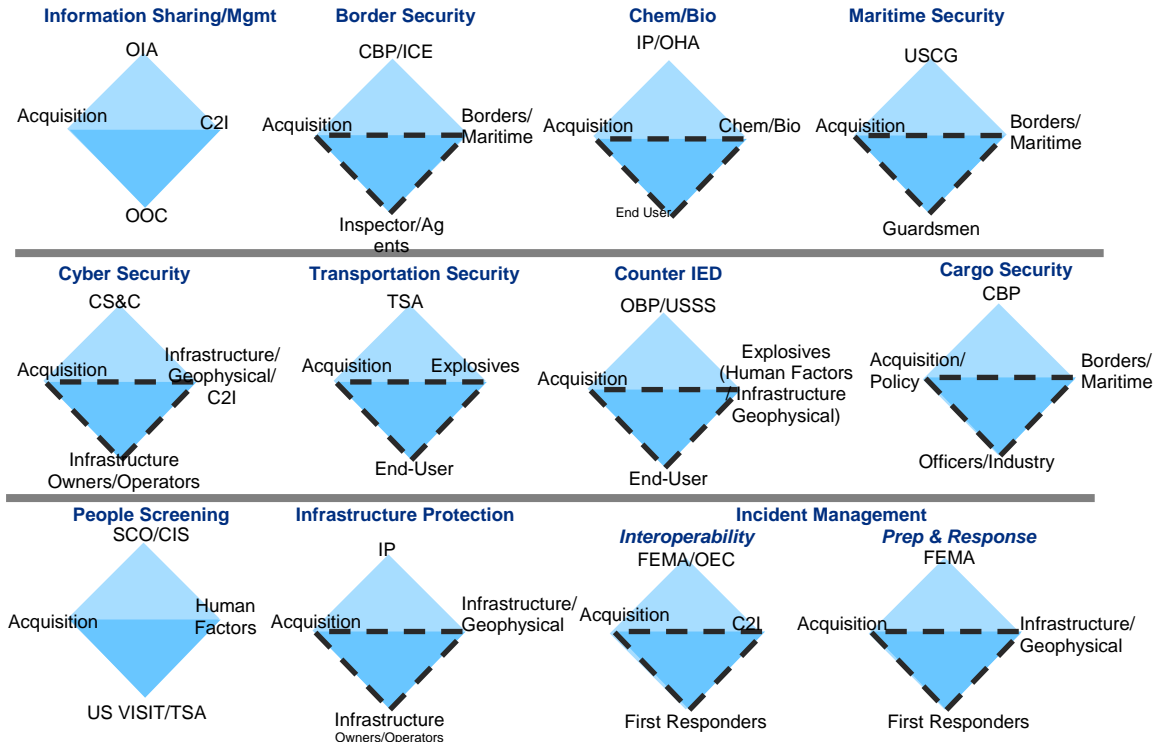


Figure 2. This diagram shows the twelve Capstone IPTs, the DHS operating component, DHS end-user(s), the S&T Division technical provider, and, when applicable, the Acquisition conducted by DHS management.

Technology development is aligned functionally, rather than by operating component “stove pipes,” to allow technologies to be used in support of multiple operating components within DHS. This broad focus aids in reducing the duplication of efforts among various operating components of DHS. In order to achieve greater insight into the facets that comprise each Capstone IPT, Project-IPTs are created to manage specific project areas within a functional area. For example, Border Officer Tools and Safety, and Container Security are Project-IPTs for the Border Security and Cargo Security Capstone IPTs, respectively. Project-IPTs consist of several subject matter experts who are responsible for clarifying the capability gaps derived from the Capstone IPTs and for developing detailed operational requirements with the operating components for the systems that will comprise the EHCs. The Project-IPTs work closely with DHS customers, through an Operational Requirements Document (ORD), to define clearly the specific requirements that must be met in order for a technological solution to address a given problem. Integration of these products into systems forms the EHCs for use by the

customers. All DHS agencies are responsible for integrating and fielding the technology deliverables into operational systems scheduled for delivery to their operating component.

Beyond Capability Gaps...

Capstone IPTs generate several outputs that guide the development and fielding of products, services and systems for the operating components. The primary role of the IPTs is to conduct strategic needs analysis to determine and prioritize the capability gaps that exist within a particular functional area. Capability gaps are broad descriptions of department level identified mission needs that are not met given current products and/or standards. Capability gaps catalog opportunities for enhanced mission effectiveness or address deficiencies in national capability.

The Capstone IPT process enables our divisions within DHS-S&T to interact regularly with their customer(s) to determine capability gaps. These capability gaps, in many ways, are just the beginning. From a product development standpoint, a capability gap is one of the initial steps in the requirements hierarchy scheme. Additional detailed requirements must be developed to enable the development of a technology or product. In our outreach efforts with the Private Sector, DHS-S&T realizes that we must work with our customers to produce a detailed set of requirements in order to communicate with other operating components and frequently to the private sector, which has the ability to develop products aligned to stated requirements.

Commercialization Model Drives the Need for Detailed Requirements

The U.S. Department of Homeland Security is forging a new paradigm with far-reaching positive consequences for DHS' customers, private sector partners, and U.S. taxpayers through the rapid, cost-effective and efficient development and deployment of products and services to protect the Homeland of the United States. As a recently formed U.S. Federal Government Department (March 6, 2003), DHS is "creating a culture" where public-private sector partnerships, beneficial to both sectors and taxpayers alike, expedite the development of products and services to protect the nation. Recently announced commercialization initiatives like the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program are truly groundbreaking and innovative approaches to foster a mutually beneficial relationship between the public and private sectors by creating an open and freely competitive program accessible by small, medium and large firms to provide potential solutions to DHS requirements. These efforts are a natural extension of the Capstone IPT process.

DHS possesses an "Acquisition Mindset," as do so many government agencies. While the Acquisition model has been, and continues to be, utilized effectively in developing custom, one-off products such as aircraft carriers, it is not particularly germane to a majority of the needs at DHS as well as the first responders (a DHS ancillary market). The timely design, development and deployment of lower priced, widely distributed products for both DHS operating components and the first responder communities represents a critical step in protecting our nation. Recognizing this fact, the Department recently started implementing a "Commercialization Mindset" in order to leverage the

vast capabilities and resources of the private sector through an innovative “win-win” private-public partnership called the SECURE Program stressing the need for detailed requirements.

Why is there a need for a commercialization process? DHS requirements, in most instances, are characterized by the need for widely distributed COTS (Commercial-Off-The-Shelf) products. Oftentimes, the need is for thousands, if not millions, of products for DHS’ seven operating components and the fragmented, yet substantial first responder market. Figure 3 shows the major differences between a “pure” Acquisition vice a “pure” commercialization processes, along with the recently developed and implemented DHS “hybrid” commercialization process. In this new “hybrid” process, both the private and public sectors share various roles and responsibilities in the cost-effective and efficient development of products and services for DHS.

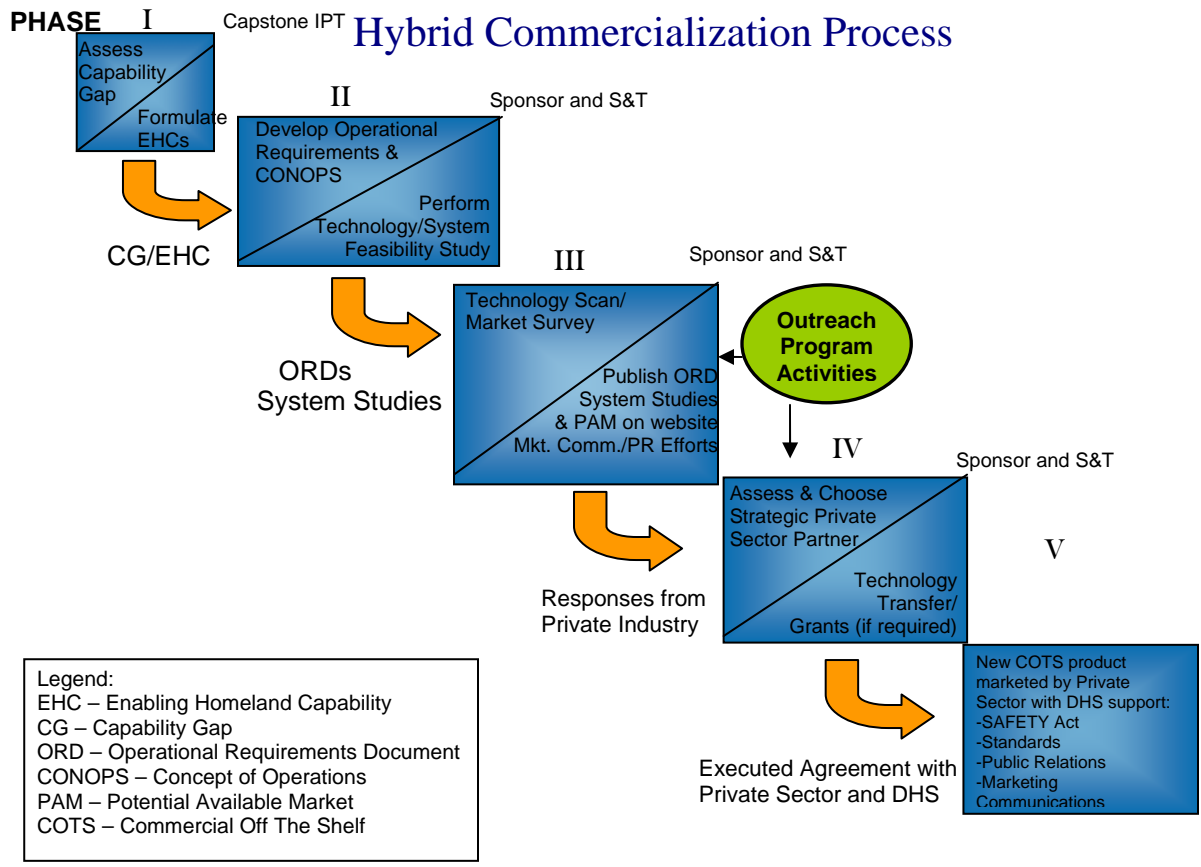
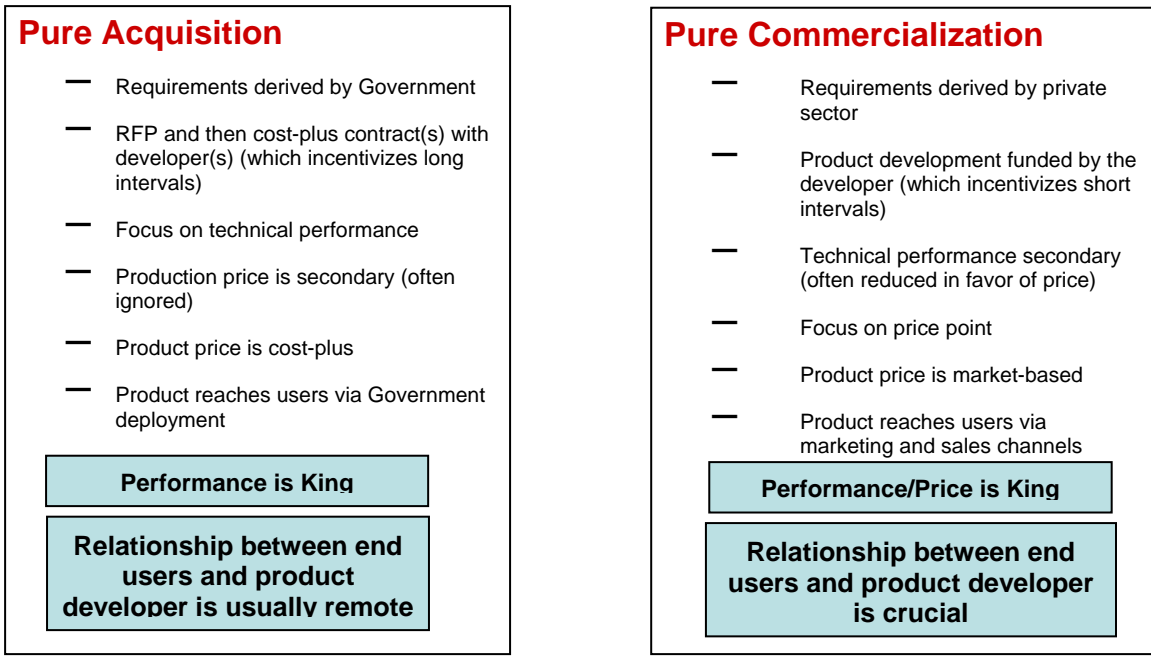


Figure 3: Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system development and the resultant hybrid model implemented by DHS.

Figure 4 delineates the overall description of DHS’s new commercialization model and its first private sector outreach program called the SECURE Program to develop products and services in a private-public “win-win” partnership described in detail at www.dhs.gov/xres/programs/gc_1211996620526.shtm. The SECURE Program is based on the simple premise that the private sector is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and resources to such activities, if and when an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two pieces of critical information from DHS: 1. detailed operational requirement(s), and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in the program.

A New Model for Commercialization...

- Develop Operational Requirements Documents (ORDs)
- Assess addressable market(s)
- Publish ORD and market assessment on public DHS web portal, solicit interest from potential partners in a way that is open to small, medium and large businesses
- Execute no-cost (CRADA-like) agreement with multiple private sector entities and transfer technology and/or IP(if necessary)
- Develop supporting grants and standards as necessary
- Assess T&E findings after product is developed to assure DHS and ancillary markets that product meet its published specifications
- New Commercial-Off-The-Shelf (COTS) product marketed by private sector with DHS support

SECURE Program



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized third-party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal to provide confidence to potential customers at DHS and its ancillary markets that product(s) meet or exceed their published specifications in reference to their actual performance.

Figure 4: Step-by-step guide to the commercialization process developed and adopted by DHS with a brief summary of the popular SECURE Program.

To augment the commercialization process, DHS has undertaken the task of developing an easy-to-use comprehensive guide to assist in developing operational requirements. This guide now enables DHS personnel to articulate, in detail, a given system’s

requirements and communicate those needs to both internal and external audiences. This effort addresses a long-standing need for DHS to fully articulate its requirements. Figure 5 clearly shows how an ORD takes a capability gap to “much higher resolution,” a necessary required if the private sector is to aid DHS in its goal of expediting the development and deployment of cost-effective and efficient widely distributed products.

Requirements Hierarchy (TSA example)

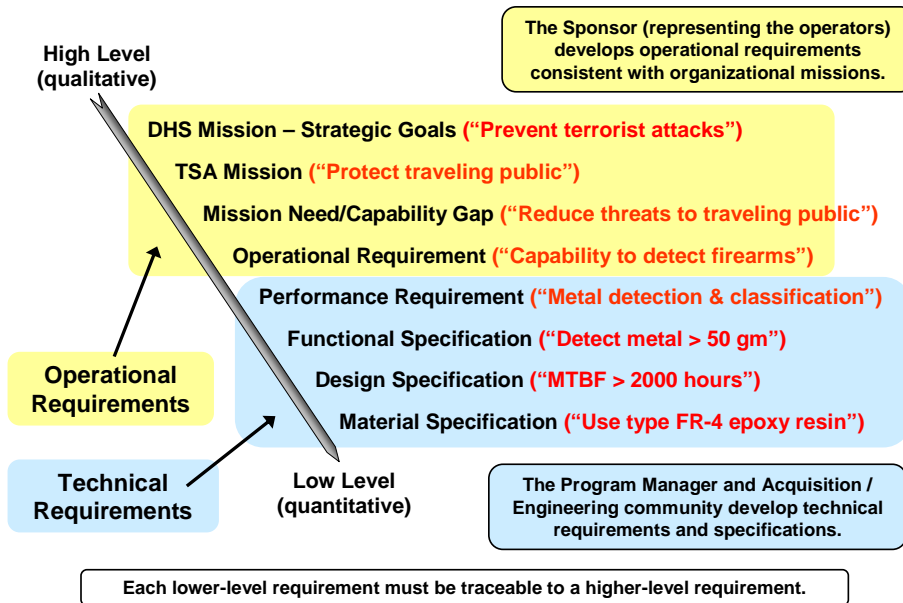


Figure 5. This requirements hierarchy shows the evolution of requirements from a high-level macro set of operational requirements to a low-level micro set of technical requirements. Note that each lower level requirement stems directly from its higher requirement so that all requirements are traceable to the overall DHS Mission.

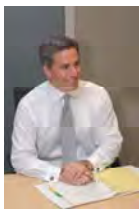
Early response from groups within DHS, the private sector, and first responders about this guide and programs like SECURE has been very favorable². The Department plans to regularly update its website with Operational Requirements Documents (ORDs) to continually expand this innovative private-public partnership. In addition, as evidenced in Figure 6, the taxpayers, private sector and public sector view programs like this as “win-win-win.”

² Margetta, R. “S&T Official Working to Move Product Development Out of DHS, Into Private Sector,” Congressional Quarterly Homeland Security. June 27, 2008.

Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Figure 6: The SECURE Program is viewed positively by DHS stakeholders. The success of the program lies in the fact that all participants receive significant benefits.

In conclusion, DHS’ newly created and implemented commercialization process offers long-awaited benefits to the rapid execution of cost-effective and efficient development of products and services to protect our nation and its resources.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security’s first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a scientist and senior executive and Board Member in high-technology firms in the private sector.

Appendix C: Bridging the Communications Gap (Article)

Bridging the “Communications Gap” between the Public and Private Sector – Making it Easier to do Business with DHS

DHS’s new commercialization outreach efforts center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

If you think about it, there are numerous examples in our professional and private lives where the lack of communication or unclear terminology has created misunderstandings, problems and myriad other issues. As in any worthwhile pursuit, effective communication is critical in the cost-effective and efficient interactions between various parties seeking a mutually beneficial partnership. The U.S. Department of Homeland Security (DHS) is putting into practice the necessary rigor to improve communication that will allow the public and private sectors to work jointly to meet the unsatisfied needs of the DHS in order to protect the Nation.

To this end, the DHS Commercialization Office has developed a number of processes, programs and tools to facilitate the clear articulation of DHS needs (See Figure 1). In that same spirit of working together with the private sector, we recently developed a “Product Realization Chart” (see Appendix H) which is a useful guide to relate concepts and correlate terminology used by both the public and private sector to clearly delineate how science, technology development and product development (terms used in the private sector) are related to basic research, innovation and transition using a Technology Readiness Level (TRL) “backbone” (terms used in the public sector).

Further examination of the Product Realization Chart shows that this resource also provides a stage-gated approach for cost-effective and efficient product development to provide a “discussion framework” useful in private-public sector discussions as well as a template for utilization to develop and communicate agreements. The chart describes the objectives, deliverables and the type of management review necessary to develop and deliver technologies/products/services that meet the specific requirements of the DHS’ operating components (U.S. Coast Guard, FEMA, TSA, CBP, USCIS, U.S. Secret Service and ICE) and its end users such as first responders.

Stage One: Needs Assessment

Needs assessment is the critical first stage of product realization (accomplished via acquisition or commercialization processes) that enables DHS to identify capability gaps

and investigate new product/technology/service capabilities. By understanding the specific and detailed requirements of its customers, the DHS Science & Technology Directorate (DHS S&T) conducts market research and technology scans to find and assess technology-based solutions that could potentially be developed, matured and delivered to DHS end users.

Commercialization programs, processes and tools...

- 1) "Developing Operational Requirements" Guide
- 2) "DHS Implements Commercialization Process" Article
- 3) "Partnership Program Benefits Taxpayers as well as Private and Public Sectors" Article
- 4) SECURE Program and website
- 5) DHS online
- 6) Invited talks to trade conventions, reaching small, medium and large businesses. Efforts also extend to meet with minority, disadvantaged and HUB Zone groups on a regular basis.

Figure 1: Outreach efforts to inform the public on "How to do Business with DHS" is receiving positive feedback from the private sector and media. See the following website for additional information:

Please note that management reviews for both the public and private sector are required to ensure that exit criteria and deliverables are met when discussing public-private programs like the SECURE Program.

The remainder of the chart shows the various key objectives and deliverables for each major phase of product realization. Entrance at any point of the chart is possible and certainly, the overall objective of many projects currently underway at DHS is to obtain widely distributed products or services (where commercialization is key). DHS also sometimes has unique "custom-like" requirements with lower unit-volume potential (normally using the Acquisition model as shown in Figure 2). It also should be noted that in a basic research program, it may certainly not be possible to generate an ORD, as the objective may be the "exploring uncharted territory" rather than the development of products or services for sale to a particular market. For this reason, a dark box is drawn around Stage 1 to indicate that the Product Realization Chart is a multiple-use chart, rather than a concrete process because it simply offers a framework to visualize several processes, some of which (developing custom or widely distributed products/services) require a Needs Assessment.

Stage Two: Science

At the beginning of the second stage, basic principles are observed and reported, and scientific research begins to be translated into applied research and development (R&D). At this stage, a program sponsor and end user/customer have been identified and the mission needs statement, feasibility study and program management visions have been developed.

Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. In the case of developing products/services, operational requirements

analysis has been conducted and operational requirements are applied to functional requirements. A risk management plan has been developed, a program cost analysis has been completed and a preliminary security assessment has been conducted.

As the technology concept and/or application is formulated, active R&D is initiated that results in an analytical and experimental critical function and/or characteristic proof of concept. This includes analytical studies to physically validate the analytical predictions of separate elements of the technology. A Systems Engineering Management Plan (SEMP), Program Management Plan (PMP) and proof of concept plan are key deliverables and serve as exit criteria for the next stage of product realization.

During the second stage, the private sector normally produces a complete product plan during commercialization that addresses marketing opportunities, financial considerations, design concept and many additional analyses. Sales/Marketing team performs a SWOT (strengths, weaknesses, opportunities, and threats), a scenario analysis and a sales forecast estimate. Research assembles the key IP disclosure submissions. Quality Assurance (QA) generates all safety/standards compliance items, calibration requirements and other quality control specifications.

Management reviews for both the public and private sector are required (in partnership projects or programs) to ensure that exit criteria and deliverables are met.

Stage Three: Technology Development

The third stage of product realization ensues when basic technological components are integrated to establish that they will work together, which is a relatively “low fidelity” analysis when compared with the eventual system. The proof of concept report and functional requirements document have been finalized. The SEMP, Test and Evaluation Master Plan (TEMP), quality assurance plan and other deliverables are revised and updated on a continuous basis.

The basic technological components are then integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. The fidelity of the breadboard technology increases significantly in this case. The Operational Requirements Document (ORD) and CONOPS are better developed. The technology scan and market survey are ongoing during the third stage, and an analysis of alternatives is provided.

Once the component is validated in a relevant environment, the system/subsystem model or prototype is demonstrated in a relevant environment. After successful T&E in a simulated operational environment, a preliminary Technology Transition Agreement (TTA) or a Technology Commercialization Agreement (TCA) is executed as applicable. A program manager is identified and an interoperability assessment is performed.

During this stage, the private sector uses its product plan to conduct a beta design review, produce a detailed supplier list and supplier benchmark, begin writing the user’s manual, develop a service strategy, confirm the risk analysis and review engineering change orders. Manufacturing creates a preliminary manufacturing plan and works with

Marketing/Sales to finalize product packaging. Quality Assurance defines regulatory requirements, prepares a preliminary quality plan and procedure for first prototype testing and designs the inspection tooling.

Management reviews for both the public and private sector are required to ensure that exit criteria and deliverables are met.

Acquisition versus Commercialization

Once a representative model or prototype system, which beyond TRL 5, is tested in a relevant environment, the product realization process splits into two paths that are extraordinarily different as evidenced in Figure 2: Acquisition and Commercialization. Acquisition occurs when a government contractor executes design, development and production, driven by DHS requirements, using DHS funding and under contract to DHS. In this case, the product is then deployed to captive users and the product unit price is determined by cost-based pricing. The contractor's customer is DHS and not the end-user community.

Commercialization, on the other hand, is a private-sector driven activity enterprise that executes design, development and production, driven by market requirements, using private funding and perhaps assisted by DHS technology licenses, standards and grants. The product is then sold as commercial-of-the-shelf (COTS) directly to end users and the product unit price is determined by market-based pricing. The vendor's major customer is the end-user community (e.g. first responders) as well as various private sector markets.

Why is there a need for commercialization? As previously mentioned, DHS requirements, in most instances are characterized by the need for widely distributed COTS products. Oftentimes, the need is for thousands, if not millions of products for DHS' seven operating components and the fragmented, yet substantial first responder end-user market. Figure 2 shows the major differences between a "pure" Acquisition versus "pure" commercialization processes, along with the recently developed and implemented DHS "hybrid" commercialization process.

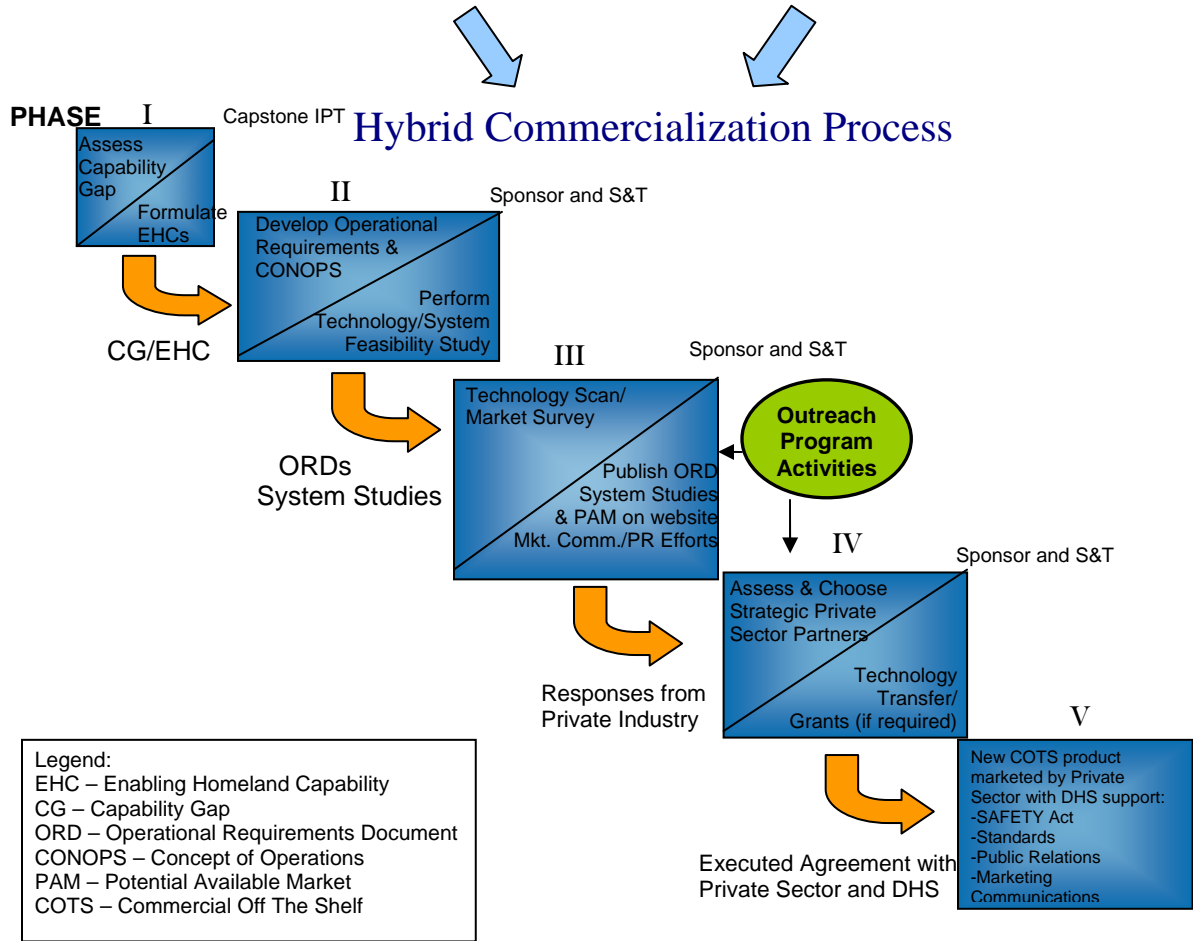
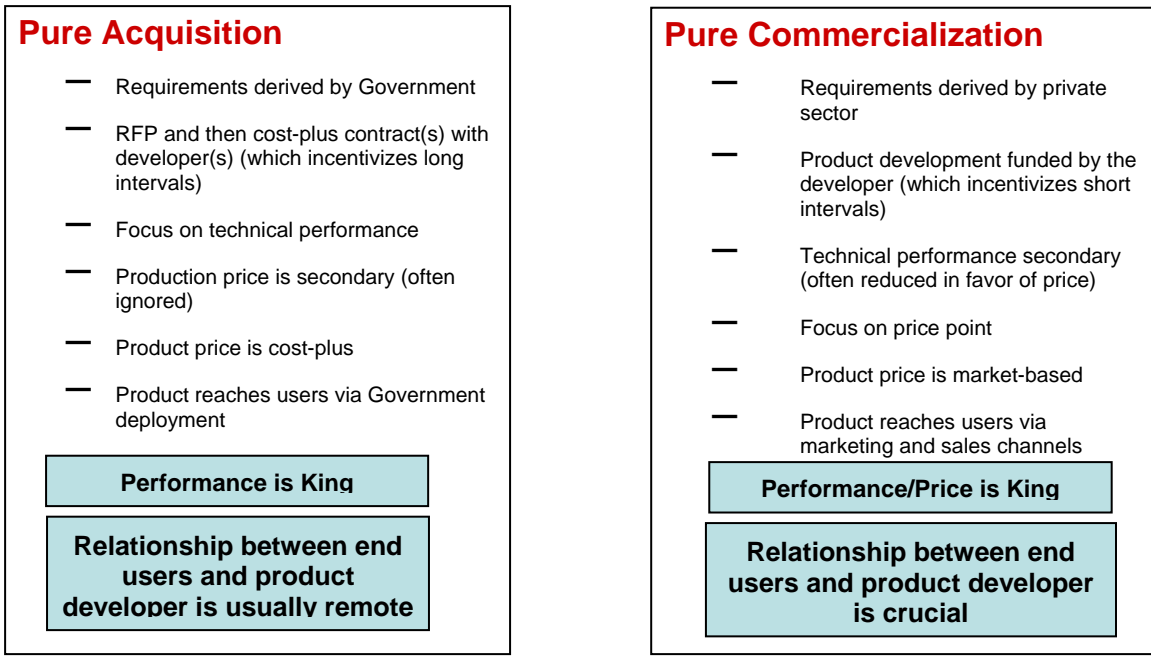


Figure 2: Comparison of “Pure Acquisition” versus “Pure Commercialization” models for product/system development and the resultant hybrid model implemented by DHS.

Figure 3 delineates the overall description of DHS' new commercialization model and its first private sector outreach program called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program to develop products and services in a private-public "win-win" partnership, recently approved in June 2008 by DHS and described in detail at www.dhs.gov/xres/programs/gc_1211996620526.shtm. Briefly, the SECURE Program is based on the premise that the private sector has shown that it is willing and able to use its own money, resources, expertise and commercialization experience to develop and produce fully developed products and services for DHS if significant market potential exists. The private sector has shown remarkable interest in devoting its time and money to such activities if and when an attractive business case can be made related to large revenue/profit opportunities that certainly exist at DHS and its ancillary markets to participate in the advancement of DHS commercialization efforts. The private sector requires two things from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s). Once this information is posted to the SECURE Program website, small, medium and large companies are open to generate their own business cases and pursue possible participation in the program.

A New Model for Commercialization...

- Develop Operational Requirements Documents (ORDs)
- Assess addressable market(s)
- Publish ORD and market assessment on public DHS web portal, solicit interest from potential partners in a way that is open to small, medium and large businesses
- Execute no-cost (CRADA-like) agreement with multiple private sector entities and transfer technology and/or IP(if necessary)
- Develop supporting grants and standards as necessary
- Assess T&E findings after product is developed to assure DHS and ancillary markets that product meet its published specifications
- New Commercial-Off-The-Shelf (COTS) product marketed by private sector with DHS support

SECURE Program



- Application – Seeking products/technologies aligned with posted DHS requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized third-party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal to provide confidence to potential customers at DHS and its ancillary markets that product(s) meet or exceed their published specifications in reference to their actual performance.

Figure 3: Step-by-step guide to the commercialization process developed and adopted by DHS with a brief summary of the popular SECURE Program.

In order to provide DHS operating components, the first responder community and other end-users with products that meet their specific requirements, the SECURE program provides a vehicle by which private sector entities can offer products and/or conduct product development geared specifically toward meeting those needs. Private sector entities currently possessing a technology/product/system rated at a Technology Readiness Level TRL-5 (i.e. applied or advanced R&D) or above that potentially closes a defined DHS capability gap by addressing detailed operational requirements supplied by DHS-S&T on the SECURE Program website will have the opportunity enter into a CRADA-like agreement to continue development of their technology/product/system to TRL-9 (i.e. fully field deployable product) at their expense. The CRADA-like agreement also provides private sector entities with the assurance that DHS-S&T will verify their recognized independent third-party test(s) of a given technology/product/system. A Cooperative Research and Development Agreement (CRADA) is a written agreement between a private company and a government agency to work together on a project⁸.

Stage Four: Product Development

After DHS determines whether the Acquisition or the Commercialization process is appropriate, the fourth stage commences and the system prototype is demonstrated in an operational environment. S&T and the end user/customer have begun to develop a final transition plan and updates have been made to the operational and/or functional requirements document. Interoperability has been demonstrated and Management Directives (MD) have been reviewed to assure compliance. An operations and maintenance manual has been completed and a security manual has been developed.

Since the technology has been proven to work in its final form and under expected conditions, TRL 8 represents the end of true system development. Technology components are therefore form, fit, and function compatible with an operational system. The operational test report has been completed and a Limited User Test (LUT) Plan has been developed. A training plan has also been developed and implemented.

The actual system is then proven through successful mission operations and the end user fully demonstrates the technology in the CONOPS. All critical documentation has been completed and planning is underway for the integration of the next generation technology into the existing program components.

During the last stage, the private sector focuses on the manufacturing plan and the development effort includes the final design reviews, product prototypes along with documented product test results and other product development deliverables. Sales/Marketing update the marketing plan, the sales and distribution plan, and all sales

⁸For more information on CRADAs, please visit:
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+15USC3710a and
<http://www.usgs.gov/tech-transfer/what-crada.html>.

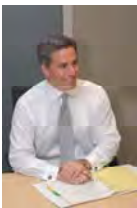
materials. Manufacturing develops assembly and manufacturing procedures, designs and fabricates manufacturing tooling. Quality Assurance updates the Test Q/A plan and creates the quality plan. They also develop testing procedures, create test and fixture designs, perform reliability testing on the prototype and design and test the shipping container.

The goal of the private sector during the final stage is to demonstrate product manufacturing according to quality assurance standards while remaining within cost/schedule targets. The development effort concludes with a customer-adopted defect-free product, implemented engineering change orders and a final user's manual. Applications engineering and technical engineering support are then implemented. Sales/Marketing also provides sales training, creates a promotional plan and coordinates literature advertising and public relations. Manufacturing establishes the final manufacturing/assembly routines and procedures, the final manufacturing tooling, and the manufacturing document release and acceptance, then undertakes an analysis for future product cost reduction. Quality Assurance does the final QA and test pooling, prepares the final QA/test procedures, and compiles the manufacturing yield data.

Management reviews for both the public and private sector are required to ensure that the final exit criteria and deliverables are met. Since the actual system has been proven through successful mission operations, the product is then deployed to captive users or sold as COTS directly to end users.

Conclusion

The Commercialization Office has developed a number of processes, programs and tools to clearly articulate the needs of DHS. Outreach efforts are also critical and center on notifying the private sector about opportunities that exist for partnership and business development to address the needs of the Department. Therefore, we have developed a "Product Realization Chart" that serves as a useful guide to relate and correlate terminology used by both the public and private sector in order to develop and deliver required technologies/products that meet the specific operational requirements of the Department of Homeland Security's operating components and its end users such as first responders.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security's first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a scientist and senior executive and Board Member in high-technology firms in the private sector.

Appendix D: Commercialization: It's Not Business as Usual at DHS S&T (Article)

Commercialization: It's Not business as usual at USDHS

*Robert R. Hooks and Thomas A. Cellucci, U.S. Department of Homeland Security:
Science and Technology Directorate, Washington D.C. 20528*

Introduction:

The U.S. Department of Homeland Security (DHS) is comprised of many organizational elements with a single purpose: to enable, support and expedite the mission critical objectives of DHS' seven operating components – Transportation Security Administration (TSA), U.S. Customs and Border Patrol (CBP), U.S. Secret Service, (USSS), U.S. Citizenship and Immigration Service (USCIS), U.S. Immigration and Customs Enforcement (ICE), Federal Emergency Management Agency (FEMA), and the U.S. Coast Guard (USCG).

In these unprecedented times, there is an immediate need for DHS to provide these operating components with the products and services they require, using efficient and cost-effective product development methods. DHS is working proactively to attract the private sector to develop, produce, test and evaluate products that meet the requirements of DHS operating components and first responders.

Why would the private sector be inclined to develop products at their own expense? This initiative's high probability for success lies in the following principles and guidelines:

1. DHS operating components determine clearly-defined capability gaps and operational requirements that can be addressed effectively with Commercial-Off-The-Shelf (COTS) items.
2. The private sector wants access to large potential available markets (PAMs) that comprise the DHS operating components and ancillary markets as it enables a presumably strong business opportunity.
3. Taxpayer cost savings will be realized by the "win-win" private-public sector partnership. Figures 2 and 3 respectively outline a market potential template and private sector outreach process of the critical elements to attract the private sector's interest in partnering with DHS.

"Win-Win" Strategic Partnerships

One often-overlooked vehicle to cost-effectively and efficiently commercialize technology is the formation of a win-win strategic partnership. The relationship between the public and the private sectors can be mutually beneficial in many ways, as each has something of value that the other desires. DHS has substantial potential available markets and direct access to the operating requirement of its large "customer base" as well as detailed information on the unmet needs and wants of ancillary market customers found in state, local and tribal communities.

Requirements development is one of the cornerstones of the commercialization process. DHS' Science & Technology Directorate (S&T) develops clear, detailed

operational requirements documents (ORDs) and intends to publish them on what would be a public web portal accessible by the private sector entities who believe they have the ability to meet those published requirements. Further benefits that DHS has to offer private sector entities come in the form of grants and Small Business Innovative Research (SBIR) programs.

Conversely, the private sector has skills, expertise, capital, established sales channels and the integrated marketing programs necessary to produce and distribute technically advanced products. The private sector appreciates a conservative estimate of the potential available markets within DHS operating component and/or ancillary markets, as well as clear, detailed operational requirements. With these two items in hand, the private sector can verify supplied estimates and generate business cases to determine if it is feasible to conduct research and development to develop and distribute products or services. This relationship enables substantial benefits given the ever-changing nature of the needs of established and potential new security applications. The private sector will need to continue its innovation as DHS adjusts to address new, emerging threats.

Synchronization:

The execution of a radically different methodology to develop, produce and distribute new products for use by DHS operating components does not come without its challenges. For many years, the U.S. government was indoctrinated and accustomed to the acquisition process of commissioning a custom-made product or service to perform a specific objective. The government would oversee the creation of the requirements, concept and technology development, system capability development, testing and evaluation, and production and deployment – paying for each step of the process. The concept of transferring responsibility of many of the steps in the process to the private sector ultimately removes control by the government. Not only is this a new way of thinking about developing and procuring products, it necessitates clear and precise communications between the public and private sectors.

In its new commercialization model, S&T acts as a facilitator between its customers, DHS' operating components and ancillary markets, and the private sector entities potentially developing products. S&T must work with its valued customers in the creation of ORDs as well as conduct market surveys and technology scans to ensure that needed technical capabilities and/or products exist within firms accessible for distribution of these ORDs. Oftentimes, private sector entities have products in development that are closely aligned with current homeland security capability gaps. In these situations, it is important to determine the exact level of development for the product.

As previously stated, clear and precise communications are paramount. To that end, the lexicon of product development was different in the public versus private sectors (see figure 4). Notice that DHS utilizes Basic Research, Innovation, and Transition nomenclature with Technology Readiness Levels as a “backbone” language, while the private sector utilizes Science, Technology Development, and then Product Development as the phases of developing a product from a concept. In order to ensure effective communications, the Technology Readiness Levels (TRL) model is used to standardize communication for all parties involved (see Figure 5). With the TRL system in use, all parties are able to assess quickly the development stage of a given product and determine an anticipated timeline for product deployment.

Open and Fair Competition leads to Cooperative New Product Development:

Once DHS has fulfilled its obligation to create realistic ORDs, conducts technology scans and market surveys to ensure that capabilities exist, the department would then post pertinent requirement information on the proposed publicly available, open access website. This web portal would be the vehicle by which private sector entities can engage DHS to find capability gaps for which solutions exist or can be produced quickly and efficiently. Given this information, private sector entities could to develop or enhance a given product or service in cooperation with S&T to enable or improve upon currently fielded DHS solutions. Close alignment with the detailed requirements are critical in this process.

In theory, in order for a company to be considered by S&T for cooperative development, it should be able to:

1. Demonstrate they possess technology at TRL-5 (i.e. applied or advanced R&D) or above and possess the resources to invest in the commercialization of its technology to TRL-9 (i.e. fully field deployable product);
2. Propose a technology development effort that has clear and substantial alignment with published S&T requirements; and

A simple, straightforward and binding agreement could then be executed whereby the private sector entity will detail milestones with dates to develop its technology to a TRL-9 state (if not already at that level). Once the private sector entity has successfully achieved TRL-9, it will perform independent third-party testing and evaluation (T&E) on the product to ensure it meets all required previously agreed-upon specifications. S&T then would review and evaluate the accuracy of the third-party T&E and publish its factual findings on the proposed Web site. The free market system should yield several companies producing similar products as is often seen in commercial markets. DHS customers and ancillary markets stand to benefit from this system.

Measurable Results:

The ultimate goal of any commercialization initiative is to produce products that are better, faster and less expensive compared to what is currently on the market. S&T hopes to leverage the private sector's endless pursuit of this idea and marry it with the vast demands created by an organization whose mission is to protect a nation. S&T has a critical role acting as the facilitator between sets of markets and a willing and able private sector looking for large, stable markets to purchase and use advanced technologies. A program like this should result in a demonstrable increase in the quality and quantity of technologies, products and services to assist not only DHS in carrying out its mission objectives, but customers engaged in many other related security applications. It is indeed expected that taxpayers will observe a significant and demonstrative increase in the amount of private sector funding used for the timely development of new and reliable products to help thwart the threat of terrorism.

Conclusion:

The U.S. Department of Homeland Security Science & Technology Directorate is forging a new paradigm that can have far-reaching positive consequences for its

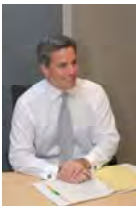
customers, private sector partners, and U.S. taxpayers through the rapid, cost-effective and efficient development and deployment of products and services to protect the United States. The relatively recent formation of DHS (its fifth anniversary was on March 1, 2008) is advantageous in many ways, particularly in that it enables flexible and forward thinking in its long-term goals and processes. Our commercialization initiatives are a groundbreaking and innovative approach to foster a mutually beneficial relationship between the public and private sectors, both of whom stand to benefit greatly from this new partnership created in open and free competition. The future of this initiative looks bright; we have already experienced an overwhelmingly positive response to the initial private sector outreach. S&T will continue to monitor and measure the benefit this program stands to provide.

Acknowledgements:

The authors would like to express their sincere appreciation for all of the valuable assistance by Mr. Mark P. Protacio in the preparation of the materials used in this paper.



Robert R. Hooks is the Director of Transition at the U.S. Department of Homeland Security’s Science and Technology Directorate (DHS S&T) in Washington, D.C. and recently accepted the position of Deputy Assistant Secretary of Weapons of Mass Destruction and BioDefense of the DHS Office of Health Affairs in Washington, D.C.



Thomas A. Cellucci, Ph.D., MBA is currently the Science & Technology Directorate’s first Chief Commercialization Officer in Washington, D.C. He has spent the vast majority of his career as a senior executive and board member in high technology firms in the private sector.

FIGURES

Fig. 1: Capstone IPT Process

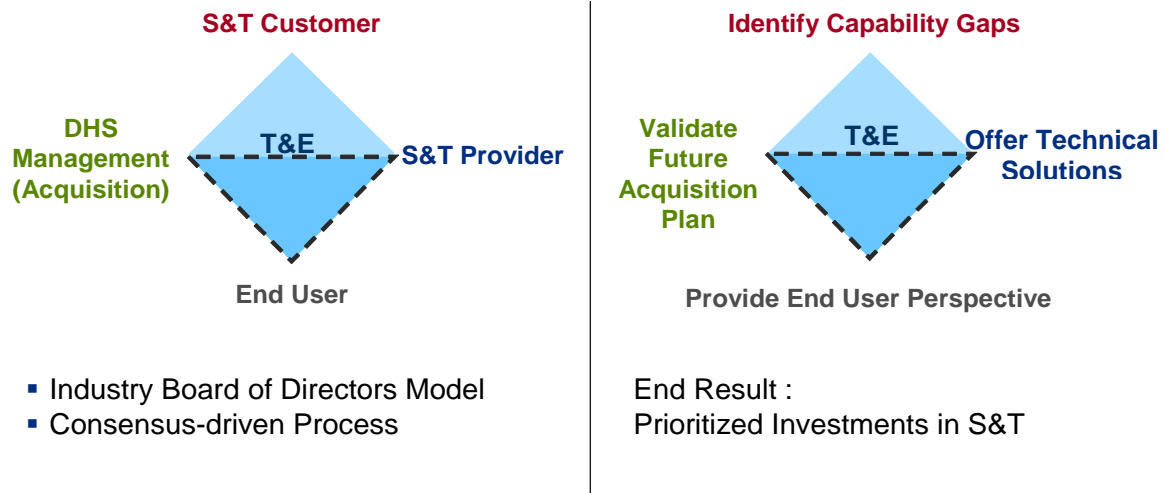


Fig.1 – This graphical representation shows the Capstone IPT (Integrated Product Team) process implemented at S&T that enables all stakeholders to participate actively in identifying and discussing the *Capability Gaps* germane to a specific functional area, such as people screening. S&T works with its customers, pertinent end-users and DHS organizational entities to delineate operational requirements to start a process to close identified capability gaps.

Fig. 2: Market Potential Template

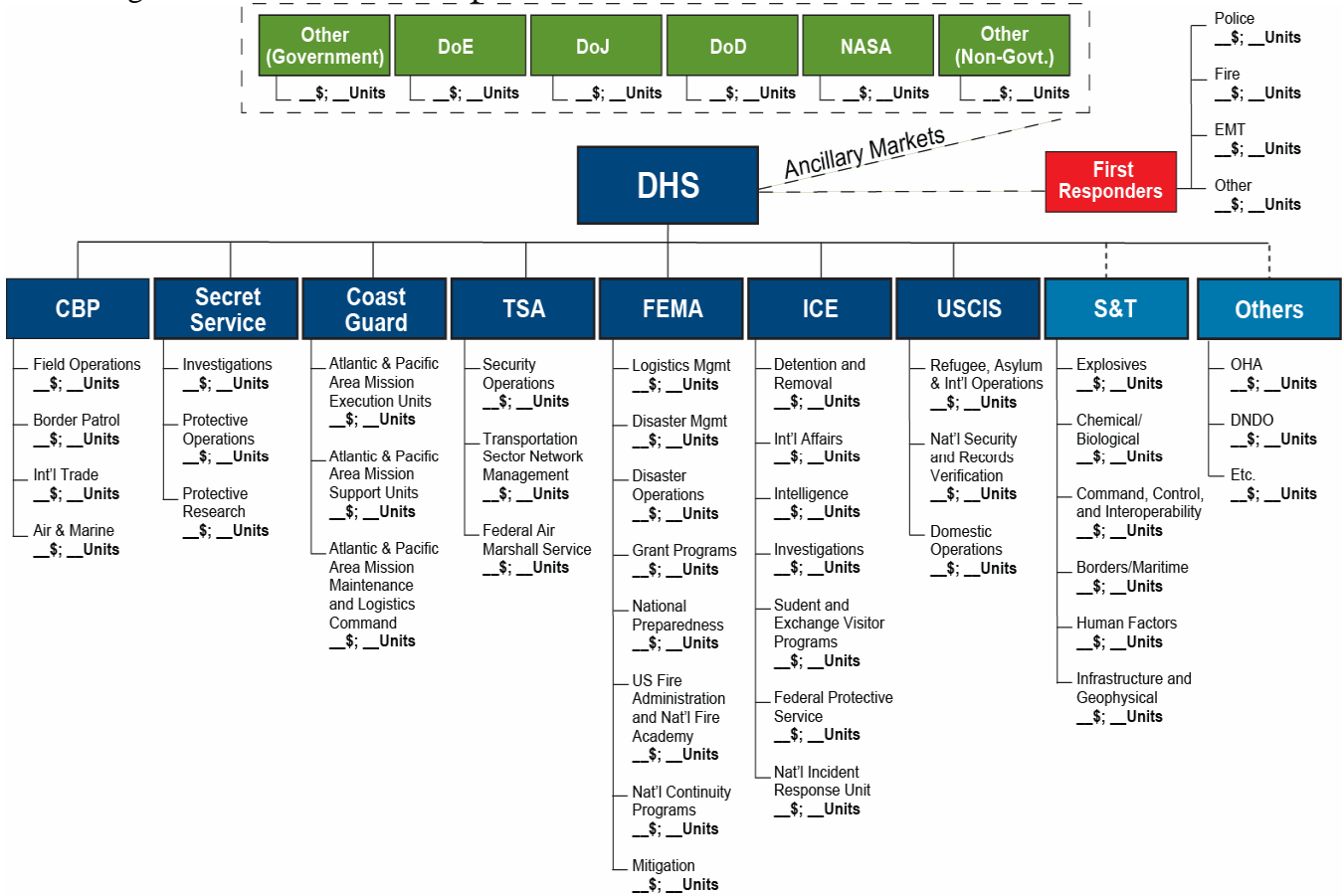
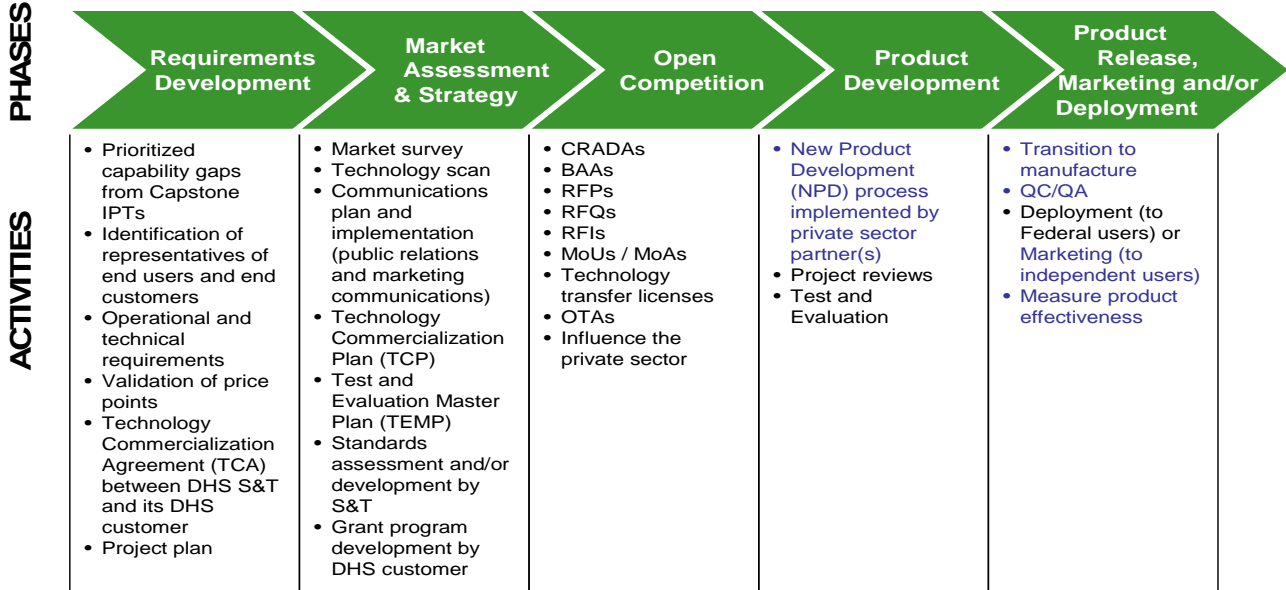


Fig. 2 – This graphic shows a market potential template used to conservatively estimate the DHS market segment by operating components, as well as demonstrate how DHS is a conduit to other large ancillary markets.

Fig. 3 Private Sector Outreach Process

Private Sector Outreach Process

Requirements Identification through Product Release



Legend: Black text = Government activities
 Blue Text = Private-sector activities

Fig.3 – The Private Sector Outreach Process outlines the steps and procedures undertaken to develop and deploy a product or service from capability gap identification to product deployment.

Fig. 4: Lexicon differences

Correlation: DHS and Private Sector

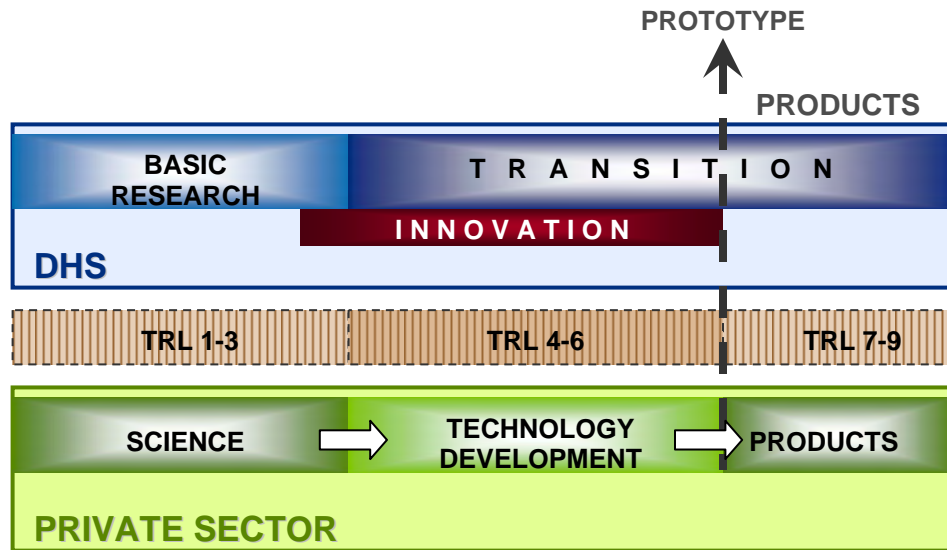


Fig. 4: This chart shows the correlation between the various nomenclatures to delineate differing levels of product development. The Technology Readiness Levels (TRL) serves as a standardized lexicon for enhanced communications.

TRLs are NASA-generated and Used Extensively by DoD

Fig. 5: Technology Readiness Levels

Fig. 5 – TRLs are used to assign a numerical value to a corresponding stage in a technology’s development and maturity. This system of standardization is useful to communicate effectively between entities that may have used varying technology-maturity lexicons.

Basic principles observed and reported	1	Basic	Technology Maturity
Technology concept and/or application formulated	2		
Analytical and experimental critical function and/or characteristic	3		
Component and/or breadboard validation in laboratory environment	4	Advanced	
Component and/or breadboard validation in relevant environment	5		
System/subsystem model or prototype demonstration in a relevant environment	6	Applied	
System prototype demonstration in a operational environment	7		
Actual system completed and 'flight qualified' through test and demonstration	8		
Actual system 'flight proven' through successful mission operations	9		

Appendix E: Partnership Program Benefits Taxpayers, Private and Public Sectors (Article)

Partnership Program Benefits Taxpayers as well as Private and Public Sectors

SECURE Program enables the cost-effective and efficient development of products and services for Homeland Security.

Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Commercialization Office
U.S. Department of Homeland Security

A recently announced initiative at the U.S. Department of Homeland Security (DHS), called the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program is part of an overall effort at the Department to create a “Commercialization Mindset” by leveraging the fact that while DHS has a limited budget compared to the Department of Defense, it does have something much more valuable – a large potential available market comprised of the seven DHS operating components (USCIS, TSA, FEMA, CBP, ICE, U.S. Coast Guard and U.S. Secret Service) and other large ancillary markets such as the diverse, yet substantial first responder market.

The SECURE Program is based on the premise that the private sector has shown that it is willing and able to use its own money, resources, expertise and experience to develop and produce fully developed products and services for DHS. When an attractive business case can be made related to large revenue/profit opportunities, which certainly exist at DHS and its ancillary markets. The private sector requires two vital pieces of information from DHS: 1. detailed operational requirements, and 2. a conservative estimate of the potential available market(s). This information can then be used to generate a business case for possible private sector participation in a program or project.

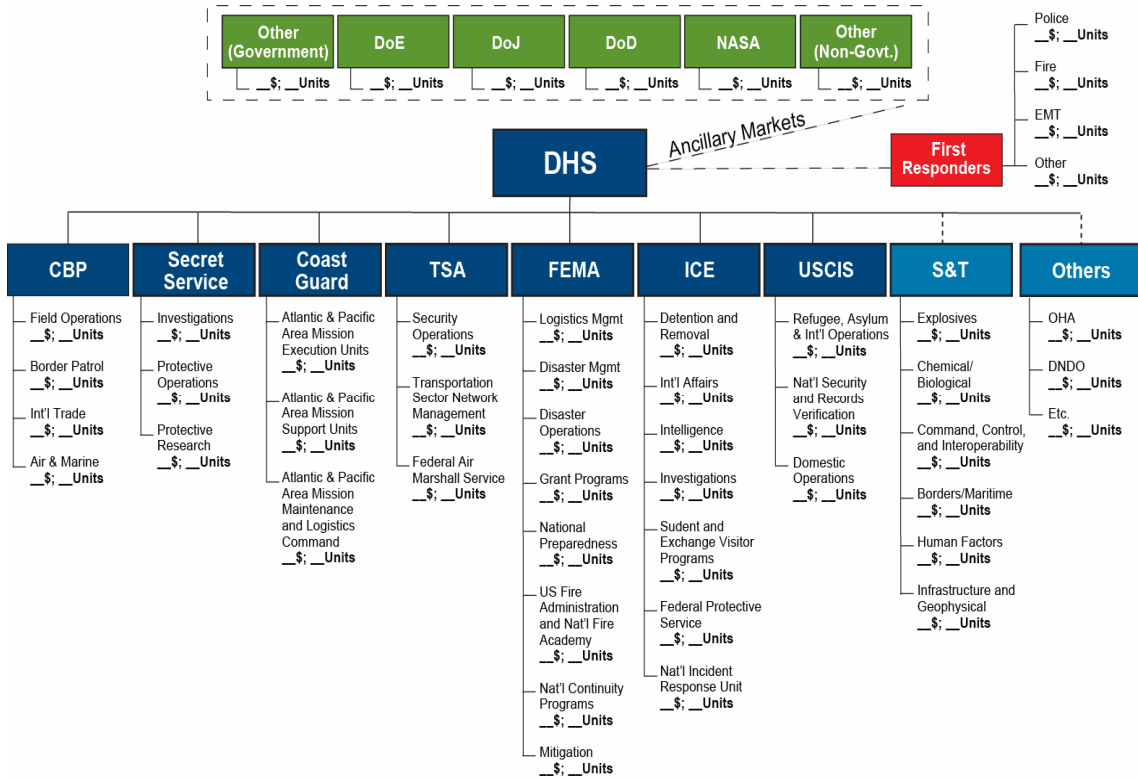


Figure 1: This Market Potential Template is used to estimate the given size of a particular market that DHS has identified as an area requiring new products or services.

This Market Potential Template is used to demonstrate how large (in both a dollar and unit volume perspective) a given market is for a particular product or service. Coupled with an Operational Requirements Document (ORD), the private sector receives ample information from DHS to generate a business case for developing a product or service sought after by DHS for its operating components or first responders, whose combined ranks are significant, as delineated in Figure 2.

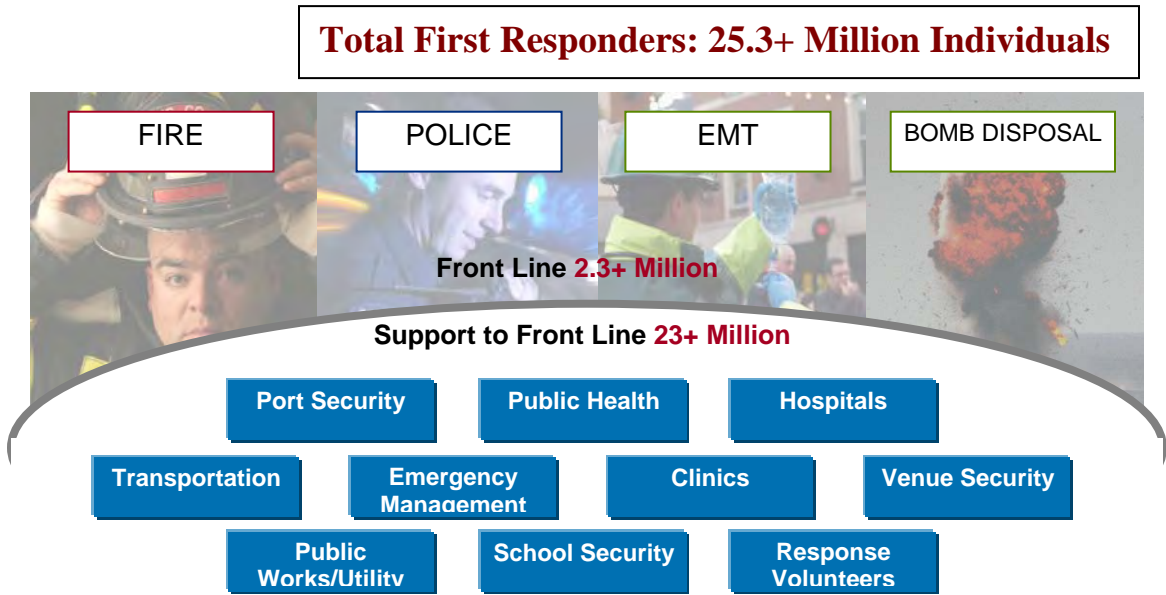
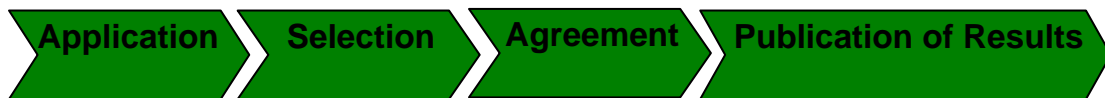


Figure 2: Homeland Security Presidential Directive Number 8 (HSPD-8) conservatively classifies 25.3+ million individuals as First Responders in the United States alone.

In return for providing this critical information, thus saving the private sector considerable time and money related to both market and business development activities, DHS expects the private sector to offer solutions – utilizing the free market system with open and fair competition – to meet published requirements. Simply stated, the private sector receives significant business opportunities, DHS and its supported entities, like the first responder communities, receive products and services developed at faster execution rates at the private sector’s cost – all to the benefit of the American taxpayer. See Figure 3 for an overview and benefits analysis of the SECURE Program.

SECURE Program

Concept of Operations

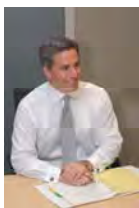


- Application – Seeking products/technologies aligned with posted DHS/First Responder requirements
- Selection – Products/Technologies TRL-5 or above, scored with internal DHS metrics
- Agreement – One-page CRADA-like document that outlines milestones and exit criteria
- Publication of Results – Recognized Third-Party T&E conducted on TRL-9 product/service. Results verified by DHS, posted on DHS web-portal

SECURE Program Benefit Analysis – “Win-Win-Win”		
Taxpayers	Public Sector	Private Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Improved understanding and communication of needs	1. Save significant time and money on market and business development activities
2. Tax savings realized through private sector investment in DHS	2. Cost-effective and rapid product development process saves resources	2. Firms can genuinely contribute to the security of the Nation
3. Positive economic growth for American economy	3. Monies can be allocated to perform greater number of essential tasks	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work.
4. Possible product “spin-offs” can aid other commercial markets	4. End users receive products aligned to specific needs	4. Significant business opportunities with sizeable DHS and DHS ancillary markets
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. End users can make informed purchasing decisions with tight budgets	5. Commercialization opportunities for small, medium and large business

Figure 3: Brief overview of the SECURE Program’ Concept-of-Operations and a benefits analysis.

To learn more about the SECURE Program and other opportunities for the private sector, please visit http://www.dhs.gov/xres/programs/gc_1211996620526.shtm or contact the Commercialization Office at SandT_Commercialization@hq.dhs.gov.



Thomas A. Cellucci, Ph.D., MBA is the U.S. Department of Homeland Security’s first Chief Commercialization Officer. In his role, he recently published two comprehensive guides: *Requirements Development Guide* and *Developing Operational Requirements* to aid in effective requirements development and communication for the department. He possesses extensive experience as a scientist and senior executive and Board Member in high-technology firms in the private sector.

Appendix F: Commercialization Briefing to Industry

The following pages include slides used in briefing the private sector on business opportunities with DHS and its stakeholders.

Slide 1

Opportunities for the Private Sector



Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Department of Homeland Security
Science and Technology
Email: Thomas.Cellucci@dhs.gov

Slide 2

Discussion Guide

- Overview of Department of Homeland Security
- Commercialization initiatives at DHS
- Capstone Integrated Product Teams (IPTs)
- Market Potential is Catalyst for Rapid New Product Development
- Getting on the Same Page
- SECURE Program
- Safety Act Protection
- Tech Clearing House
- SBIR Opportunities
- Getting Involved
- Summary



Slide 3

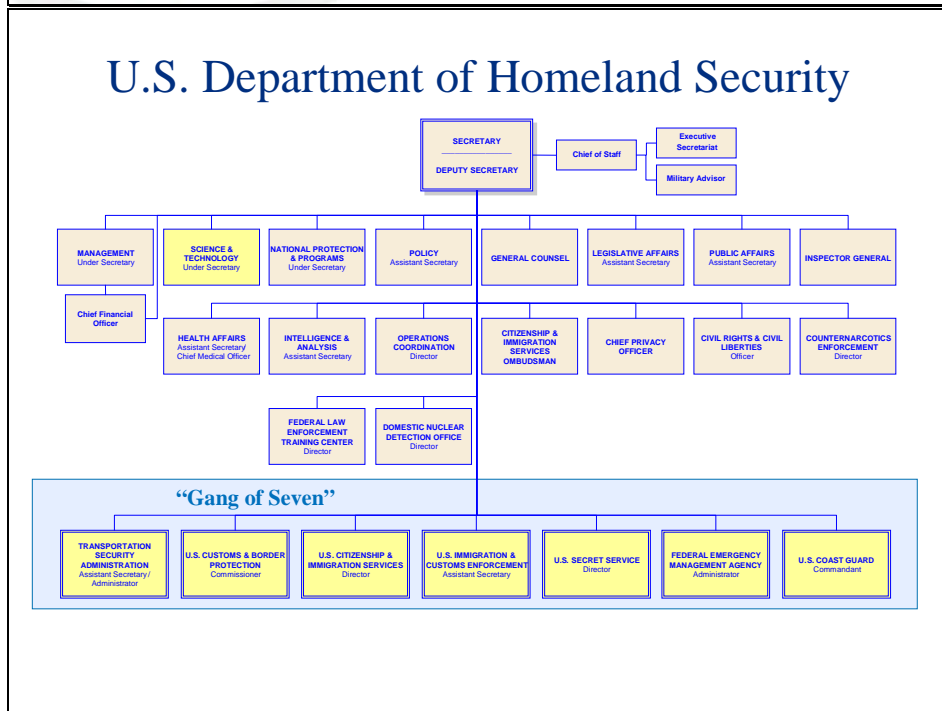
Homeland Security Mission



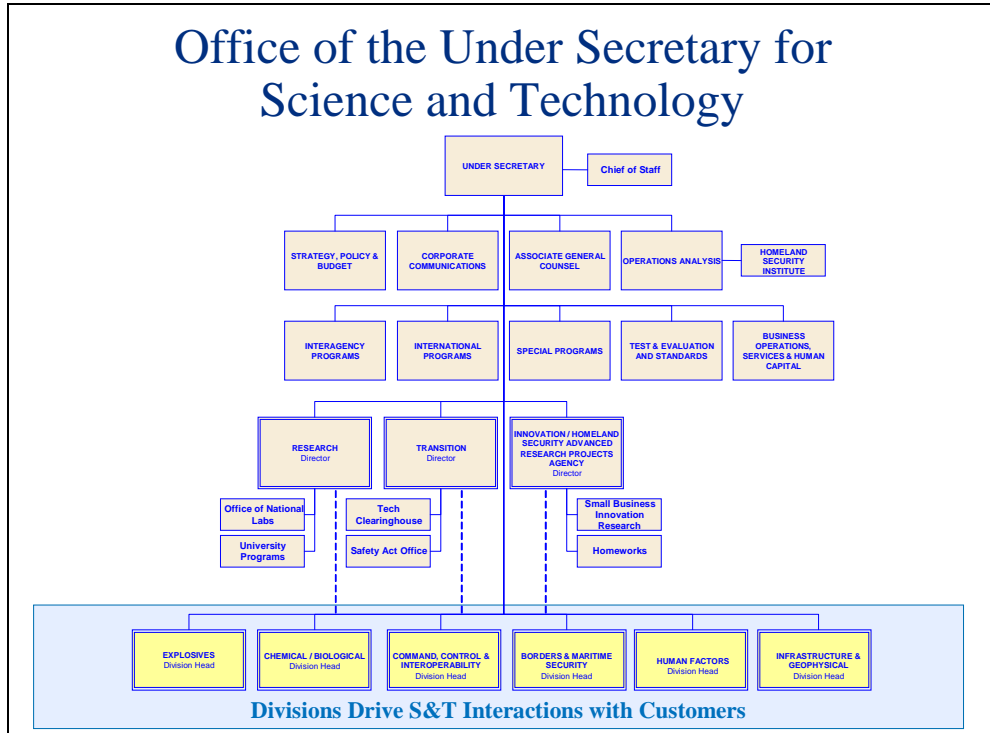
- Lead Unified National Effort to Secure America
- Prevent Terrorist Attacks Within the U.S.
- Respond to Threats and Hazards to the Nation
- Ensure Safe and Secure Borders
- Welcome Lawful Immigrants and Visitors
- Promote Free Flow of Commerce



Slide 4



Slide 5




Slide 6

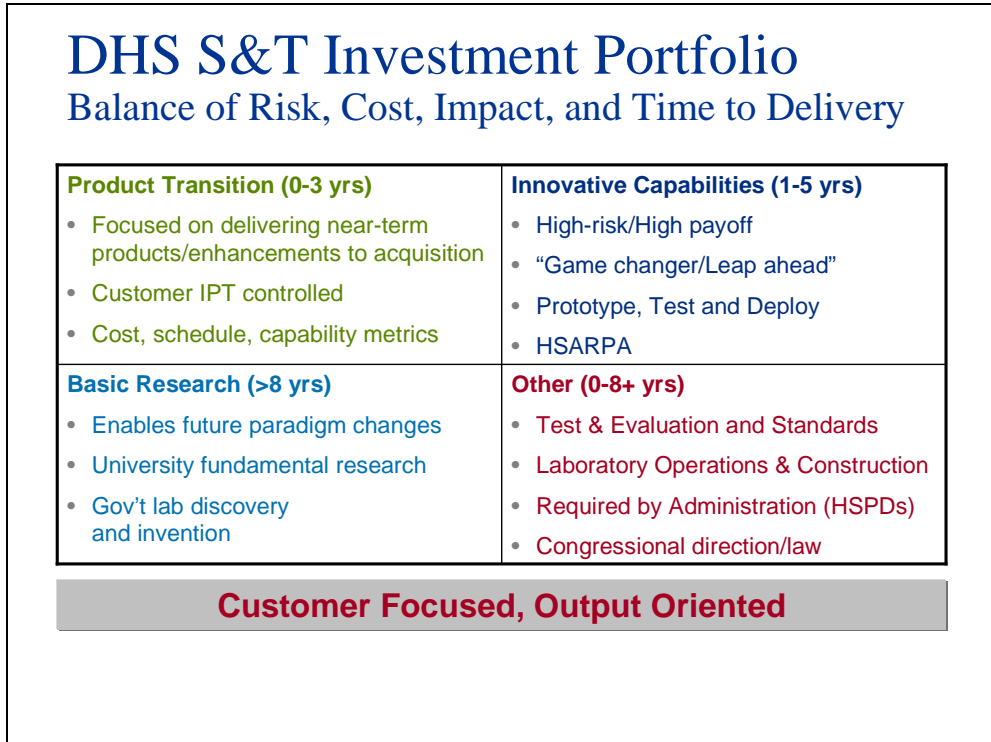
S&T Goals

Consistent with the Homeland Security Act of 2002

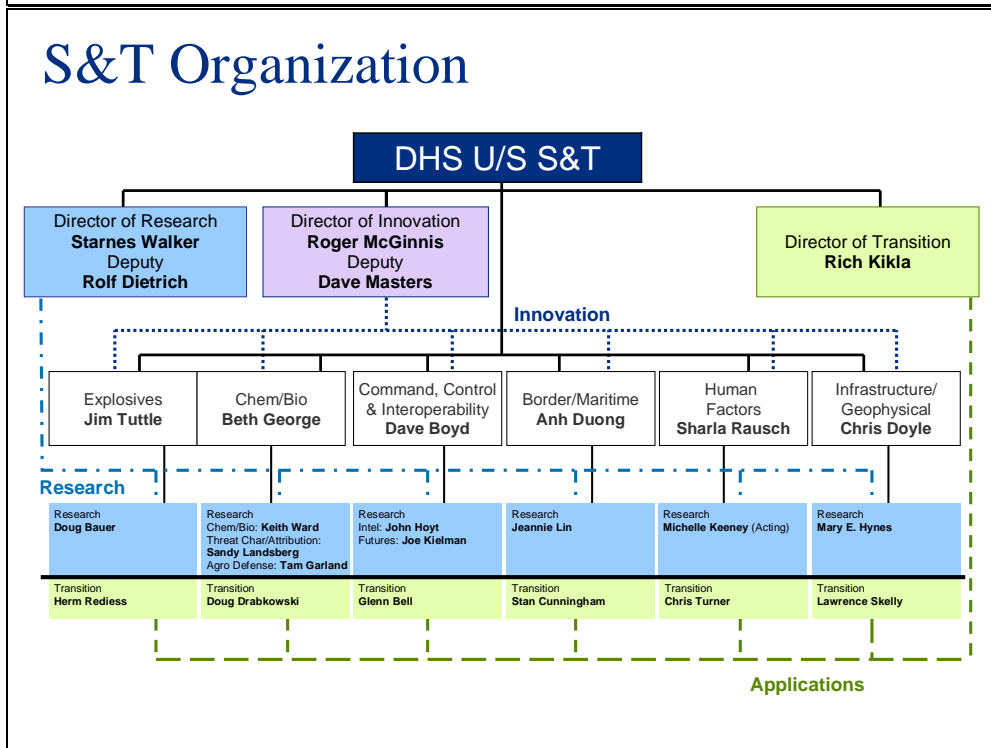
- **Accelerate the delivery of enhanced technological capabilities** to meet the requirements and fill capability gaps to support DHS agencies in accomplishing their mission.
- Establish a lean and agile world-class S&T management team to deliver the technological advantage necessary to ensure DHS Agency mission success and prevent technological surprise.
- Provide leadership, research and educational opportunities and resources to develop the necessary intellectual basis to enable a national S&T workforce to secure the homeland.



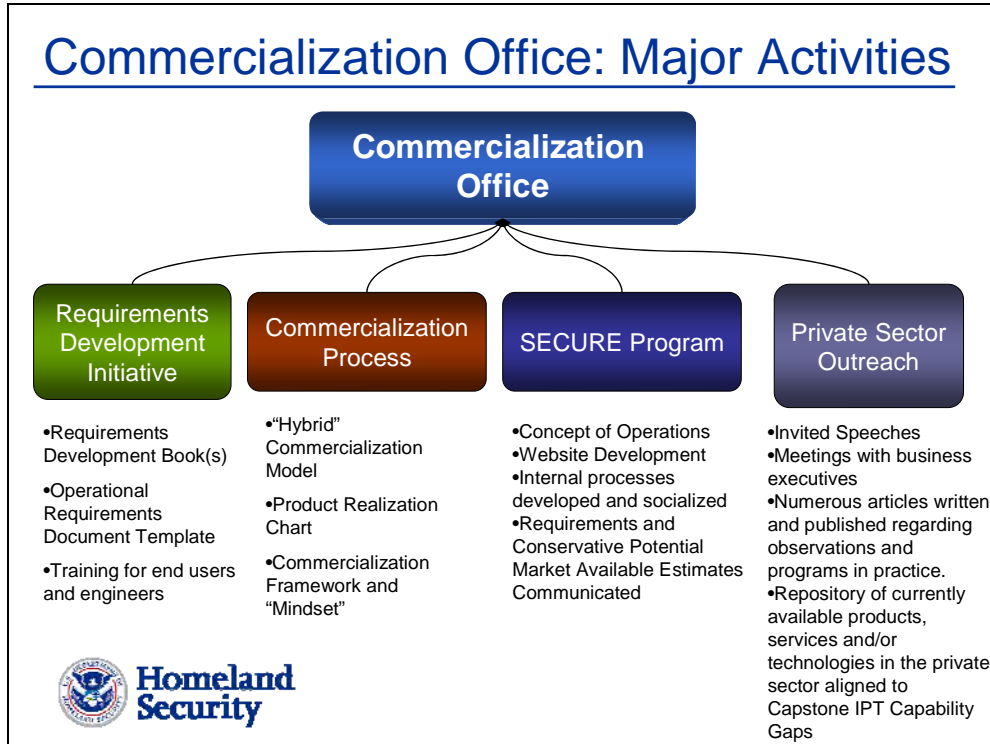
Slide 7



Slide 8



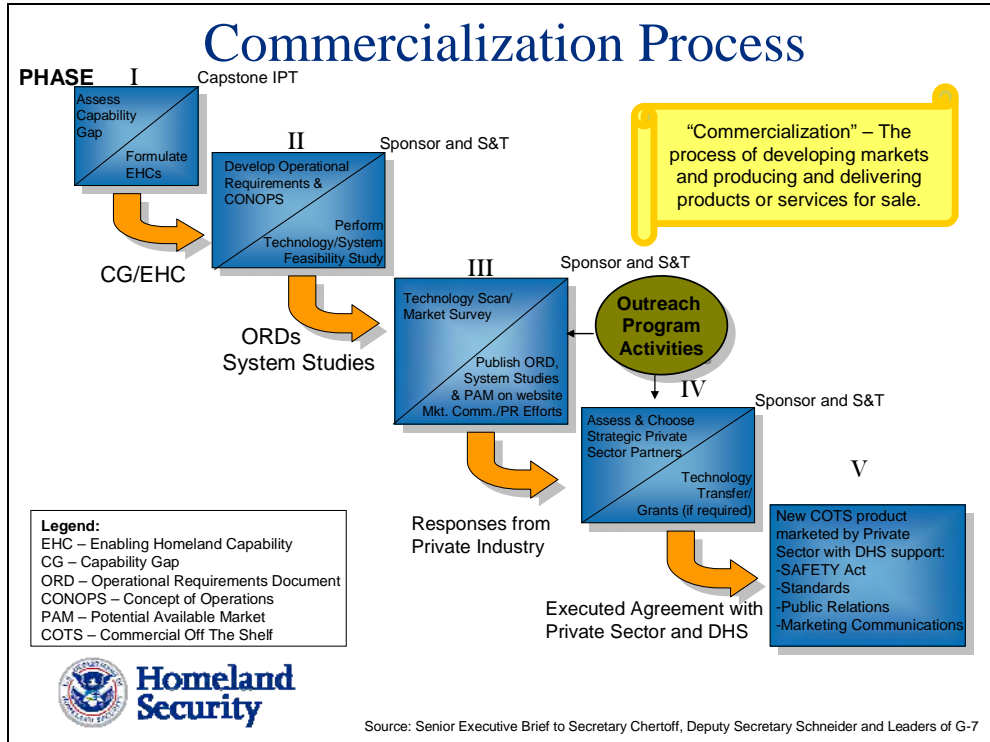
Slide 9



Slide 10



Slide 11



Slide 12

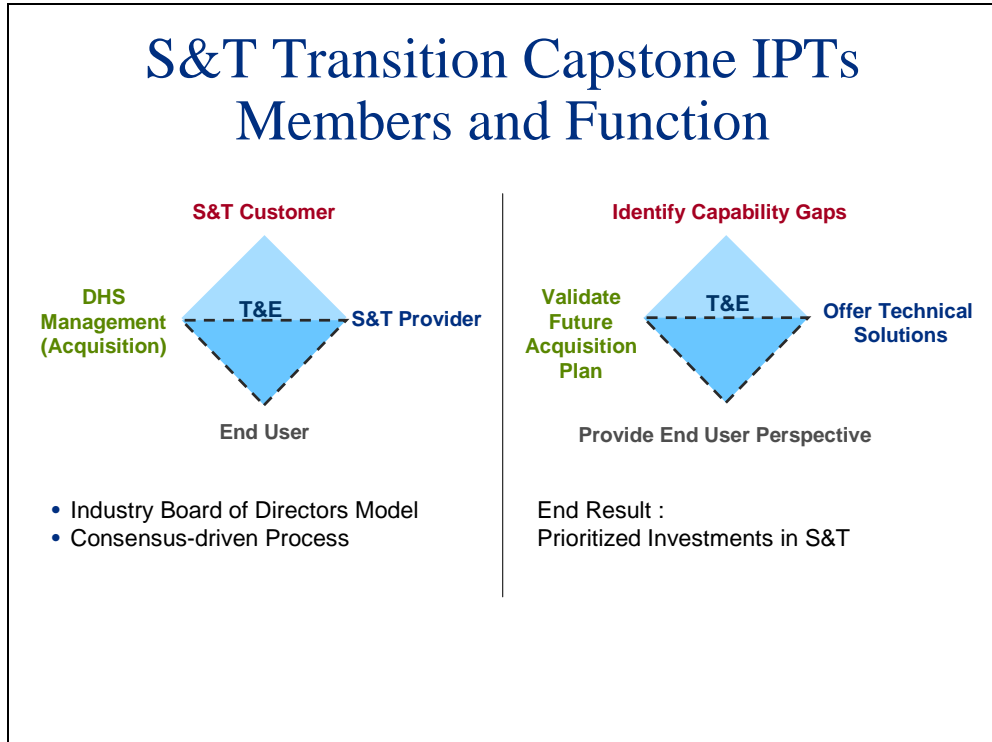
10 Reasons to Partner with DHS Science & Technology

Reasons Color Legend:

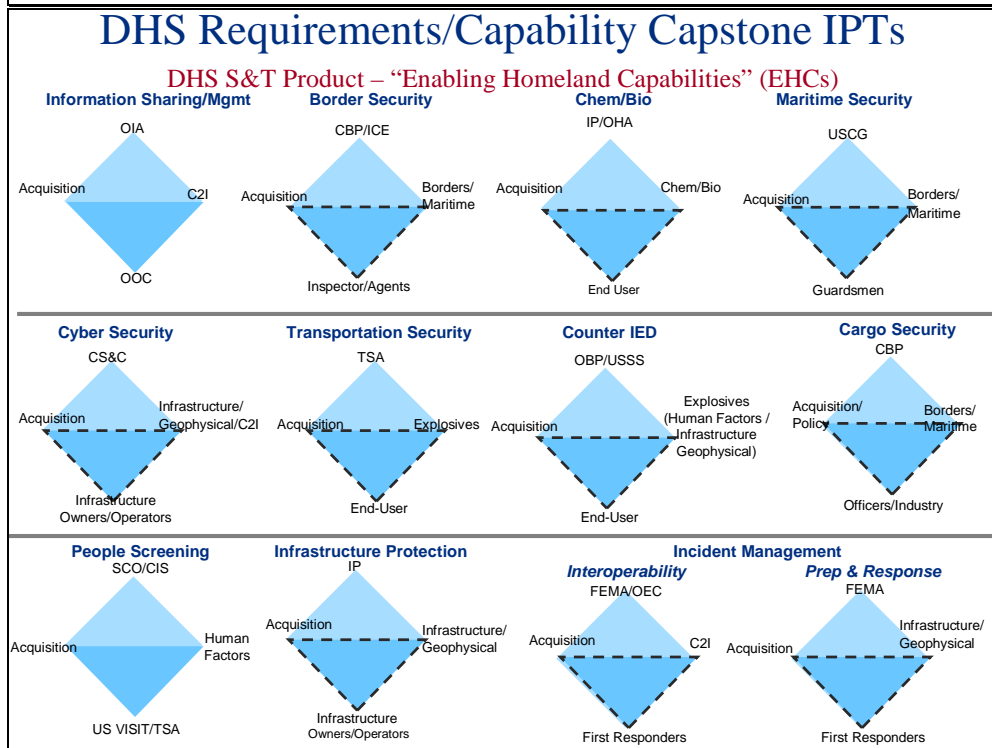
- Economics-based**
- Public Relations-based**
- Business Development-based**
- Strategic Marketing-based**
- Technical Resources-based**

1. **Access to Sizeable DHS Market and Ancillary Markets**
2. Leverage the Financial Strength/Stability of DHS and offset R&D costs through participation in mutually beneficial cost-sharing Programs
3. **Utilize the SAFETY Act to gain liability protection and access DHS' array of PR and Market Communications services**
4. **Effectively reach the First Responders Market through FEMA-sponsored grant programs, the AEL (Approved Equipment List), other sponsored equipment lists and fast-track programs**
5. Team with Science & Technology Personnel to leverage a vast Network of Laboratory Facilities for Technology and Product Development
6. **Gain access to Test and Evaluation (T&E) Facilities for Product Development and actively participate in the generation of Standards, T&E methods and Regulations used at the tribal, local, state, and federal levels**
7. **Meet and establish Partnerships with others in the University, Business, and National Lab Communities**
8. **Potentially generate Licensing revenue and capture potential Derivative Product revenue**
9. **Leverage SBIRs, HITS and HIPS to gain experience with homeland security applications**
10. **Make a Real Difference by Developing Products to Defend the Homeland for Generations to come as well as gain recognition as a Corporate Citizen contributing to the Security of our Homeland**

Slide 13



Slide 14



Cargo Security

Representative Technology Needs

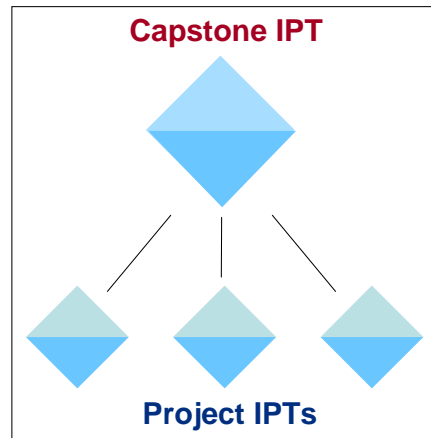


- Enhanced screening and examination by non-intrusive inspection
- Increased information fusion, anomaly detection, Automatic Target Recognition capability
- Detect and identify WMD materials and contraband
- Capability to screen 100% of air cargo
- Test the feasibility of seal security; detection of intrusion
- Track domestic high-threat cargo
- Harden air cargo conveyances and containers
- Positive ID of cargo and detection of intrusion or unauthorized access

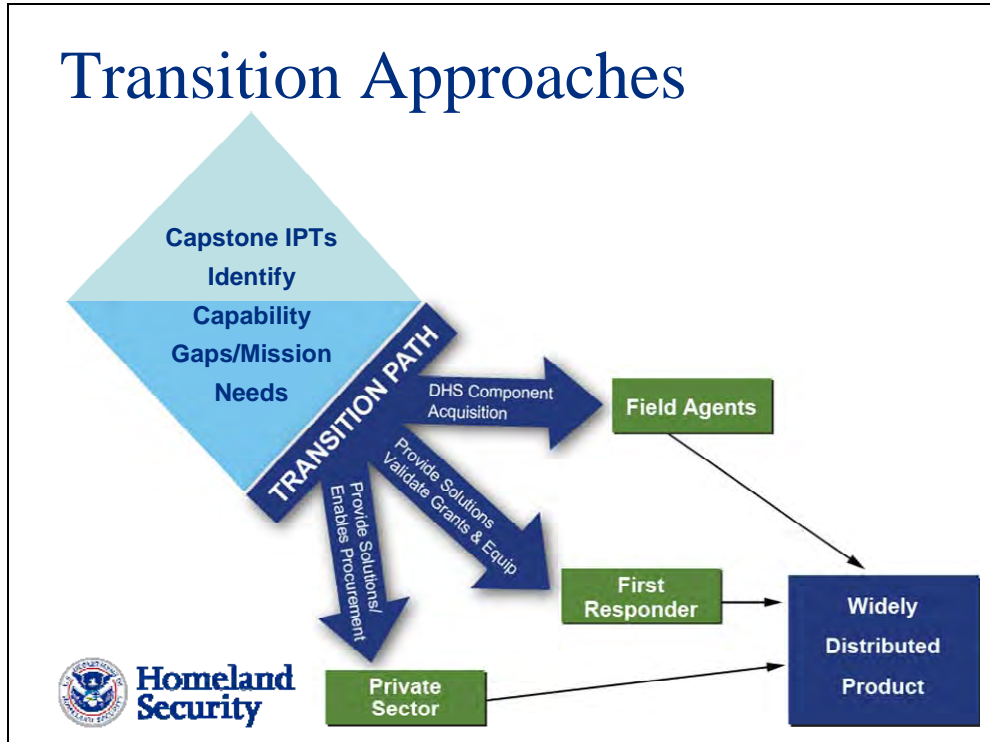
Source: S&T High Priority Technology Needs, May 2007

Establishment of Project IPTs: Detailed Specifications/Requirements

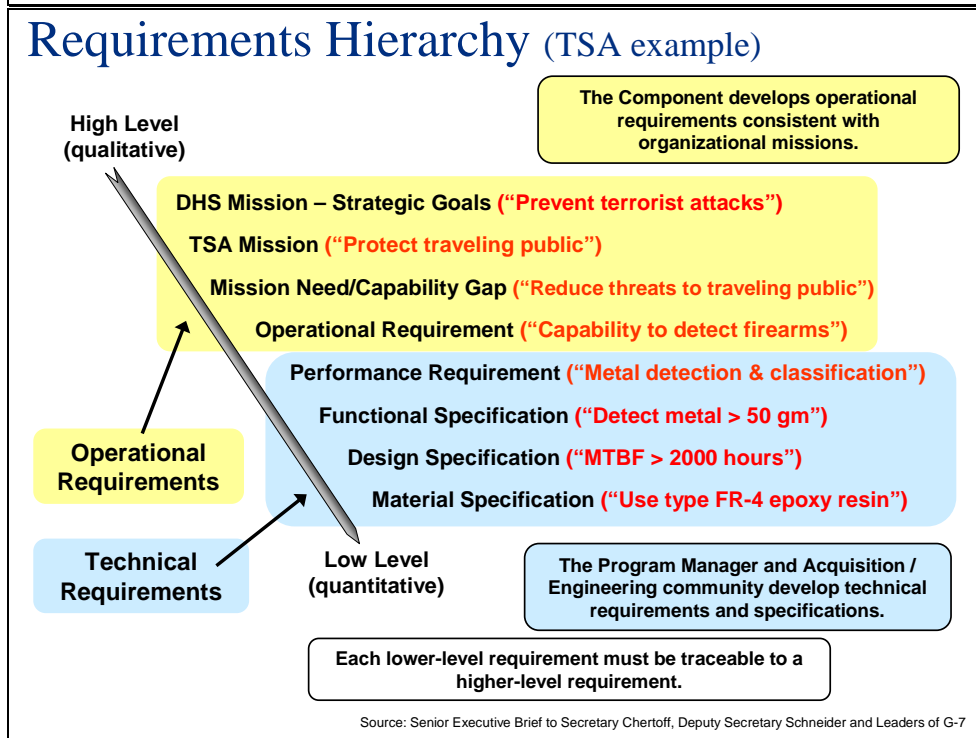
- Members:
 - S&T Program Manager(s)
 - Operating Component's Program Manager(s)
 - End-User(s)
 - Supplier/Provider
- Meet at Least Monthly
- Report to Capstone IPT Quarterly



Slide 17



Slide 18



ORD: Operational Requirements Document

What: ORDs provide a clear definition and articulation of a given problem.

How: Training materials have been developed to assist drafting an ORD.

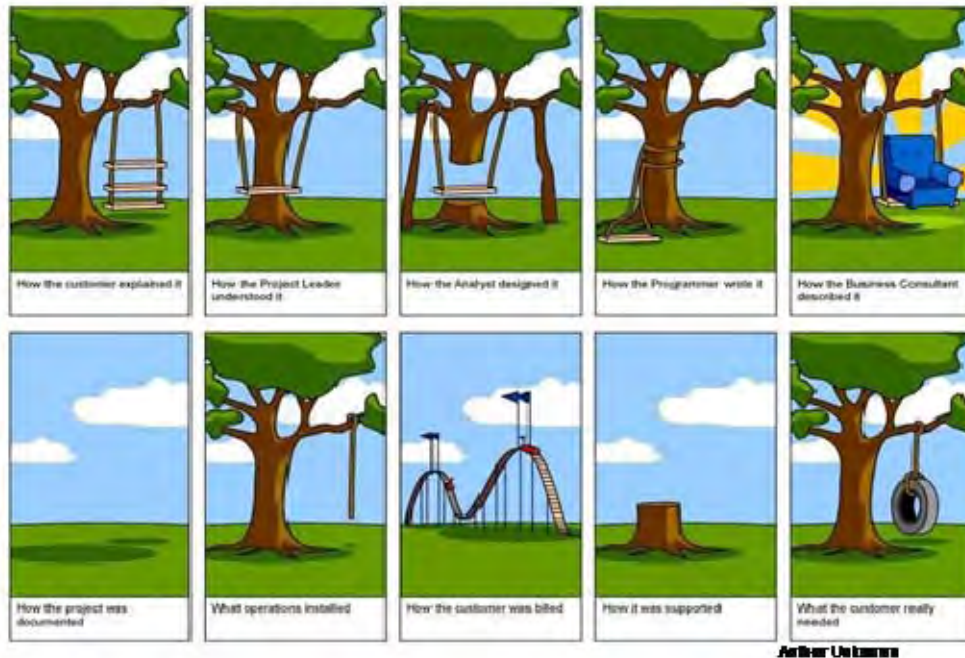
- *Developing Operational Requirements*, 194pp. Available online: http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf

When: For Use in Acquisition, Procurement, Commercialization and Outreach Programs –Any situation that dictates detailed requirements (e.g. RFQ, BAA, RFP, RFI, etc.)

Why: It's cost-effective and efficient for both DHS and all of its stakeholders.



Does this look familiar?!



Slide 21

Getting on the “Same Page”

- Historical Perspective
- Language is Key
- Communication is Paramount

Slide 22

Technology Readiness Levels (TRLs): Overview

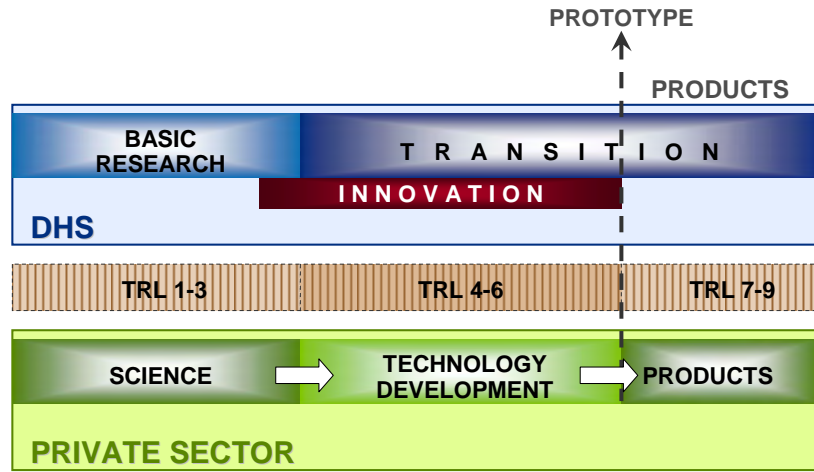
TRLs are NASA-generated and Used Extensively by DoD

Basic principles observed and reported	1	Basic
Technology concept and/or application formulated	2	
Analytical and experimental critical function and/or characteristic	3	
Component and/or breadboard validation in laboratory environment	4	Advanced
Component and/or breadboard validation in relevant environment	5	
System/subsystem model or prototype demonstration in a relevant environment	6	Applied
System prototype demonstration in a operational environment	7	
Actual system completed and 'flight qualified' through test and demonstration	8	
Actual system 'flight proven' through successful mission operations	9	

TECHNOLOGY MATURITY

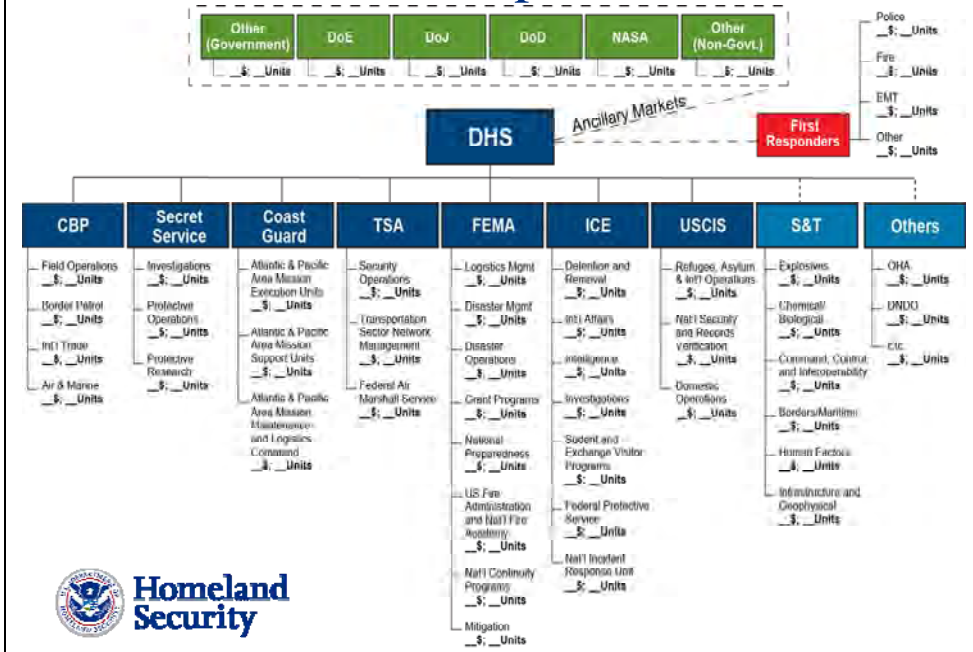
Slide 23

TRL Correlation: DHS and Private Sector



Slide 24

Market Potential Template



Slide 25

Conservative Estimate: Number of First Responders in the US

- Homeland Security Presidential Directive 8
- Steve Golubic (FEMA)

Total: > 25.3 Million Individuals

Front Line > 2.3 Million

Support to Front Line > 23 Million

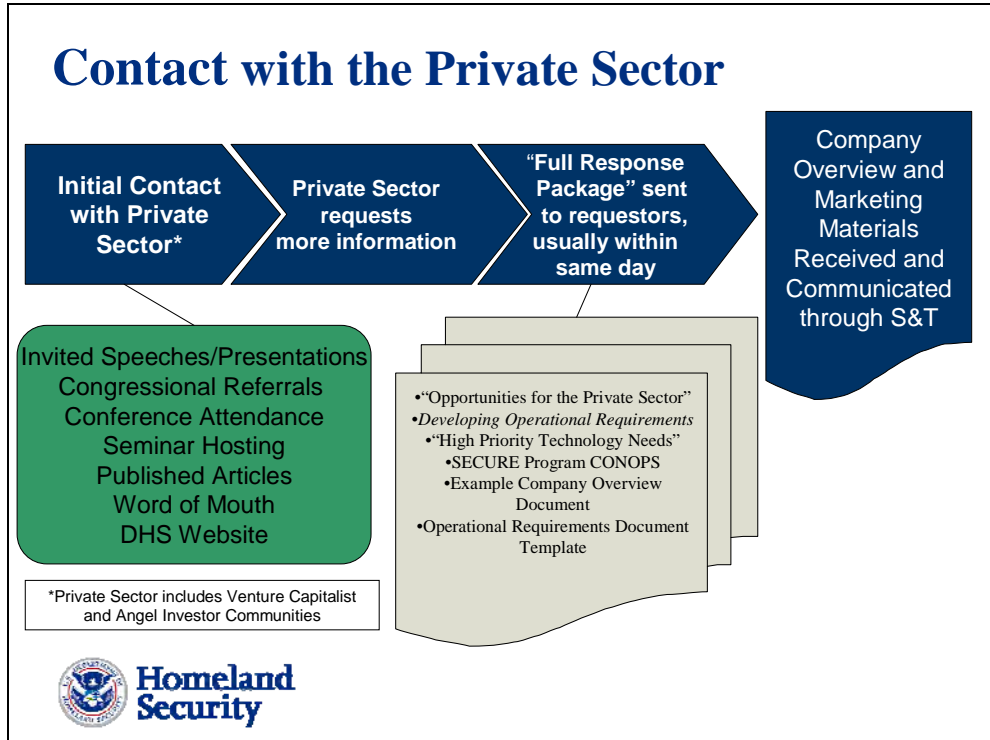
- Port Security
- Public Health
- Hospitals
- Transportation
- Emergency Management
- Clinics
- Venue Security
- Public Works/Utility
- School Security
- Response Volunteers

Slide 26

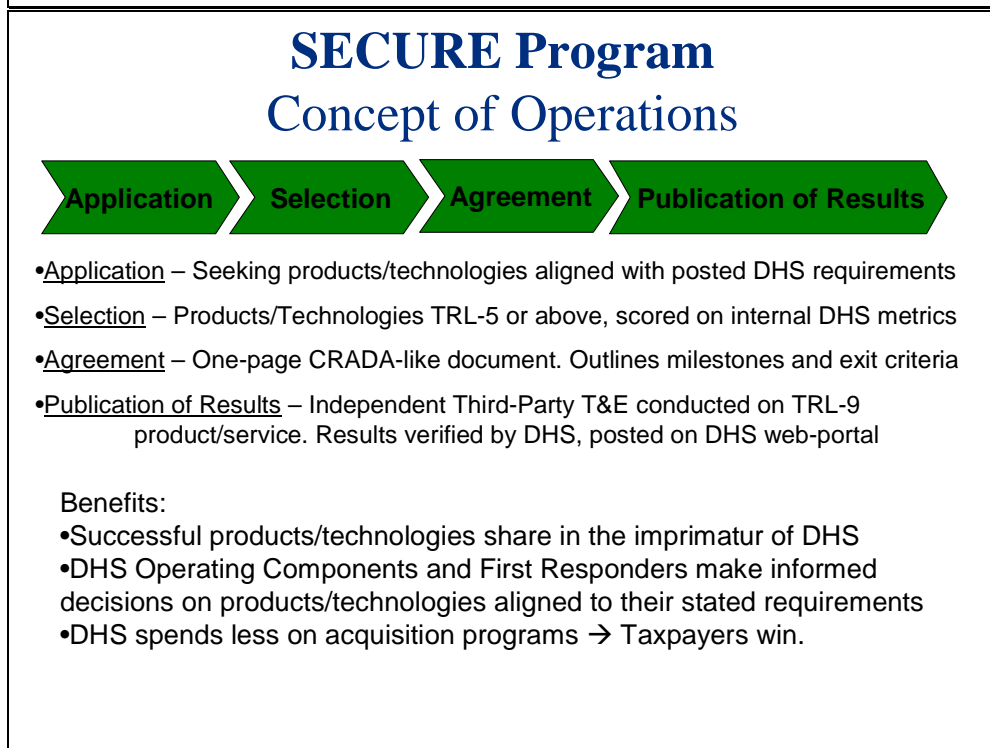
Call to Action: Mutual Benefits Create “Win-Win-Win” Relationships

- 1** Learn Current DHS Needs
Visit www.FedBizOpps.gov and www.hsarpabaa.com for current solicitations
- 2** Inform DHS of Products/Capabilities
Request DHS – S&T Full Response Package at thomas.cellucci@dhs.gov
- 3** Interact with DHS
Establish Mutually-beneficial Relationship

Slide 27



Slide 28



Slide 29

SECURE Program

Benefit Analysis “Win-Win-Win”

Taxpayers	Private Sector	Public Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Save significant time and money on market and business development activities	1. Improved understanding and communication of needs
2. Tax savings realized through Private Sector investment in DHS	2. Firms can genuinely contribute to the security of the Nation	2. Cost-effective and rapid product development process saves resources
3. Positive economic growth for American economy	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work	3. Monies can be allocated to perform greater number of essential tasks
4. Possible product “spin-offs” can aid other commercial markets	4. Significant business opportunities with sizeable DHS and DHS ancillary markets	4. End users receive products aligned to specific needs
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. Commercialization opportunities for small, medium and large business	5. End users can make informed purchasing decisions with tight budgets

Slide 30

The screenshot shows the DHS Open for Business website in a Microsoft Internet Explorer browser window. The address bar displays <http://www.dhs.gov/xopnbiz/>. The website header includes the Homeland Security logo and navigation tabs such as Home, Information Sharing & Analysis, Prevention & Protection, Preparedness & Response, Research, Commerce & Trade, Travel Security, and Immigration. The main content area features a sidebar with links for Grants, Contract Opportunities, Small Business Assistance, Policy and Regulations, and Events. The central content area is titled "Open For Business" and includes a "Spotlight" section with links to Information Technology Acquisitions, E-Verify Program, and a PDF document. Below this is a "Programs and Services" section with links to Acquisition Policies and Regulations, Opportunities, Small Business Procurement Assistance, Grants, Reports and Notices, and Forms. A "Resources" section at the bottom lists the SAFETY Act and System Efficacy through Commercialization, Utilization, Relevance and Evaluation (SECURE) Program. Two blue callout boxes with arrows point to the "Open for Business" header and the "SECURE Program" resource link.

Slide 31

Federal Business Opportunities

Sites where the Office of Procurement Operations (OPO) posts opportunities for prospective suppliers to offer solutions to DHS – S&T's needs:

- www.FedBizOpps.gov
- www.HSARPAbaa.com
- www.SBIR.dhs.gov
- www.Grants.gov

take advantage of...

- **Vendor Notification Service:** Sign up to receive procurement announcements and solicitations/BAA amendment releases, and general procurement announcements.
<http://www.fedbizopps.gov>
- **S&T's HSARPA website:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to Representative High Priority Technology Areas, where DHS areas of interest can be found.
<http://www.hsarpabaa.com>
- **Truly Innovative and Unique Solution:** Refer to Part 15.6 of the Federal Acquisition Regulation (FAR) which provides specific criteria that must be met before a unsolicited proposal can be submitted to Kathy Ferrell.
http://www.acquisition.gov/far/current/html/Subpart%2015_6.html

Contact Information:
Kathy Ferrell
Department of Homeland Security
Office of the Chief Procurement Officer
245 Murray Dr., Bldg. 410
Washington, DC 20528
unsolicited.proposal@dhs.gov
202-447-5576

Slide 32

Show Us the Difference...

Hall's Competitive Model

Differentiation ↑

↓ **Price** →

Differentiation = (A+B)C/(D+E)

As a function of:

- Market
- Application
- Technology

Slide 33



Slide 34

SAFETY Act

Support Anti-Terrorism by Fostering Effective Technologies Act of 2002

- Enables the development and deployment of qualified anti-terrorism technologies
- Provides important legal liability protections for manufacturers and sellers of effective technologies
- Removes barriers to industry investments in new and unique technologies
- Creates market incentives for industry to invest in measures to enhance our homeland security
- The SAFETY Act liability protections apply to a vast range of technologies, including:
 - Products
 - Services
 - Software and other forms of intellectual property (IP)

Examples of eligible technologies:

- Threat and vulnerability assessment services
- Detection Systems
- Blast Mitigation Materials
- Screening Services
- Sensors and Sensor Integration
- Vaccines
- Metal Detectors
- Decision Support Software
- Security Services
- Data Mining Software

Protecting You, Protecting U.S.

Criteria as stated in the SAFETY Act

- Is it an Anti-Terrorism Technology?
- Is it effective and available?
- Does it possess large potential third party liability risk exposure?
- Does Seller need SAFETY Act?
- Does it perform as intended?
- Does it conform to Seller's specifications?
- Is it safe for use as intended?

Addition SAFETY Act information...

Online: www.safetyact.gov Email: helpdesk@safetyact.gov

Toll-Free: 1-866-788-9318

Award Criteria

	Developmental Testing and Evaluation (DT&E)	Designation	Certification
Effectiveness Evaluation Conclusion	Needs more proof, has potential	Demonstrated effectiveness, i.e. Developmental testing (with confidence of repeatability)	Consistently proven effectiveness, i.e. operational performance (with high confidence of enduring effectiveness)
Protection	Liability cap <ul style="list-style-type: none"> • only for identified test event(s) and for limited duration (=3yrs) 	Liability cap <ul style="list-style-type: none"> • for any and all deployments in 5-8 year term 	Government Contractor Defense (GCD) <ul style="list-style-type: none"> • for any and all deployments in 5-8 years term
Examples	<ul style="list-style-type: none"> • EDS not yet TSL Certified • Novel incident pattern matching service 	<ul style="list-style-type: none"> • Radiological detector with <u>laboratory</u> success Opt-out screeners, only similar projects completed 	<ul style="list-style-type: none"> • EDS TSL Certified • Well-documented infrastructure protection service with history of excellent performance and meeting DoE standards

EDS=Explosive Detection System TSL=Transportation Security Laboratory (TSA)

Slide 37



Slide 38

Tech Clearinghouse Mission

To rapidly disseminate technical information concerning existing and desired products and services to/between Federal, State, Local, and Tribal Government and the Private Sector in order to encourage technological innovation and facilitate the mission of the Department of Homeland Security.

- Establishes Central Federal Technology Clearinghouse
- Issues Announcements for Innovative Solutions
- Establishes S&T Technical Assessment Team
- Provides guidance for the evaluation, purchase, and implementation of homeland security enhancing technologies
- Provides users with information to develop or deploy technologies that would enhance homeland security
- Enables technology transfer

Improved Knowledge Sound Acquisition Decisions

TechSolutions

The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders

- Field prototypical solutions in 12 months
- Cost should be commensurate with proposal but less than \$1M per project
- Solution should meet 80% of identified requirements
- Provide a mechanism for Emergency Responders to relay their capability gaps
 - Capability gaps are gathered using a web site (www.dhs.gov/techsolutions)
- Gaps are addressed using existing technology, spiral development, and rapid prototyping
- Emergency Responders partner with DHS from start to finish

Rapid Technology Development
Target: Solutions Fielded within 1 year, at <\$1M

TechSolutions Investments

Seatbelt Safety for
Emergency Vehicles



Next Generation
Breathing Apparatus



Fire Ground Compass



----- Under Consideration -----

Vehicle Mounted Chem/Bio
Sensor Detection



Slide 41

Getting Involved: S&T Contacts

Division	Email
Jim Tuttle	S&T-Explosives@dhs.gov
Beth George	S&T-ChemBio@dhs.gov
David Boyd	S&T-C2I@dhs.gov
Anh Duong	S&T-BordersMaritime@dhs.gov
Sharla Rausch	S&T-HumanFactors@dhs.gov
Chris Doyle	S&T-InfrastructureGeophysical@dhs.gov
Rich Kikla	S&T-Transition@dhs.gov
Starnes Walker	S&T-Research@dhs.gov
Roger McGinnis	S&T-Innovation@dhs.gov

Slide 42

Summary

Detailed Requirements
Sizeable Market Potential
Delivered Products – PERIOD!

How Can You Afford NOT to Partner with DHS S&T?


Questions/Comments:
Thomas A. Cellucci, Ph.D., MBA
thomas.cellucci@dhs.gov



Appendix G: Capability Gap-Based Thinking

The following slides were prepared by Dr. Arch Turner of DHS S&T and discuss capability gap driven thinking and processes.


Slide 1



Homeland Security Capabilities

Arch Turner, Ph.D.
U. S. Department of Homeland Security
Science & Technology Directorate
Operations Analysis Division
12 November, 2008


Slide 2



Purpose

Discuss Capabilities-Based Thinking for
Defining, Developing, and Fielding Homeland
Security Needs

Slide 3

 **Homeland Security**

Capabilities in Department of Homeland Security (DHS)

DHS Strategic Requirements Planning Process “Foundational Principle 1”:
“Requirements will be described in terms of **operational capability**¹ need”

DHS Strategic Planning Process: “Through its recurring strategic planning process, the Department identifies **capabilities** needed across components to accomplish its strategic objectives”

DHS S&T Mission: “To conduct, stimulate and enable research, development, test, evaluation, and timely **transition of homeland security capabilities** to Federal, State, and Local operational end-users”


DHS S&T Strategy: “The S&T Directorate is committed to being customer focused and to **delivering capabilities** that DHS Components can rely on to meet their operational needs.”

DHS S&T Capstone IPTs: “Will identify, validate, and prioritize **capability requirements** for S&T Directorate customers”

DHS Has Operational Capability Focus

Note: 1. All emphases (bold) added.

Slide 4

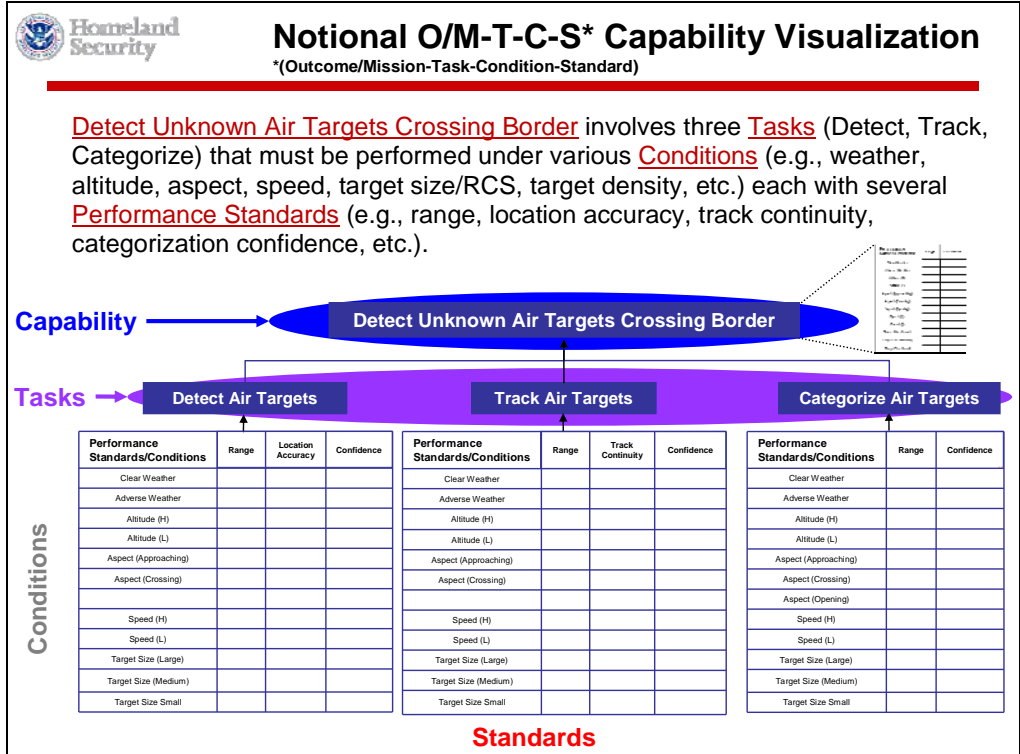
 **Homeland Security**

Capability Definition/Capability Construct

- **What Is A “Capability”?**
 - “means To Accomplish A Mission And Achieve Desired Outcomes By Performing Critical Tasks, Under Specified Conditions, To Target Levels Of Performance” (DHS, TCL² 2, Sept., 2007)
- **Capabilities Can Be Defined In Terms Of**
 - **Outcome/Mission** → What Needs To Be Achieved
 - **Tasks** → Actions That Must Be Accomplished To Achieve Outcome/Mission
 - **Conditions** → Circumstances Under Which Mission/Tasks Must Be Achieved And Which Can Affect Performance
 - **Standards** → Performance Levels To Which Mission/Tasks Must Be Completed For Outcome/Mission To Be Considered Successfully Achieved (E.G., Time, Affordability, Ease/Difficulty, Etc.)

We Need Common Terminology & Understanding

Note 2. Target Capabilities List



Capability-Based Planning (C-BP)


Capability-Based Planning

“planning under uncertainty to provide capabilities for a wide range of modern-day challenges and circumstances while working within an economic framework that necessitates choice” (Davis, Analytic Architecture for Capabilities-Based Planning, RAND)

“involves a functional analysis of operational requirements.capabilities are identified based on tasks required...” (NATO Handbook in Long Term Defense Planning)

U.S./Close Ally Defense Institutions Have Embraced C-BP To Deal With Uncertainty of 21st Century Security Environment


Slide 7



C-BP “Building Blocks”


- High Level Capability Objectives Derived from Top Level Government Guidance
- Understanding Of How Organization Will Operate - Top Level Doctrine Or Overarching Operational Concept
- Capability Assessment In Context Of Multiple Plausible But Uncertain Futures/Scenarios
- Resource Constraint Requiring Tradeoffs in Definition/ Prioritization of Capabilities

Slide 8



Characteristics of C-BP


- **Outcome Oriented**
 - Focused On Ability To Perform Assigned Missions
 - “What Do We Need To Do?” Not “What Do We Have Or Need To Replace?”
- **Holistic**
 - Explicit Recognition/Consideration Of Interdependence Of Material Resources, People, Doctrine, Organization, Support In Capability In Performing Mission
 - Emphasis On Cost, Performance, Risk Tradeoffs Among Resources Comprising Capabilities
- **Cross-Organization Focus**
 - Helps Break Down Stovepipes
 - Reveal Redundant/Excess Capacity
- **Encourages Innovation**
 - Avoids Identifying Solutions Early In Process, Keeps Options Open
 - Opens Door To New Ideas - “Overcome Simply Replacing Platforms”



Characteristics of C-BP (2)

- **Hedges Against Uncertainty**
 - Contrast With “*Threat Based Planning*” A “Red Herring”
 - Capabilities Tested Against Multiple Diverse Scenarios/Time Frames
 - Does Not Focus On “Bounding Threat” Of One/Few Scenarios
 - Stressing Scenarios Context For Identifying Tasks Most Critical To Achieving Desired Outcomes/End States Across Scenario Spectrum
- **Product**
 - Robust, Adaptable, Flexible And Affordable Capability Set
 - Set Best Suited Across Multiple Plausible, Uncertain Futures

“Nothing New” - Eliminates Cold War Practice Of Focusing On Single/Few Well-Defined “Bounding Threats” (Paul Davis, RAND)




Capability Definition & Capability Construct

Capability - “means to accomplish a mission and achieve desired outcomes by performing critical tasks, under specified conditions, to target levels of performance” (DHS, TCL 2, Sept., 2007)

- **Capabilities Defined By O/M-T-C-S Construct**
 - **Outcome/Mission** → What do we need to achieve?
 - **Tasks** → What actions must be accomplished to achieve outcome/mission?
 - **Conditions** → What are the operational circumstances under which mission/tasks must be performed and which can affect performance?
 - **Standards** → How well must we be able to perform mission/tasks under these conditions for outcome/mission to be successfully achieved?

Operational Outcome/Mission – Not Process – Oriented




Second Essential Way of Looking At Capabilities

Capabilities must also be considered from resource perspective

- “Combination of resources (people, equipment, and other elements) that provide a means to achieve an outcome, under specified conditions and to national standards” (DHS ODP³ Concept Paper, 2004)
- “Capability elements define the resources required to perform the critical tasks to the specified levels of performance” (DHS, TCL, Sept., 2006)
- “Capability elements serve as a guide for identifying and prioritizing investments when working to establish a capability” (DHS, TCL, Sept., 2007)
- “There is rarely a single combination of capability elements that can be used to achieve a capability” (DHS, TCL, Sept., 2006)

Capabilities Defined By O/M-T-C-S And By Resources Needed To Constitute & Apply Them

Note 3. Office of Domestic Preparedness




DHS Operational Capability Elements (OCE)

- DHS OCE From HSPD-8 National Preparedness Guidelines

DHS Operational Capability Elements (DHS, Target Capabilities List 2, September, 2007)	
Planning	Collection and analysis of intelligence and information, and development of policies, plans, procedures, mutual aid agreements, strategies, and other publications that comply with relevant laws, regulations, and guidance necessary to perform assigned missions and tasks.
Organization & Leadership	Individual teams, an overall organizational structure, and leadership at each level in the structure that comply with relevant laws, regulations, and guidance necessary to perform assigned missions and tasks
Personnel	Paid and volunteer staff who meet relevant qualification and certification standards necessary to perform assigned missions and tasks
Equipment & Systems	Major items of equipment, supplies, facilities, and systems that comply with relevant standards necessary to perform assigned missions and tasks
Training	Content and methods of delivery that comply with relevant training standards necessary to perform assigned missions and tasks
Exercises, Evaluations, and Corrective Actions	Exercises, self-assessments, peer assessments, outside review, compliance monitoring, and actual major events that provide opportunities to demonstrate, evaluate, and improve combined capability and interoperability of the other elements to perform assigned missions and tasks to standards necessary to achieve successful outcomes.

- Analogous to DOD DOTMLPF Capability Element Construct

Capability = Planning + Organization/Leadership + People + Equipment/Systems + Training + Exercises/Evaluations



Capabilities Must Be Complete

(Lt. Gen. (Ret.) George Mac Donald, Canadian Defence Staff Vice Chief, 2001-2004, Testimony to Standing Committee on National Defence, 13 Feb., 2007)

"I should add an aside at this point to be clear about what I mean by a capability.

Too often the assumption is made that the purchase and delivery of capital equipment constitutes a new capability, where in fact it is usually only the first step, and often not even the most expensive portion.

To provide a complete, balanced capability, personnel must be available and they need to be properly trained and supervised.


Operating concepts need to be put in place and access to robust command and control must be assured.

Infrastructure – both buildings and information technology – must be accounted for.

Also, it is critical to ensure that the necessary support services for spares, maintenance, repair and overhaul are provided for the long term.

In short, ***capabilities must be complete to be useful.***" (Emphasis added)

Avoid Becoming Overly Focused On “Guns, Guards, Gates, Gadgets & Gizmos” (i.e. “Things”) → Outcome Is The Key



Capability Gaps

- **Capability Gap: Mismatch Between What We Need To Be Able To Do And What We Can Currently Do**
 - Discrepancy Between Required Capability and Current Capability
 - Can Be Either a Capability Excess or a Shortfall
 - Both Important - Focus Here on Capability Shortfalls

- **What Are Attributes of “Good” – i.e. “Actionable” - Capability Gap Statement**
 - √ Specifies Required Outcome(s)/Mission(s) Presently Not Achievable
 - √ Specifies Required Tasks/Conditions/Standards Combinations Which Cannot Presently Be Achieved
 - √ Is “Solution Agnostic” – Specifies “What” needs to be done, Not “How” it needs to be done (i.e., A “Problem” not a “Solution”)

What DHS Operators Need To Be Able To Do to Perform Mission, But Can't. How Well? Under What Conditions?

Homeland Security

Capability Gap Statements Compared

Poor Initial Capability Gap Statement:
 "Need New Border Air Surveillance Radar"

- × Not Outcome/Mission Oriented
- × No Condition/Performance Standard Information
- × Not Solution Agnostic

More Actionable Initial Capability Gap Statement:
 "Need ability to reliably (≥.95 Confidence) categorize approaching/closing (≥ = 25 nm. range, slow (≤100 knots), low-flying (500 - 2,500 feet altitude), unknown small (light plane sized) air contacts in adverse weather conditions from site located in benign terrain"

- ✓ Identifies Specifically What User Needs To Be Able To Do But Can't
- ✓ Provides Some Key Condition/Performance Standard Information
- ✓ Solution Agnostic

Accurate/Precise Capability Gap Statement More Likely To Be Filled Sooner, Correctly, More Affordably

Homeland Security

Notional O/M-T-C-S Capability Gap Visualization

Detect Unknown Targets Crossing Border

Detect Air Targets

Performance Metrics/Conditions	Range	Location Accuracy	Confidence
Clear Weather	✓	✓	✓
Adverse Weather	✓	✓	✓
Altitude (H)	✓	✓	✓
Altitude (L)	✓	✓	✓
Aspect (Approaching)	✓	✓	✓
Aspect (Crossing)	✓	✓	✓
Aspect (Opening)	✓	✓	✓
Speed (H)	✓	✓	✓
Speed (L)	✓	✓	✓
Target Size (Large)	✓	✓	✓
Target Size (Medium)	✓	✓	✓
Target Size Small	✓	✓	✓

Track Air Targets

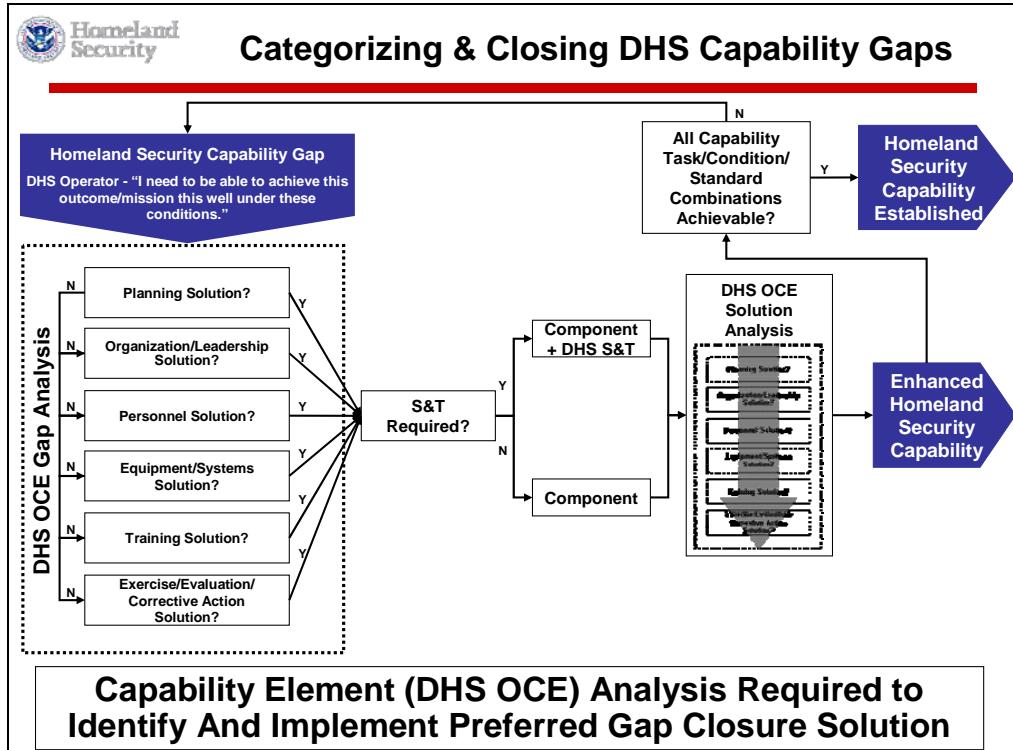
Performance Metrics/Conditions	Range	Track Continuity	Confidence
Clear Weather	✓	✓	✓
Adverse Weather	✓	✓	✓
Altitude (H)	✓	✓	✓
Altitude (L)	✓	✓	✓
Aspect (Approaching)	✓	✓	✓
Aspect (Crossing)	✓	✓	✓
Aspect (Opening)	✓	✓	✓
Speed (H)	✓	✓	✓
Speed (L)	✓	✓	✓
Target Size (Large)	✓	✓	✓
Target Size (Medium)	✓	✓	✓
Target Size Small	✓	✓	✓

Categorize Air Targets

Performance Metrics/Conditions	Range	Confidence
Clear Weather	✓	✓
Adverse Weather	✗	✗
Altitude (H)	✓	✓
Altitude (L)	✓	✗
Aspect (Approaching)	✓	✗
Aspect (Crossing)	✓	✓
Aspect (Opening)	✓	✓
Speed (H)	✓	✓
Speed (L)	✓	✗
Target Size (Large)	✓	✓
Target Size (Medium)	✓	✓
Target Size Small	✓	✗


Legend: ✓ Can achieve performance standard in condition ✗ Cannot achieve performance standard in condition
 Green: "Current Capability" Red: "Capability Gap"

More Specific Statement Of Need Enables Solution Providers To Focus Quickly On What Needs To Be "Fixed"



-
- Homeland Security**
- ### DHS Strategic Requirements Planning Process
- Management Directorate/Office of Policy initiative
 - Important element of over arching PPBE process
 - Requirements Generation + Programming + Acquisition → DHS PPBE
 - Embodies Key C-BP precepts
 - Flows from 5 DHS Strategic Goals
 - Identifies 7 DHS "Functional Requirement Areas" (FRA)
 - First Foundational Principle: "Requirements" must be described "in terms of strategic capabilities"
 - Deputy Secretary chaired Joint Requirements Council
 - Multi-discipline Requirements Planning Teams review selected FRA "Areas of Interest"
 - **Capability-Objectives-Resources-Evaluative Measures (CORE) Document** Capability Mismatches
 - Embraces integrated capability resource perspective (DOTMLPF RAGS)
 - Primary Input to DHS Integrated Planning Guidance


Slide 19



DHS Strategic Requirements Planning Process

- DHS Strategic Goals
 - Protect U.S. from Dangerous People
 - Protect U.S. from Dangerous Goods
 - Protect Critical Infrastructure
 - Build Effective Emergency Response System & Culture of Preparedness
 - Strengthen & Unify DHS Operations Management
- DHS Functional Areas
 - Screening (e.g., Cargo and People)
 - Securing (e.g., Critical Infrastructure)
 - Law Enforcement (e.g., Investigations, Immigration)
 - Domain Awareness (e.g., Border Surveillance)
 - Benefits Administration (e.g., FEMA, USCIS benefits)
 - Incident Management (e.g., Hurricane, Terrorist Attack)
 - Enterprise Operations (e.g., Operations Integration)

Slide 20



Closing Thoughts

- Capability-Based Planning A Strategy For Dealing With Uncertain Threat In Resource-Constrained Environment
- Common Capability/Gap Understanding And Terminology Important
- Capabilities Can Be Characterized Using Outcome/Mission-Task-Conditions-Standards Construct (O/M -T-C-S)
- Capabilities Can Also Be Characterized In Terms Of Capability Elements – Resources Needed To Realize Them – Which Must Be Considered When Classifying Gaps And Designing/Fielding Solutions
- Important To Think Of Capabilities And Gaps With Both O/M-T-C-S And Capability Element/Resource Perspectives In Mind
- DHS Office of Policy/Management Directorate Providing Important Leadership Toward Institutionalizing Capability-Based Thinking And Planning

Appendix H: Product Realization Chart

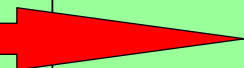


U.S. Department of Homeland Security: Commercialization Office

Product Realization Chart

DHS S&T Portfolio	N/A		Basic Research				Innovation and Transition				
Technology Phase	Needs Assessment		Science				Technology Development		Product Development		
Technology Readiness Level (TRL)	N/A		TRL 1 - TRL 3		TRL 4 - TRL 6		TRL 7 - TRL 9				
Key Objectives	<ul style="list-style-type: none"> Identify S&T capability gaps (mission needs) requiring material solutions. Preliminary operational requirements are developed. Market survey. Technology scan. Assess technology-based solutions to address gaps. Develop rough order-of-magnitude (ROM) estimates of project cost and schedule. Investigate the value proposition of a product idea. Establish technical objectives and milestones. Conduct preliminary IP review. Ensure the qualification of tools, materials, processes, and suppliers as required. Provide a preliminary production plan. Develop preliminary marketing objectives and milestones. Inclusion of Congressional Appropriations Memo, Technology Transition Agreements (TTA), Program Descriptions (Research and Innovation), and Feasibility Studies lead to Program and Budget Execution. List other objectives when defined. 	<p>TRL 1</p> <ul style="list-style-type: none"> A program sponsor and end-users / customers have been identified. Mission Needs Statement has been developed. Communication with end-users and customers has been initiated. Preliminary operational requirements have been defined. Program Management Vision has been developed. A Feasibility Study White Paper has been developed and accepted. (TRL 1 and 2) A threat, vulnerability, or gap has been identified. Initial risks have been identified. Develop and update the preliminary product plan. List other objectives when defined. 	<p>TRL 2</p> <ul style="list-style-type: none"> End-user is involved in concept and requirements development. An empirical or theoretical design solution has been identified. Analytical studies to confirm the basic principles of the technology have been conducted. Operational requirements analysis has been completed. Operational requirements are applied to Functional Requirements. (TRL 2 and 3) System concept(s) / architecture have been assessed. Program Risk Assessment has been conducted. Risk Management Plan has been developed. (TRL 2 and 3) Program Cost Analysis has been completed and updated. (TRL 2 and 3) Preliminary Security Assessment has been conducted. Develop a Technology Roadmap. Refine the market assessment and technology scan. List other objectives when defined. 	<p>TRL 3</p> <ul style="list-style-type: none"> Supplemental and alternate technologies throughout DHS S&T have been surveyed. Technology's physical validity has been proven in laboratory experiments. Program Management Plan (PMP) has been developed. Systems Engineering Management Plan (SEMP) draft. Proof of Concept Plan has been developed. Manufacturing / production strategy has been developed. Develop Quality Control Plan to include standards conformance, reliability testing, etc. Develop Marketing Plan to include market size and research. List other objectives when defined. 	<p>TRL 4</p> <ul style="list-style-type: none"> All required technology components are integrated for Proof of Concept. Proof of Concept is conducted. IP has been briefed on progress of the technology's development. The customer has been briefed on the Proof of Concept results. Functional Requirements Document has been finalized. SEMP has been finalized and updated. (TRL 4, 5, & 6) TEMP has been completed and updated. (TRL 4, 5, & 6) Risk Management Plan is updated. (TRL 4, 5, and 6) Program Cost Analysis is updated. (TRL 4, 5, and 6) Quality Assurance Plan exists. Program Transition Manager is engaged in transition planning. List other objectives when defined. 	<p>TRL 5</p> <ul style="list-style-type: none"> ORD and CONOPs are developed. Security Assessment is updated. OMB 300 and Acquisition Plan have been completed (if required). IP has certified readiness for the transition of the Technology. Program Transition Manager has assisted in transition documentation development. Technology scan and market survey. (ongoing) Analysis of Alternatives is completed and updated. (TRL 5 & 6) Entry Criteria Checklist is developed and delivered to the TM. POD has been created, approved, and signed. (TRL 5 & 6) Director has approved the transition. List other objectives when defined. 	<p>TRL 6</p> <p>Germane to both Acquisition and Commercialization</p> <ul style="list-style-type: none"> Execute a preliminary Technology Transition Agreement (TTA), or Technology Commercialization Agreement (TCA) as applicable. Program Manager has been identified. Successful TAE in a simulated operational environment has been conducted. End-user / customer has been briefed on the results of T&E. Initial Security Guidelines have been developed. Draft Program Assessment Rating Tool (PART) plan exists, if required. National Environmental Policy Act (NEPA) plan / assessment, if required. Interoperability Assessment. List other objectives when defined. <p>Specific to Commercialization</p> <ul style="list-style-type: none"> Finalize Manufacturing Plan. Finalize engineering documentation. Develop and implement a test plan for quality control. List other objectives when defined. 	<p>TRL 7</p> <p>Germane to both Acquisition and Commercialization</p> <ul style="list-style-type: none"> S&T and the end-user / customer have begun to develop final transition planning document. Transition Plan has been developed. (TRL 7 and 8) Technology has been successfully demonstrated in an operational environment. (TRL 7 and 8) Updates (if required) have been made to the Operational and / or Functional Requirements Document. Risk Management Plan, Program Cost Analysis and PMP have been updated (as needed). Strategic Program Planning (e.g. Balanced Scorecard) has been conducted. Operations and Maintenance Manual has been completed / updated. Security Manual has been developed. Interoperability has been demonstrated. Management Directives (MD) have been reviewed to assure compliance. List other objectives when defined. <p>Specific to Commercialization</p> <ul style="list-style-type: none"> IP Protection and Licensing. Finalize sales release package. Verify and update quality control requirements. List other objectives when defined. 	<p>TRL 8</p> <p>Germane to both Acquisition and Commercialization</p> <ul style="list-style-type: none"> Technology components are form, fit, and function compatible with an operational system. Technology production has been addressed and planned by DHS and the end-user / customer. Training Plan has been developed and implemented. (TRL 8 and 9) Operational Test Report has been completed. Limited User Test (LUT) Plan has been developed. List other objectives when defined. <p>Specific to Commercialization</p> <ul style="list-style-type: none"> IP Protection and Licensing. Finalize product plan sales release package (to be distributed). Finalize manufacturing and assembly routines. List other objectives when defined. 	<p>TRL 9</p> <p>Germane to both Acquisition and Commercialization</p> <ul style="list-style-type: none"> All critical program documentation has been completed. Planning is underway for the integration of the next generation technology into the existing program components. End-user fully demonstrates the technology in CONOPS. Lessons Learned completed. After Action Review completed. Support Plan is completed. List other objectives when defined. <p>Specific to Commercialization</p> <ul style="list-style-type: none"> Finalize quality plan. Finalize marketing plan. Finalize manufacturing and assembly routines. List other objectives when defined. 	
		Key Deliverables	<ul style="list-style-type: none"> Preliminary market assessment and technology scan. Congressional Appropriations Memo, Technology Transition Agreements, Program Descriptions (Research and Innovation), and Feasibility Studies lead to Program and Budget Execution. Preliminary product plan that assesses features, benefits, and risk. Initial plan for marketing, production, and supply control. List other deliverables when defined. 	<ul style="list-style-type: none"> Mission Needs Statement. Feasibility Study. Program Management Vision, or Description of Leap-ahead Capability. Written report of findings and recommendations (preliminary product plan). Feasibility Review meeting. List other deliverables when defined. 	<ul style="list-style-type: none"> Preliminary Operational Requirements Document (end-user / customer validation). Program Cost Analysis (updated). (TRL 2 and 3) Program Management Plan (PMP) draft. End-user / Customer Status Review. Detailed product and marketing plan. Quality control plan. Optimization Review meeting. List other deliverables when defined. 	<ul style="list-style-type: none"> Proof of Concept Report. Functional Requirements Document. SEMP (TRL 4, 5, and 6) TEMP (TRL 4, 5, and 6) Quality Assurance Plan. Configuration Plan Management. PMP (updated). (TRL 4, 5, & 6) Risk Management Plan (updated). (TRL 4, 5, and 6) Program Cost Analysis (updated). (TRL 4, 5, and 6) End-user / Customer Status Review. List other deliverables when defined. 	<ul style="list-style-type: none"> ORD and CONOPs. Security Assessment (updated). Program Definition Document (POD). OMB 300 Capital Asset Plan. Acquisition Plan. Entry Criteria Checklist. Analysis of Alternatives. (TRL 5 & 6) List other deliverables when defined. 	<p>Germane to both Acquisition and Commercialization</p> <ul style="list-style-type: none"> Technology Transition Agreement (TTA), or Technology Commercialization Agreement (TCA) as applicable. Initial Security Guidelines. Draft Program Assessment Rating Tool (PART) plan, if required. National Environmental Policy Act (NEPA) initial assessment, if required. Interoperability Assessment. List other deliverables when defined. <p>Specific to Commercialization</p> <ul style="list-style-type: none"> Engineering documentation package release and manufacturing plan. Updated marketing plan. Test plan for quality control. Development Phase Review meeting. List other deliverables when defined. 	<p>Germane to both Acquisition and Commercialization</p> <ul style="list-style-type: none"> Technology Transition (draft). Operational and Functional Requirements Documentation (updated). Risk Management Plan (updated). Program Cost Analysis (updated). PMP (updated). Strategic Program Planning Documentation (if conducted). Operations and Maintenance Manual. Security Manual. Finalized Interoperability Assurance Report. (TRL 7 and 8) Applicable Management Directives (MD), if required. (TRL 7) List other deliverables when defined. <p>Specific to Commercialization</p> <ul style="list-style-type: none"> IP Protection and Licensing. Manufacturing and sales plan release package (to be distributed). Finalize sales release package. Pilot Phase Review meeting. List other deliverables when defined. 	<p>Germane to both Acquisition and Commercialization</p> <ul style="list-style-type: none"> Limited User Test (LUT) Plan. Deployment or Transition Plan. Training Plan. Operational Test Report. Customer Acceptance Document. Initial System-level Metrics Assessment. List other deliverables when defined. <p>Specific to Commercialization</p> <ul style="list-style-type: none"> Demonstrate that a defect-free product can be manufactured on schedule and at a cost consistent with the target price points. Execution of the acceptance, shipment, and after-sales support of the new product. List other deliverables when defined. 	<p>Germane to both Acquisition and Commercialization</p> <ul style="list-style-type: none"> Customer Feedback. Lessons-learned. After-action Review. Support Plan is completed (a. Spiral Development Assessment, b. Prepared Product Improvement, c. Emerging Threats) Assessment, d. Technology Refresh / Insertion, e. Quality Assurance / Metrics Report, f. Risk Management Reassessment). List other deliverables when defined. <p>Specific to Commercialization</p> <ul style="list-style-type: none"> Finalized product plan sales release package (to be distributed). Sales Release Phase Review meeting. Execution of the acceptance, shipment, and after-sales support of the new product. List other deliverables when defined.
Management Review	<ul style="list-style-type: none"> STIC review meeting to ensure exit criteria / deliverables are met. EOC review and approval to move onto the next phase. Corporate Review meeting of value proposition and product overview. Results and follow up actions. 			<ul style="list-style-type: none"> STIC review meeting to ensure exit criteria / deliverables are met (incorporate S&T Director of Research). Corporate Review meeting of the preliminary product plan. Feasibility Review meeting. Results and follow up actions. 	<ul style="list-style-type: none"> STIC review meeting to ensure exit criteria / deliverables are met (incorporate S&T Director of Research). EOC review and approval to move onto the next phase. Optimization Review meeting. Results and follow up actions. 	<ul style="list-style-type: none"> STIC review meeting to ensure exit criteria / deliverables are met (incorporate S&T Director of Innovation, or Transition). Analysis of the engineering and manufacturing plan. Results and follow up actions. 	<ul style="list-style-type: none"> STIC review meeting to ensure exit criteria / deliverables are met (incorporate S&T Director of Innovation, or Transition). Analysis of the engineering and manufacturing plan. Results and follow up actions. 	<ul style="list-style-type: none"> STIC review meeting to ensure exit criteria / deliverables are met (incorporate S&T Director of Innovation, or Transition). EOC review and approval to move onto the next phase. Development Phase Review meeting. Comprehensive analysis of the engineering and manufacturing plan. Results and follow up actions. 	<ul style="list-style-type: none"> STIC review meeting to ensure exit criteria / deliverables are met (incorporate S&T Director of Innovation, or Transition). Analysis and review of the manufacturing release package. Development Phase Review meeting. Results and follow up actions. 	<ul style="list-style-type: none"> STIC review meeting to ensure exit criteria / deliverables are met (incorporate S&T Director of Innovation). Analysis and review of the manufacturing plan. Results and follow up actions. 	<ul style="list-style-type: none"> STIC review meeting to ensure exit criteria / deliverables are met (incorporate S&T Director of Transition). EOC review and approval to move onto the next phase / transition. Corporate review of the finalized product plan sales release package. Sales Release Phase Review meeting.

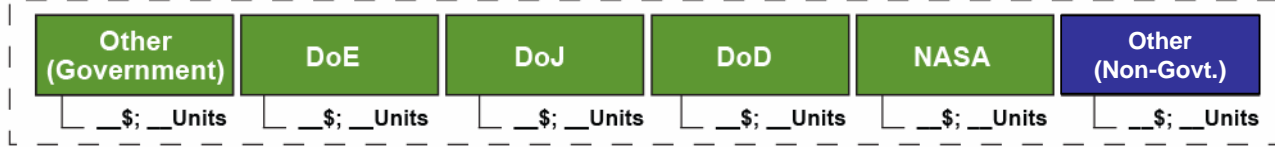
SECURE PROGRAM



Notes Executive Oversight Committee (EOC) – consists of the Dep Sec, Under Secretary of Management, Under Secretary of DHS S&T and the corresponding G7 Head (appropriate representative from the operating component) Science and Technology Internal Committee (STIC) – consists of the relevant S&T Director (Research, Innovation, or Transition), S&T Division Head, S&T Division Program Manager, and the corresponding G7 Head (appropriate representative from the operating component)

Appendix I: Market Potential Templates

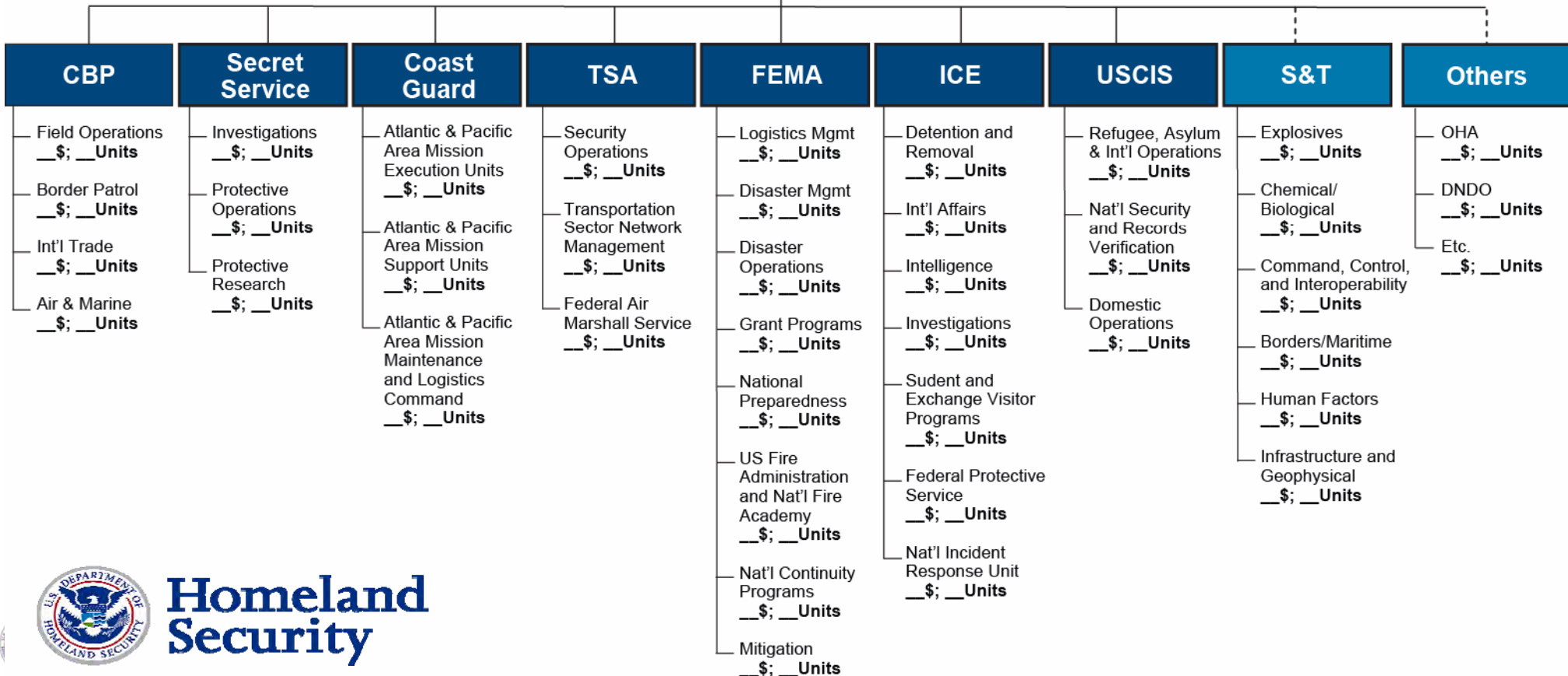
Market Potential Template



DHS

Ancillary Markets

First Responders



Homeland Security

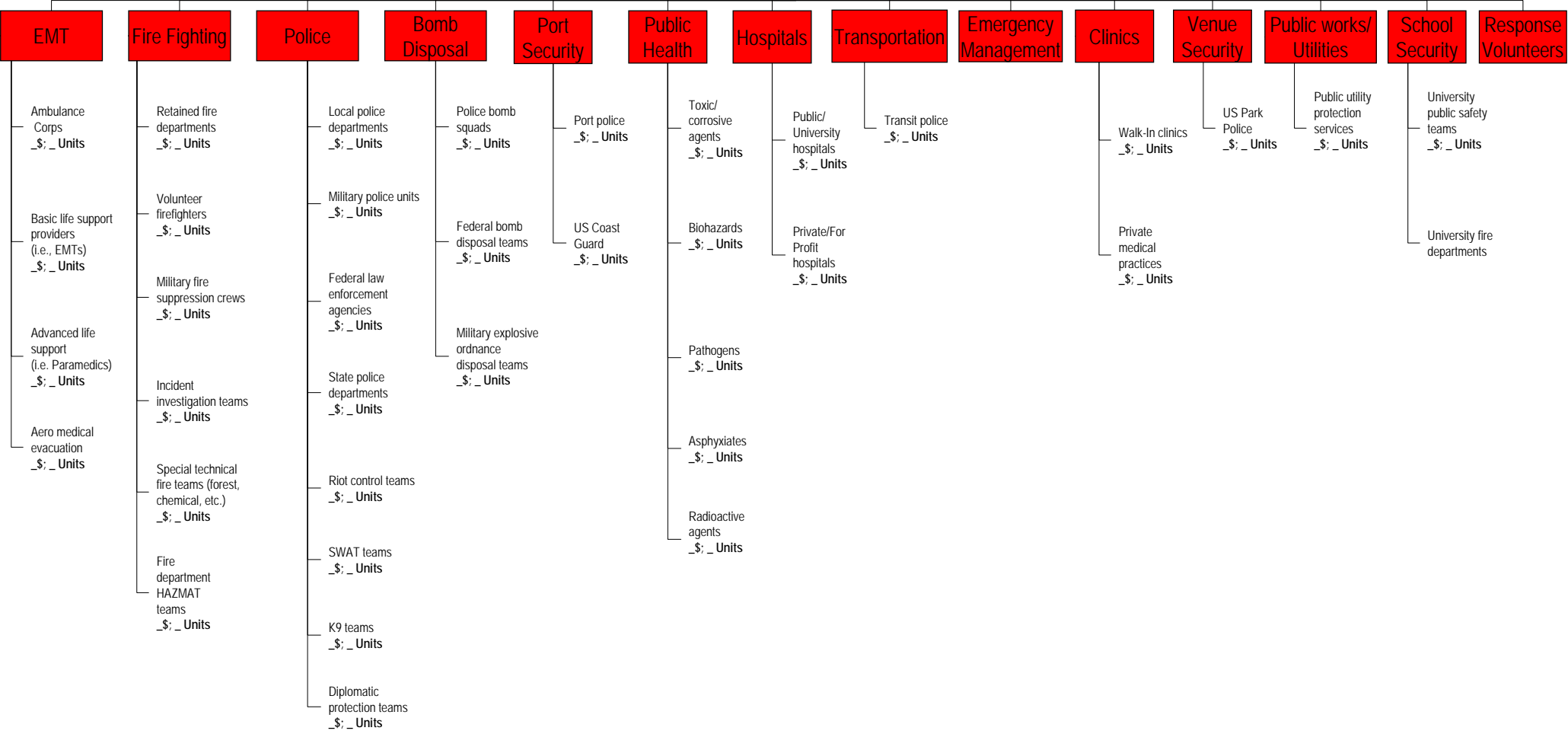
Critical Infrastructure Key Resources (CIKR)

Agriculture and Food	Defense Industrial Base	Energy	Public Health and Healthcare	National Monuments and Icons	Banking and Finance	Water	Chemical	Commercial facilities	Emergency Services	Materials, Reactors and	Telecommunications	Critical Manufacturing	Postal and Shipping Services	Transportation	Information Technology
Food Retail _\$_; _ Units	Defense Contractors _\$_; _ Units	Coal mining operations _\$_; _ Units	Public/University hospitals _\$_; _ Units	Guided tour services _\$_; _ Units	Credit lending institutions _\$_; _ Units	Public utilities _\$_; _ Units	Inorganic chemical production _\$_; _ Units	Hotels _\$_; _ Units	Fire Departments _\$_; _ Units	Electric utilities _\$_; _ Units	Telephone/Cellular services _\$_; _ Units	Iron and Steel mills _\$_; _ Units	United States Postal Service _\$_; _ Units	AMTRAK _\$_; _ Units	Hardware providers _\$_; _ Units
Farm Equipment _\$_; _ Units	Industry analysis _\$_; _ Units	Coal power plants _\$_; _ Units	Private/For Profit hospitals _\$_; _ Units	Travel services _\$_; _ Units	Commercial banking _\$_; _ Units	Desalinization plants _\$_; _ Units	Organic industrial production _\$_; _ Units	Shopping centers _\$_; _ Units	Law enforcement agencies _\$_; _ Units	Reactor and associated materials _\$_; _ Units	Satellite data transmission _\$_; _ Units	Aluminum production and processing _\$_; _ Units	High volume document and parcel shipping _\$_; _ Units	Commuter rail _\$_; _ Units	IT Conglomerates _\$_; _ Units
Meat/Poultry Processing _\$_; _ Units	Think tanks/research institutions _\$_; _ Units	Coal equipment manufacturers _\$_; _ Units	Clinics _\$_; _ Units	Lodging/Hotel _\$_; _ Units	Private equity _\$_; _ Units	Treatment plants _\$_; _ Units	Ceramics _\$_; _ Units	Stadiums and sport arenas _\$_; _ Units	Search and rescue teams _\$_; _ Units	University and educational institutions _\$_; _ Units	Broadcasting entities _\$_; _ Units	Nonferrous metal production and processing _\$_; _ Units	Container shipping services _\$_; _ Units	Intracity rail services _\$_; _ Units	Semiconductor production _\$_; _ Units
Food Processing _\$_; _ Units	University partnership programs _\$_; _ Units	Hydroelectric _\$_; _ Units	Private medical practices _\$_; _ Units	Guest services/tourist hospitality _\$_; _ Units	Consumer banking _\$_; _ Units	Equipment manufacturers _\$_; _ Units	Petrochemicals _\$_; _ Units	Schools _\$_; _ Units	Ambulance companies _\$_; _ Units	Control systems _\$_; _ Units	Broadcast equipment manufacturing _\$_; _ Units	Engine, Turbine and Power transmission _\$_; _ Units	Marine shipping _\$_; _ Units	Commercial airline _\$_; _ Units	Electronics manufacture _\$_; _ Units
Dairy Processing _\$_; _ Units	National laboratories _\$_; _ Units	Dam operations _\$_; _ Units	Medical laboratories _\$_; _ Units	People moving services _\$_; _ Units	Building societies/Private banks _\$_; _ Units	Pipe and water control device manufacturers _\$_; _ Units	Agrochemicals _\$_; _ Units	Commercial office buildings _\$_; _ Units	Mountain/Cave/ Mine rescue teams _\$_; _ Units	Nuclear safety systems _\$_; _ Units	Radio equipment manufacturing _\$_; _ Units	Marine shipping _\$_; _ Units	Private air services _\$_; _ Units	IT services _\$_; _ Units	Server and network hardware _\$_; _ Units
Dairy Farms _\$_; _ Units		Wind power _\$_; _ Units	Pharmaceutical _\$_; _ Units	Queuing equipment makers _\$_; _ Units	Merchant banks _\$_; _ Units		Polymers _\$_; _ Units	Museums _\$_; _ Units	Other technical rescue teams _\$_; _ Units	Waste disposal services _\$_; _ Units	Electrical equipment manufacturing _\$_; _ Units	Trucking industry _\$_; _ Units	Cruise lines _\$_; _ Units	Subway systems _\$_; _ Units	Display/digital TV _\$_; _ Units
Ranching _\$_; _ Units		Solar power _\$_; _ Units	Health insurance _\$_; _ Units	Private security _\$_; _ Units	Global financial services firms _\$_; _ Units		Elastomer production _\$_; _ Units	Zoos and Aquariums _\$_; _ Units	Bomb disposal units _\$_; _ Units	Uranium processors _\$_; _ Units	Motor Vehicle manufacturing _\$_; _ Units	Airborne shipping _\$_; _ Units	Distribution services _\$_; _ Units	Long-haul maritime shipping _\$_; _ Units	Software production _\$_; _ Units
Organic Farming/Sustainable Agriculture _\$_; _ Units		Public utilities companies _\$_; _ Units	Medical material providers _\$_; _ Units		Community development _\$_; _ Units		Oleochemicals _\$_; _ Units	Public Libraries _\$_; _ Units	Blood/Organ transplant supply _\$_; _ Units	Protective garment manufacturers _\$_; _ Units	High speed data transmission _\$_; _ Units	Aerospace product & parts manufacturing _\$_; _ Units	Trucking _\$_; _ Units	Trucking _\$_; _ Units	Gaming _\$_; _ Units
Traditional Planning _\$_; _ Units		Oil companies _\$_; _ Units	Medical equipment manufacturers _\$_; _ Units		Community banks _\$_; _ Units		Explosives _\$_; _ Units	Amusement parks _\$_; _ Units	Amateur radio emergency comms _\$_; _ Units	Internet service providers _\$_; _ Units	Print media _\$_; _ Units	Railroad rolling stock _\$_; _ Units	Bus services _\$_; _ Units	Freight rail service _\$_; _ Units	Information security _\$_; _ Units
Commercial fishing _\$_; _ Units			Medical technology manufacturers _\$_; _ Units		Savings and Loans _\$_; _ Units		Fragrance production _\$_; _ Units		Public utility protection providers _\$_; _ Units	Internet technology providers _\$_; _ Units	Other Transportation equipment _\$_; _ Units	Automobile travel _\$_; _ Units	Roads, Highways, bridges and tunnels _\$_; _ Units	Semiconductor equipment _\$_; _ Units	
			Biotechnology _\$_; _ Units		Credit unions _\$_; _ Units		Chemical wholesale _\$_; _ Units		Emergency Road services _\$_; _ Units						
					Insurance companies _\$_; _ Units		Exotic chemicals _\$_; _ Units		Emergency Social services _\$_; _ Units						
					Insurance brokerages _\$_; _ Units				Community emergency response teams _\$_; _ Units						
					Reinsurance companies _\$_; _ Units				Disaster relief _\$_; _ Units						
					Stock brokerages _\$_; _ Units				Famine relief teams _\$_; _ Units						
					Capital market banks _\$_; _ Units				Poison Control units _\$_; _ Units						
					Custody services _\$_; _ Units				Animal control teams _\$_; _ Units						
					Angel investment _\$_; _ Units				Wildlife services _\$_; _ Units						
					Venture capital _\$_; _ Units										



Homeland Security

First Responders



NOTES

NOTES

NOTES

NOTES

Appendix J: Requirements Development Guide (April 2008)



Requirements Development Guide

April 2008



Homeland
Security

Science and Technology

Preface

This Requirements Development Guide assists the S&T Project/Program Managers, Transition Managers and Division Leaders in the development of detailed requirements to aid in the cost-effective and efficient development and deployment of products and services for our customers – DHS Operating Components and First Responders.

We sincerely believe this guide also provides value to the DHS Operating Components and First Responder communities in developing and articulating their operating requirements and helps to ensure the accurate and timely development and deployment of products and services to aid in the implementation of the mission-critical objectives of the Operating Components and First Responders.

Tom Cellucci
April 2008

Acknowledgement:

I extend my sincerest thanks and appreciation to all those at DHS who contributed in creating this guide. In particular, Sam Francis and Mark Protacio deserve a special thanks for their endless efforts in developing materials for this resource and working not only with others within the Science & Technology Directorate, but also with personnel throughout DHS and with countless input from representatives in the Private Sector. Please give them all the credit for the value this guide brings, while I accept the responsibility for any errors or shortcomings.

Contents

Requirements Development Guide	1
Preface.....	2
Contents	3
List of Figures	4
Introduction.....	5
Quick Overview	5
Why Requirements?	6
The Requirements Hierarchy and Traceability	7
Requirements and the Product Life Cycle	10
Characteristics of Good Requirements.....	12
Requirements and Test and Evaluation (T&E).....	12
Developing Operational Requirements: Customer Input	13
Tailored Product Life Cycle: Acquisition	20
Tailored Product Life Cycle: Commercialization	22
Tailored Product Life Cycle: Other Project Types	24
Summary	26
Additional Requirements Development Readings	26
Glossary	28
Appendix A: Operational Requirements Document (ORD) Template	31
Appendix B: Acquisition Mini-Course	35
Appendix C: Commercialization Mini-Course	48
Appendix D: Requirements Mini-Course	64
Appendix E: Commercialization Briefing to Industry.....	100
Appendix F: SECURE Program Concept of Operations.....	123
Appendix G: DHS Management Directive 1400	129
Appendix H: Uncovering Requirements	141

List of Figures

Figure 1. The requirements hierarchy	8
Figure 2. An example of a specification tree	10
Figure 3. A generic product life cycle	10
Figure 4. The linkage between requirements and T&E	13
Figure 5. The contents of an Operational Requirements Document	14
Figure 6. The generic product life cycle (revisited)	20
Figure 7. DHS's Acquisition Life Cycle (MD1400)	20
Figure 8. The Concept and Technology Development phase, expanded	21
Figure 9. A product life cycle to govern Commercialization	22
Figure 10. Expansion of the Req'ts and Tech. Development phase	23
Figure 11. Another view of the Commercialization product life cycle	24
Figure 12. The generic product life cycle (revisited again)	25

Introduction

This guide introduces the role of requirements in product and system development in S&T and, more broadly, in DHS. The target readership is, principally, S&T project managers. The subject matter relates directly to S&T Transition projects, and only indirectly to Basic Research and Innovation projects.

There is no universally accepted standard vocabulary regarding requirements and specifications. In this document, definitions from DHS management directives by the Project Management Institute (in its *Guide to the Project Management Body of Knowledge*) have been used. The terms “product” and “system” are used interchangeably. Occasionally, the terms “sponsor” and “customer” are used interchangeably, as DHS Acquisition sponsors are S&T’s customers. As always, it is more important to understand the principles than to memorize the vocabulary.

Furthermore, requirements development, in general, is a topic that has received great attention. There exists an incredible volume of books, articles and various other writings on the topic of requirements development. This Requirements Development Guide is just one resource. Please refer to the “Additional Requirements Development Readings” section of this guide for other publications that focus on various aspects of requirements development. Many of these readings are easily accessible on the internet.

Address comments to the Chief Commercialization Officer Tom Cellucci, Ph.D., MBA, at Thomas.Cellucci@dhs.gov.

Quick Overview

Requirements-driven product development is a difficult enterprise, for two fundamental reasons:

- Needs are difficult to articulate, even if users have the breadth of vision to look outside the constraints of their current operational procedures
- Developers tend to jump to preconceived solutions, because of a bias toward a favorite technology or because of a belief that their solution is what the users “should want” or “really need.”

This document presents a brief overview of requirements-driven product development, organized into the following topics:

- **“Why Requirements?”** summarizes the advantages of requirements-driven design and illustrates the pitfalls of its opposite, “technology push.”
- **“The Requirements Hierarchy and Traceability”** summarizes the hierarchy of requirements and specifications, underscoring the important distinction between “defining the problem” and “defining the solution.”
- **“Requirements and the Product Life Cycle”** illustrates the evolution of requirements and specifications through the life cycle of product development.
- **“Characteristics of Good Requirements”** lists the characteristics that distinguish good requirements from bad.

- **“Requirements and Test and Evaluation”** illustrates the close linkage between operational requirements and operational test and evaluation, and the similar linkage between technical requirements and developmental test and evaluation.
- **“Developing Operational Requirements: Customer Input”** lists nine techniques for eliciting user requirements.
- **“Tailored Product Life Cycle: Acquisition”** introduces the concept of a generic product life cycle and shows how it is tailored to DHS’ Acquisition life cycle defined in MD1400.
- **“Tailored Product Life Cycle: Commercialization”** shows how the same generic product life cycle can be tailored to govern a Commercialization project.
- **“Tailored Product Life Cycle: Other Project Types”** shows how the same generic product life cycle can be tailored to govern the development of S&T products which are not used by end users in the field.

Why Requirements?

A requirement is an attribute of a product or system necessary to satisfy the needs of a sponsor, customer, end user or other stakeholder. Requirements therefore define “the problem.” In contrast, “the solution” is defined by technical specifications, which represent the engineering community’s “technical interpretation” of the requirements.

We could save ourselves a lot of work if we jump straight to “the solution” without defining “the problem.” Why don’t we do that? Because if we take that shortcut we are likely to find that our solution is not the best choice among possible alternatives or, even worse, we’re likely to find that our “solution” doesn’t even solve the problem!

For example, faced with the problem of potential intruders to a sensitive facility, we might define the requirement as “build a wall” whereas the real requirement is “detect, thwart, and capture intruders.” Our wall might “thwart” intruders (or might not, if they’re adept at tunneling), but it would not detect them or facilitate their capture. In short, the solution would not solve the problem.



The robust requirement to “detect, thwart, and capture intruders,” which includes no preconceived solutions, prompts us to analyze alternative conceptual solutions and choose the best. This analysis is often called an “analysis of alternatives”, or AoA, and is an intrinsic part of requirements-driven design.

One way to ensure that we are defining a problem, rather than a solution, is to begin the statement of the requirement with the phrase “we need the capability to ...” It’s nearly impossible to complete this sentence with a solution (“a wall”), and much easier to

complete the sentence with a problem (“capability to detect intruders”). This approach is sometimes called capability-based planning. It is a very simple, yet powerful, concept.

At the other extreme from the “requirements-pull” approach is its opposite: “technology push.” Here we start with a solution (perhaps a new technology) and see what problems it might enable us to solve. The danger in this approach is to become enamored of “the solution” and neglect to ensure that it actually solves a problem. With technology push, it is likely that real user requirements will be modified or even ignored to force-fit the desired solution. A historical example was the product known as Picture Phone introduced (and discontinued) in the 1960s, when the advance of telecommunications technology first made possible the transmission and display of video as well as voice. Picture Phone, which allowed telephone users to see each other during a call, was a technological success but a market disaster. It turned out that callers generally don’t want to be seen, as a bit of unbiased market analysis would have disclosed.

Technology push should not be ignored, but if the goal is successful transition to the field with acceptable risk, the technology being pushed must be compared with alternative solutions against a real set of user requirements.

Aside from assuring that the “solution” actually solves the “problem,” requirements-driven design has a further advantage in that the requirements provide criteria against which the product’s successful development can be measured. Specifically, if the product was developed to address a set of quantified operational requirements, then its success is measured by Operational Test and Evaluation (OT&E) to validate that an end-user can use the product and achieve the stated operational goals.

Prior to OT&E, it is common practice to subject products to Developmental Test and Evaluation (DT&E). The purpose of DT&E is to verify that the product meets its technical specifications, which are the engineers’ interpretation of the operational requirements. Such DT&E does not obviate the need for OT&E, which validates that the engineers’ solution is not only technically successfully but also represents a successful interpretation of the end users’ needs, satisfying the original operational requirements (not just the technical specifications) when operated by representative users.

Often requirements are stated in terms of “threshold values” and “objective values,” where the “objective value” is the desired performance and the “threshold value” is the minimum acceptable performance. This formalism is useful in allowing stretch goals to be asserted without saddling the system development with unacceptable risk.

The Requirements Hierarchy and Traceability

To reiterate the definitions above, the documents that govern product development include requirements, which define the problem, and specifications, which define the solution. Nevertheless, the hierarchy of requirements and specifications is more complex than that simple dichotomy, as depicted in Figure 1.

The hierarchy is divided into two domains, operational requirements and technical requirements, highlighted in yellow and blue in the figure, representing the “problem space” and the “solution space” respectively. The sponsor (or, from S&T’s perspective, the customer), representing the end users in the field (the operators), is responsible for all operational requirements, from the top-level mission requirements to the detailed

system-level operational requirements. The system developer is responsible for translating the operational requirements into a system solution, documented in a hierarchy of technical specifications.

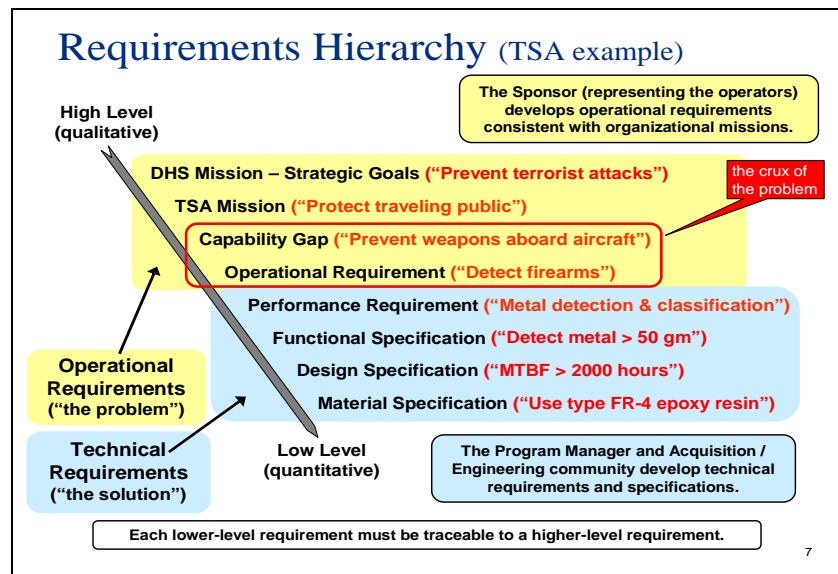


Figure 1. The requirements hierarchy

The highest-level type of technical “specification” is actually called a performance “requirement.” A performance requirement actually represents a bridge from operational requirements to the engineering interpretation of those requirements. Put another way, in the course of developing a new system it is necessary to transform the system operational requirements, which are stated from the users’ perspective as required outcomes of system action, into a set of system performance requirements, which are stated in terms of engineering characteristics.

The requirements and specifications are described below, first those which define the problem and then those that define the solution:

- **Problem Definition**
 - **Mission Needs Statement (MNS)** is required by the DHS *Investment Review Process* (Management Directive 1400, Appendix G) and is developed by the DHS sponsor (S&T’s customer) who represents the end users. The MNS provides a high-level description of the mission need (or, equivalently, capability gap), and is used to justify the initiation of an Acquisition program.
 - **Operational Requirements Document (ORD)** is also required by the DHS *Investment Review Process* and, like the MNS, is developed by the DHS sponsor. The ORD specifies operational requirements and a concept of operations (CONOPS), written from the point of view of the end user. The ORD is independent of any particular implementation, should not refer to any specific technologies, and does not commit the developers to a design.
- **Solution Definition**

- **Performance Requirements** represent a bridge between the operationally oriented view of the system defined in the ORD and an engineering-oriented view required to define the solution. Performance requirements are an interpretation, not a replacement of operational requirements. Performance requirements define the functions that the system *and its subsystems* must perform to achieve the operational objectives and define the performance parameters for each function. These definitions are in engineering rather than operational terms.
- **Functional Specifications** define the system solution functionally, though not physically. Sometimes called the “system specification” or “A-Spec,” these specifications define functions at the system, subsystem, *and component level* including:
 - Configuration, organization, and interfaces between system elements
 - Performance characteristics and compatibility requirements
 - Human engineering
 - Security and safety
 - Reliability, maintainability and availability
 - Support requirements such as shipping, handling, storage, training and special facilities
- **Design Specifications** convert the functional specifications of *what* the system is to do into a specification of *how* the required functions are to be implemented in hardware and software. The design specifications therefore govern the materialization of the system components.
- **Material Specifications** are an example of lower-level supporting specifications which support the higher-level specifications. Material specifications define the required properties of materials and parts used to fabricate the system. Other supporting specifications include **Process Specifications** (defining required properties of fabrication processes such as soldering and welding) and **Product Specifications** (defining required properties of non-developmental items to be procured commercially).

The hierarchy of specifications, which specifies the solution, is often depicted as a specification tree, of which a notional example is shown in Figure 2.

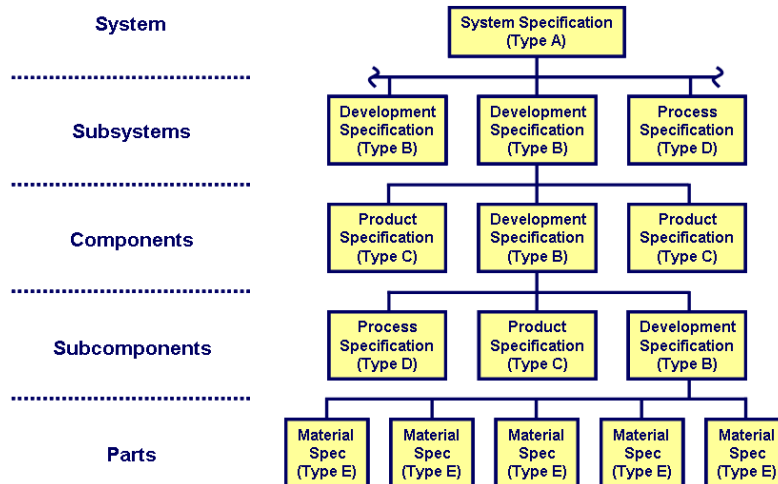


Figure 2. An example of a specification tree

An important feature of a requirements and specification hierarchy is a concept termed *traceability*, which is the thread that weaves this hierarchy into a coherent fabric with no loose ends. Traceability ensures completeness, that all lower-level requirements and acceptance criteria come from higher-level requirements and that all higher-level requirements are allocated to lower-level requirements. Traceability is also used to manage change and provides the basis for test planning, often using a tool called the Requirements Verification Matrix (RVM).

Please refer to Appendix D for more details concerning requirements.

Requirements and the Product Life Cycle

The previous section described the logical flow from high-level requirements to low-level specifications but did not address when these activities happen. To relate requirements development to other project activities, consider the generic product life cycle in Figure 3:

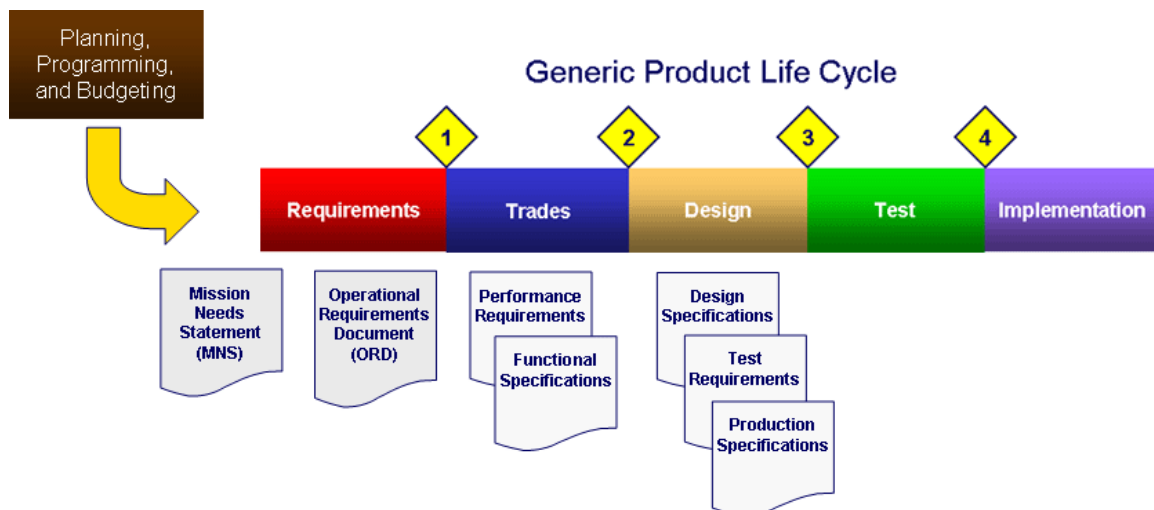


Figure 3. A generic product life cycle

The life cycle is a phase-gate framework, consisting of 5 sequential phases separated by 4 gates allowing the opportunity to assess a given project's progress before it advances to the next phase. Prior to the life cycle is an activity called Planning, Programming, and Budgeting (PP&B) during which preliminary versions of the requirements may be developed along with preliminary system concepts. Because of the time delay in the budget cycle, considerable time elapses between PP&B and project execution, so these preliminary requirements and concepts must be reassessed at project start. The phases include the following activities:

- Planning, Programming, and Budgeting
 - Capstone IPTs identify capability gaps (mission needs) requiring materiel solutions, and convey these capability gaps to S&T. In turn, S&T assesses technology-based solutions to address these gaps and develops rough order-of-magnitude (ROM) estimates of project cost and schedule. To develop these estimates and gain Capstone IPT support for a future project, S&T considers alternative system concepts. This PP&B activity is often informal and quite preliminary.
 - When the intent is to launch an Acquisition program to develop an end-user system, the sponsoring DHS Component documents the capability gap in a Mission Needs Statement.
- Requirements Phase
 - If the purpose of the project is to develop a product or system to be operated by end users, the Mission Needs Statement is updated, refined, and formalized.
 - The operational requirements are developed and documented in an Operational Requirements Document (ORD), providing the detailed quantitative definition of the problem to be solved. (We will later consider the case of other types of projects which do not develop end-user products and which therefore do not require operational requirements.)
 - Preliminary performance requirements may also be defined and documented in this phase, as the first step in defining the engineering solution. The preliminary performance requirements should be independent of any particular implementation, so as not to bias the subsequent analysis of alternatives.
- Trades Phase
 - Alternative system concepts are explored and the system requirements are allocated to subsystems whose performance requirements are defined. After selection of the optimum system concept, the functions necessary for system performance are defined down to the component level and documented as functional specifications. Often the interfaces between system elements are defined in separate documents called Interface Control Documents (ICDs).
- Design Phase
 - With the functional specifications defined, designers proceed to engineer the physical realization of the system and document this design in a set of design specifications and engineering drawings. Test requirements are finalized and preliminary production specifications are developed.

- Test Phase
 - Developmental test and evaluation verifies a representative test item or items against the functional specifications and performance requirements. Operational test and evaluation validates conformance to the Operational Requirements Document (ORD).
- Implementation Phase
 - The tested product is transitioned to its target environment. If the product is an end-user product, implementation consists of transition to production, followed by deployment, field operation, and support. If the product is a technology product not intended for use by end users, implementation consists of transition to a follow-on program (perhaps an Acquisition program) which will integrate the technology product into an end-user system.

Characteristics of Good Requirements

Requirements engineering is difficult and time-consuming, but must be done well if the final product or system is to be judged by the end users as successful. From the International Council of Systems Engineers (INCOSE) Requirements Working Group¹, here are eight attributes of good requirements:

- Necessary: Can the system meet prioritized, real needs without it? If yes, the requirement isn't necessary.
- Verifiable: Can one ensure that the requirement is met in the system? If not, the requirement should be removed or revised.
- Unambiguous: Can the requirement be interpreted in more than one way? If yes, the requirement should be clarified or removed. Ambiguous or poorly worded requirements can lead to serious misunderstandings and needless rework.
- Complete: Are all conditions under which the requirement applies stated? Also, does the specification include all known requirements?
- Consistent: Can the requirement be met without conflicting with any other requirement? If not, the requirement should be revised or removed.
- Traceable: Is the origin (source) of the requirement known, and is there a clear path from the requirement back to its origin?
- Concise: Is the requirement stated simply and clearly?
- Standard constructs: Requirements are stated as imperative needs using "shall." Statements indicating "goals" or using the words "will" or "should" are not imperatives.

Requirements and Test and Evaluation (T&E)

As described in the preceding section, one characteristic of good requirements is that they be verifiable. Accordingly, a project's test and evaluation strategy must be designed so that all requirements are verified. To assure that the product or system meets all its requirements, a construct known as a Requirements Verification Matrix is often used to map all requirements into specific verification methods such as analysis, inspection,

¹ Kar, Pradip and Bailey, Michelle. Characteristics of Good Requirements. International Council of Systems Engineers, Requirements Working Group. INCOSE Symposium, 1996. Found online: <http://www.afis.fr/nav/gt/ie/doc/Articles/CHARACTE.HTM>.

demonstration, and test. The distinction between test and demonstration is that a test usually involves some sort of instrumentation and collection of data, whereas a demonstration verifies compliance by mere observation of results.

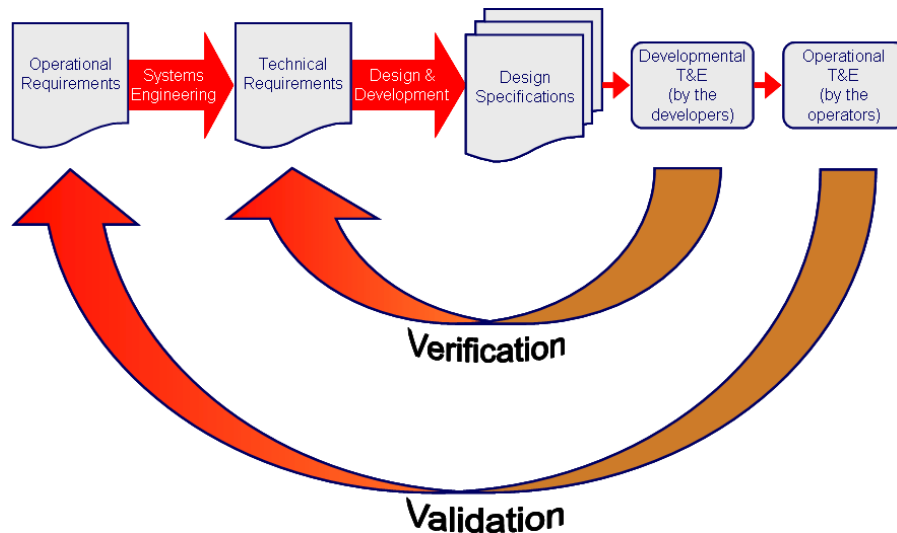


Figure 4. The linkage between requirements and T&E

Figure 4 above illustrates that the purpose of DT&E is to verify that the product or system meets its technical requirements (such as performance requirements and functional specifications). However, since the technical requirements are an engineering interpretation of the operational requirements, it is quite possible that a product or system can satisfy its technical requirements without satisfying its operational requirements. It's for this reason that products and systems also undergo OT&E conducted by an independent test agent, to provide objective validation that the system satisfies its operational requirements when operated by real end users in the most realistic environment available.

The simplified figure above does not depict T&E below the system level. However, as the system is integrated in preparation for system-level DT&E, components are tested prior to integration into subsystems, and subsystems are tested prior to integration into the total operational system. The strategy for testing at the component, subsystem, and system level is documented in a Test and Evaluation Master Plan.

Developing Operational Requirements: Customer Input

So far, we've discussed operational requirements but have not provided any insight into how to develop them. Let's first look at the contents of a typical Operational Requirements Document (ORD) shown in Figure 5 and discussed in more detail in Appendix A.

OPERATIONAL REQUIREMENTS DOCUMENT	
1.0	General Description of Operational Capability
1.1	Capability Gap
1.2	Overall Mission Area Description
1.3	Description of the Proposed System
1.4	Supporting Analysis
1.5	Mission the Proposed System Will Accomplish
1.6	Operational and Support Concept
1.6.1	Concept of Operations
1.6.2	Support Concept
2.0	Threat
3.0	Existing System Shortfalls
4.0	Capabilities Required
4.1	Operational Performance Parameters
4.2	Key Performance Parameters (KPPs)
4.3	System Performance.
4.3.1	Mission Scenarios
4.3.2	System Performance Parameters
4.3.3	Interoperability
4.3.4	Human Interface Requirements
4.3.5	Logistics and Readiness
4.3.6	Other System Characteristics
5.0	System Support
5.1	Maintenance
5.2	Supply
5.3	Support Equipment
5.4	Training
5.5	Transportation and Facilities
6.0	Force Structure
7.0	Schedule
8.0	System Affordability
	Appendixes
	Glossary

Figure 5. The contents of an Operational Requirements Document

The complexity of the intended system and its operational context will govern the required level of detail in the ORD. The most difficult sections to develop are probably Section 4.0, which describes the capabilities required of the system to be developed, and Section 1.6, which describes the operational and support concepts.

In a perfect world, the operational requirements would be developed by S&T's customer, the sponsoring organization, representing the end users and support personnel in the field. Ideally, the role played by S&T in the development of the ORD would be limited to assessing technical feasibility and risk. However, if the sponsor's organization needs assistance in developing operational requirements, S&T should assist.

In helping DHS customers fill in the blanks, an S&T project manager will almost certainly discover that neither the end users nor their management know what they want in sufficient detail to proceed with product or system development. This barrier is only the first of many challenges to overcome in the development of operational requirements. These challenges may include:

- Users who may not understand precisely what they want or have a clear idea of their requirements. Few users talk about their tasks, needs, and operational environment in neat, concise statements about product requirements.
- Users who don't always understand the distinction between a problem and a solution and may insist on a specific preconceived solution that may be a poor fit to the problem.
- Users who may not commit to a set of written requirements.
- Users who may insist on new requirements throughout project execution, without regard to impact on cost and schedule.
- Poor communication between S&T program managers and due to differing vocabularies. Sometimes users and technologists use the same term to mean different things, leading them to believe they're in agreement when they're not.
- Users who often do not participate in reviews (or are incapable of doing so).
- Users who may be technically unsophisticated and may not understand the development process.
- Requirements discovery may be carried out by technical experts rather than by personnel with the people skills and the domain knowledge to understand user needs properly.

On the other hand, there are several challenges that face S&T program managers throughout the requirements gathering process. S&T program managers must interact with customers to gather and better understand the users' needs.

- Some program managers are not familiar with gathering requirements and communicating with end users.
- Some program managers do not know how to ask users questions to uncover hidden requirements.
- Poor communication between S&T program managers and due to differing vocabularies. Sometimes users and technologists use the same term to mean different things, leading them to believe they're in agreement when they're not.

Please refer to Appendix H for a briefing on "How to Start the Conversation."

There is no silver bullet to solve these potential challenges, but since the issues are universal, there is a wealth of literature that offers approaches to requirements development. As an example, here are nine requirements-elicitation techniques described in the *Business Analyst Body of Knowledge* (from the International Institute of Business Analysis)².

² International Institute of Business Analysis. *A Guide to the Business Analyst Body of Knowledge*, Release 1.6. 2006. Found online: http://www.theiiba.org/Content/NavigationMenu/Learning/BodyofKnowledge/Version16/BOKV1_6.pdf.

1. Brainstorming
 - Purpose
 - An excellent way of eliciting many creative ideas for an area of interest. Structured brainstorming produces numerous creative ideas.
 - Strengths
 - Able to elicit many ideas in a short time period.
 - Non-judgmental environment enables outside-the-box thinking.
 - Weaknesses
 - Dependent on participants' creativity.
2. Document Analysis
 - Purpose
 - Used if the objective is to gather details of the "As Is" environment such as existing standard procedures or attributes that need to be included in a new system.
 - Strengths
 - Not starting from a blank page.
 - Leveraging existing materials to discover and/or confirm requirements.
 - A means to cross-check requirements from other elicitation techniques such as interviews, job shadowing, surveys or focus groups.
 - Weaknesses
 - Limited to "as-is" perspective.
 - Existing documentation may not be up-to-date or valid.
 - Can be a time-consuming and even tedious process to locate the relevant information.
3. Focus Group
 - Purpose
 - A means to elicit ideas and attitudes about a specific product, service or opportunity in an interactive group environment. The participants share their impressions, preferences and needs, guided by a moderator.
 - Strengths
 - Ability to elicit data from a group of people in a single session saves time and costs as compared to conducting individual interviews with the same number of people.
 - Effective for learning people's attitudes, experiences and desires.
 - Active discussion and the ability to ask others questions creates an environment where participants can consider their personal view in relation to other perspectives.
 - Weaknesses
 - In the group setting, participants may be concerned about issues of trust, or may be unwilling to discuss sensitive or personal topics.
 - Data collected (what people say) may not be consistent with how people actually behave.
 - If the group is too homogenous, the group's responses may not represent the complete set of requirements.
 - A skilled moderator is needed to manage the group interactions and discussions.
 - It may be difficult to schedule the group for the same date and time.
4. Interface Analysis
 - Purpose
 - An interface is a connection between two components. Most systems require one or more interfaces with external parties, systems or devices.

Interface analysis is initiated by project managers and analysts to reach agreement with the stakeholders on what interfaces are needed. Subsequent analysis uncovers the detailed requirements for each interface.

- Strengths
 - The elicitation of the interfaces' functional requirements early in the system life cycle provides valuable details for project management:
 - Impact on delivery date. Knowing what interfaces are needed, their complexity and testing needs enables more accurate project planning and potential savings in time and cost.
 - Collaboration with other systems or projects. If the interface to an existing system, product or device and the interface already exists, it may not be easily changed. If the interface is new, then the ownership, development and testing of the interface needs to be addressed and coordinated in both projects' plan. In either case, eliciting the interface requirements will require negotiation and cooperation between the owning systems.
 - Weaknesses
 - Does not provide an understanding of the total system or operational concept since this technique only exposes the inputs, outputs and key data elements related to the interfaces.
5. Interview
- Purpose
 - A systematic approach to elicit information from a person or group of people in an informal or formal setting by asking relevant questions and documenting the responses.
 - Strengths
 - Encourages participation and establishes rapport with the stakeholder.
 - Simple, direct technique that can be used in varying situations.
 - Allows the interviewer and participant to have full discussions and explanations of the questions and answers.
 - Enables observations of non-verbal behavior.
 - The interviewer can ask follow-up and probing questions to confirm own understanding.
 - Maintain focus through the use of clear objectives for the interview that are agreed upon by all participants and can be met in the time allotted.
 - Weaknesses
 - Interviews are not an ideal means of reaching consensus across a group of stakeholders.
 - Requires considerable commitment and involvement of the participants.
 - Training is required to conduct good interviews. Unstructured interviews, especially, require special skills. Facilitation/virtual facilitation and active listening are a few of them.
 - Depth of follow-on questions may be dependent on the interviewer's knowledge of the operational domain.
 - Transcription and analysis of interview data can be complex and expensive.
 - Resulting documentation is subject to interviewer's interpretation.

- 6. Observation
 - Purpose
 - A means to elicit requirements by conducting an assessment of the operational environment. This technique is appropriate when documenting details about current operations or if the project intends to enhance or change a current operational concept.
 - Strengths
 - Provides a realistic and practical insight into field operations by getting a hands-on feel for current operations.
 - Elicits details of informal communication and ways people actually work around the system that may not be documented anywhere.
 - Weaknesses
 - Only possible for existing operations.
 - Could be time-consuming.
 - May be disruptive to the person being shadowed.
 - Unusual exceptions and critical situations that happen infrequently may not occur during the observation.
 - May not well work if current operations involve a lot of intellectual work or other work that is not easily observable.
- 7. Prototyping
 - Purpose
 - Prototyping, when used as an elicitation technique, aims to uncover and visualize user requirements before the system is designed or developed.
 - Strengths
 - Supports users who are more comfortable and effective at articulating their needs by using pictures or hands-on prototypes, as prototyping lets them “see” the future system’s interface.
 - A prototype allows for early user interaction and feedback.
 - A throw-away prototype is an inexpensive means to quickly uncover and confirm user interface requirements.
 - A revolutionary prototype can demonstrate what is feasible with existing technology, and where there may be technical gaps.
 - An evolutionary prototype provides a vehicle for designers and developers to learn about the users’ interface needs and to evolve system requirements.
 - Weaknesses
 - Depending on the complexity of the target system, using prototyping to elicit requirements can take considerable time if the process is bogged down by the “how’s” rather than “what’s”.
 - Assumptions about the underlying technology may need to be made in order to present a starting prototype.
 - A prototype may lead users to set unrealistic expectations of the delivered system’s performance, reliability and usability characteristics.
- 8. Requirements Workshop
 - Purpose
 - A requirements workshop is a structured way to capture requirements. A workshop may be used to scope, discover, define, prioritize and reach closure on requirements for the target system. Well-run workshops are considered one of the most effective ways to deliver high quality requirements quickly. They promote trust, mutual understanding, and

- strong communications among the project stakeholders and project team and produce deliverables that structure and guide future analysis.
 - Strengths
 - A workshop can be a means to elicit detailed requirements in a relatively short period of time.
 - A workshop provides a means for stakeholders to collaborate, make decisions and gain a mutual understanding of the requirements.
 - Workshop costs are often lower than the cost of performing multiple interviews.
 - A requirements workshop enables the participants to work together to reach consensus which is typically a cheaper and faster approach than doing serial interviews as interviews may yield conflicting requirements and the effort needed to resolve those conflicts across all interviewees can be very costly.
 - Feedback is immediate, if the facilitator's interpretation of requirements is fed back immediately to the stakeholders and confirmed.
 - Weaknesses
 - Due to stakeholders availability it may be difficult to schedule the workshop.
 - The success of the workshop is highly dependent on the expertise of the facilitator and knowledge of the participants.
 - Requirements workshops that involve too many participants can slow down the workshop process thus negatively impacting the schedule. Conversely, collecting input from too few participants can lead to overlooking requirements that are important to users, or to specifying requirements that don't represent the needs of the majority of the users.
- 9. Survey/Questionnaire
 - Purpose
 - A means of eliciting information from many people, anonymously, in a relatively short time. A survey can collect information about customers, products, operational practices and attitudes. A survey is often referred to as a questionnaire.
 - Strengths
 - When using 'closed-ended' questions, effective in obtaining quantitative data for use in statistical analysis.
 - When using open-ended questions, the survey results may yield insights and opinions not easily obtainable through other elicitation techniques.
 - Does not typically require significant time from the responders.
 - Effective and efficient when stakeholders are not located at one place.
 - May result in large number of responses.
 - Quick and relatively inexpensive to administer.
 - Weaknesses
 - Use of open-ended questions requires more analysis.
 - To achieve unbiased-results, specialized skills in statistical sampling methods are needed when the decision has been made to survey a sample subset.
 - Some questions may be left unanswered or answered incorrectly due to their ambiguous nature.
 - May require follow up questions or more survey iterations depending on the answers provided.
 - Not well suited for collecting information on actual behaviors.

Tailored Product Life Cycle: Acquisition

Earlier we considered a generic product life cycle, shown in Figure 6. For present purposes, we will ignore the PP&B phase, which precedes project execution.

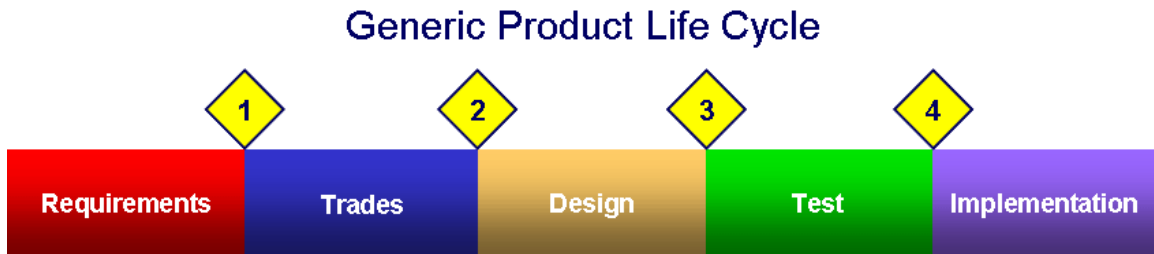


Figure 6. The generic product life cycle (revisited)

It is the nature of such generic management frameworks that they must be adapted (“tailored”) to suit the specific needs of each project. For example, DHS has defined an Acquisition life cycle in MD1400 which governs major DHS Acquisitions, and whose structure is depicted in Figure 7.

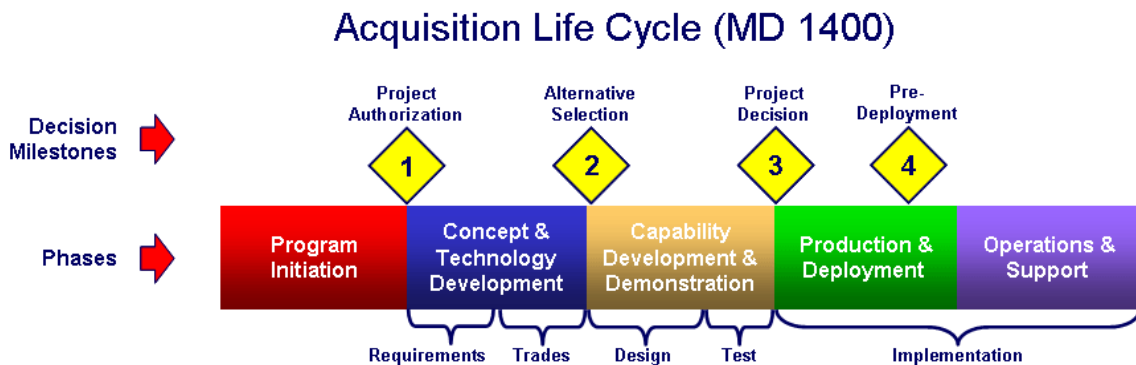


Figure 7. DHS' Acquisition Life Cycle (MD1400)

The mapping of the 5 phases in the generic life cycle model (Requirements, Trades, etc.) is shown. DHS development of end-user systems must use this framework which consists of 5 major phases punctuated by 4 major decision milestones called Key Decision Points. The framework also mandates standard documentation, including the MNS and the ORD.

Since we are focusing on requirements development in this document, we will focus on the Concept and Technology Development phase which, when expanded, can be diagrammed as shown in Figure 8.

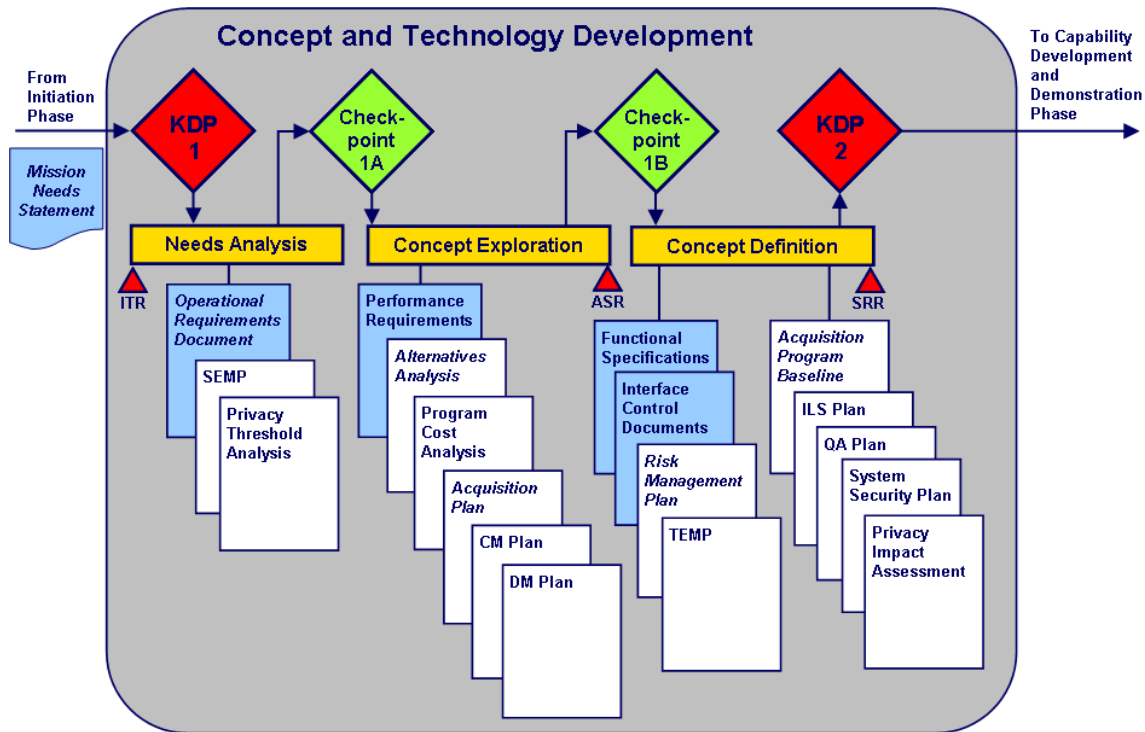


Figure 8. The Concept and Technology Development phase, expanded

The program documentation is depicted with the requirements documents highlighted in blue. Documents whose titles are in italics are mandated by MD1400, with the remaining documents representing industry best practice. Gates depicted as red diamonds are formal Key Decision Points defined in MD1400. Gates depicted as green diamonds are informal checkpoints which may be implemented by the program manager in the interests of program discipline. Technical reviews are depicted as red triangles. The acronyms are defined in the Glossary.

The Mission Needs Statement (MNS) is developed or refined during the Program Initiation Phase and is used to justify the Acquisition program to the appropriate Acquisition authority. The Operational Requirements Document (ORD) is developed during the Needs Analysis sub-phase, and represents a compromise that balances user needs against technological risk. The remaining requirements and specifications, which represent the engineering interpretation of the ORD, are developed later in the program, as depicted.

Further details concerning the Acquisition framework can be found in Appendix G and in MD1400.

The Acquisition framework assumes a conventional Acquisition program in which DHS controls the requirements and funds the system development and production, typically through a contract with a prime contractor. Such a model is appropriate where the end users are Federal employees under the management and control of a DHS Component, and where the product is sufficiently specialized that there is no commercial market. However, for end users in the private sector, such as the first-responder community, this model is unworkable because DHS cannot “deploy” to these users.

Tailored Product Life Cycle: Commercialization

As mentioned above, addressing capability gaps in user communities not under Federal control is impossible using a conventional Acquisition approach. Such users make independent buying decisions and procure commercial off-the-shelf (COTS) products and systems using conventional commercial channels, such as catalog and/or direct sales. In general, the private sector addresses the needs of these users without Government intervention, support, or subsidy. However, there are capability gaps that require Government intervention to cause a new COTS product to be developed and marketed by the private sector. DHS intervention in such cases may involve a combination of requirements development, technology transfers, grants programs, standards development, regulatory activism, and postings on DHS business and marketing vehicles.

It should be noted that the potential market for such new COTS products may be large, and is described in Appendix E which contains a briefing to industry used by S&T's Chief Commercialization Officer. Even when the users are Federal employees and therefore reachable by a conventional Acquisition approach, it may be in the Government's interest to prompt the private sector to address capability gaps by developing products and systems using their own funds, thus avoiding the up-front costs of an Acquisition program.

MD1400 is not relevant in such situations, as it does not apply when the major investments will be made by private-sector entities and by private-sector end users. Accordingly, S&T has developed a Commercialization framework which can be tailored to govern DHS support of product commercialization by the private sector. The phases of the framework are depicted in Figure 9, and the sub-phases are related to the 5 phases of the generic product life cycle (Requirements, Trades, Design, Test, and Implementation).

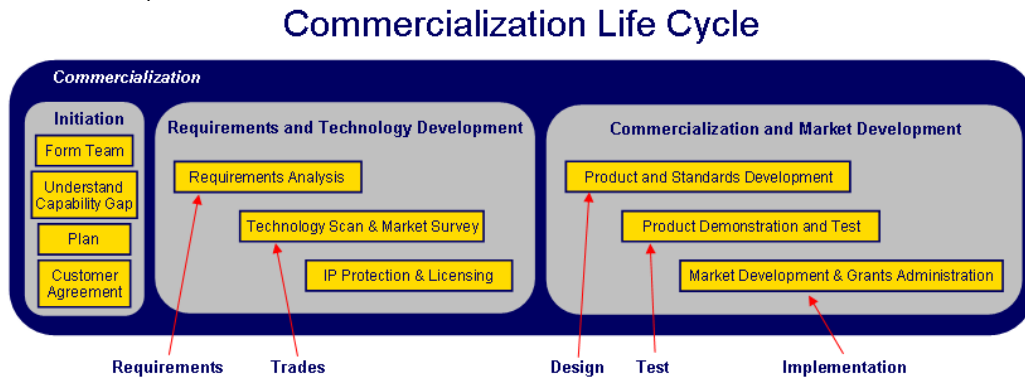


Figure 9. A product life cycle to govern Commercialization

Since our focus in this document is on requirements, we expand the Requirements and Technology Development sub-phase in Figure 10:

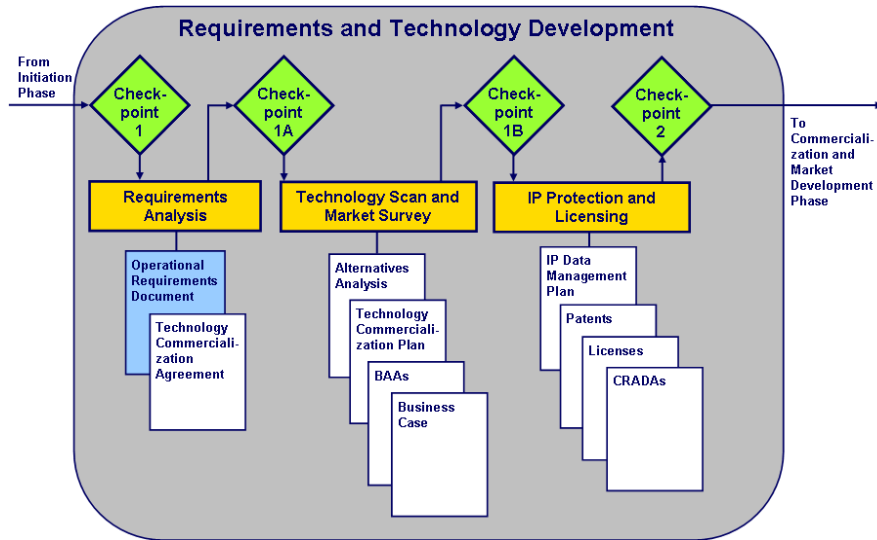


Figure 10. Expansion of the Req'ts and Tech. Development phase

Note that there is only one requirements document in this framework, which is the Operational Requirements Document (ORD) highlighted in blue. There is no required Mission Needs Statement because DHS has not formally acknowledged Commercialization as an alternative to Acquisition (as of this writing), though senior officials at DHS are closely monitoring pilot Commercialization programs. Nor are there downstream requirements and specifications (such as performance requirements and functional specifications) under DHS control, since the product or system development is done independently by a private-sector enterprise using their own funds and their own product realization or new product development process. The development of the ORD, however, proceeds in this framework just as it does in the Acquisition framework.

Another view of the Commercialization framework is depicted in Figure 11. It shows the program flow starting with the identification of a capability gap by a Capstone IPT and ending with the market availability and support of a new COTS product.

Commercialization Process

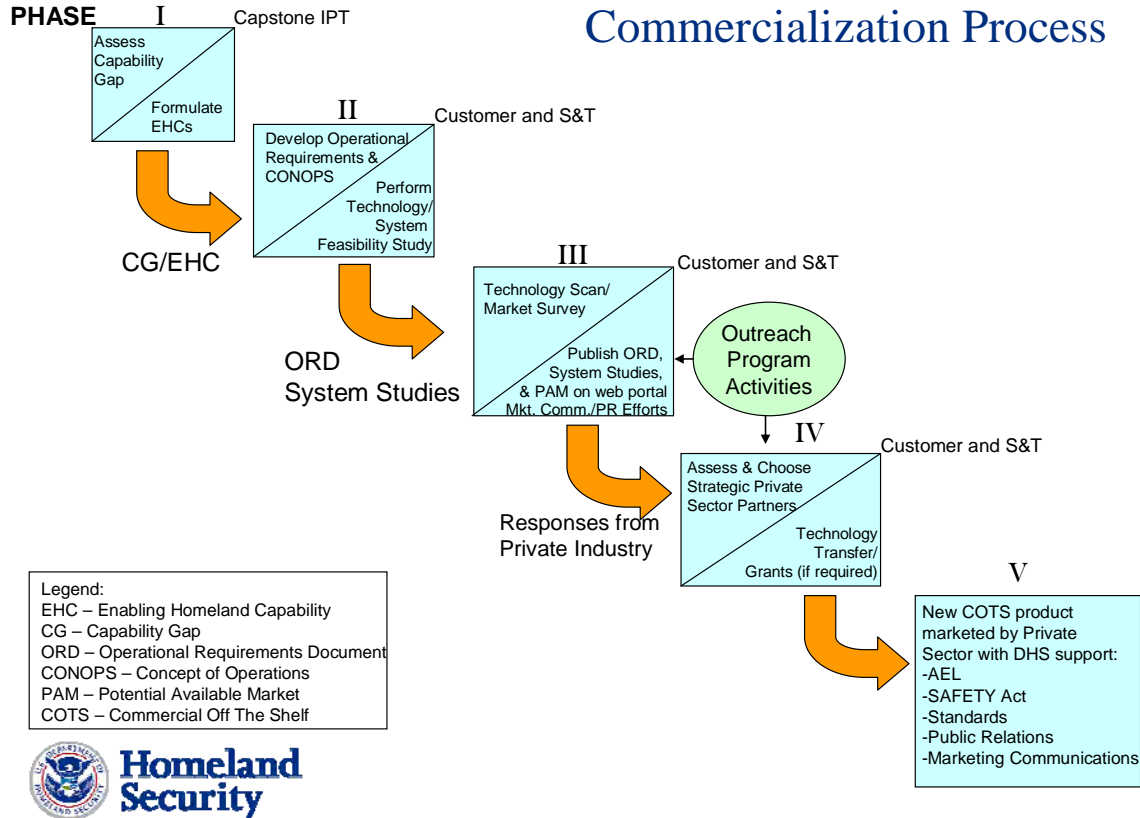


Figure 11. Another view of the Commercialization product life cycle

DHS-S&T has developed the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program that is designed to leverage the skills, productivity and resources of the private sector to develop new technologies, products or services aligned to DHS’ customer requirements. The SECURE Program (currently in the Pilot phase) allows private sector entities to develop products that are tailored specifically to address detailed operational requirements of DHS customers, validate T&E on their product, and enables end users to make informed decisions on products that meet their requirements. See Appendix F for the SECURE Program Concept of Operations.

Further details concerning Commercialization are found in Appendix C.

Tailored Product Life Cycle: Other Project Types

If a project’s goal is to develop an end-user system, the Acquisition and Commercialization frameworks described in the two preceding sections are relevant. However, in many cases, S&T’s customers do not task us to develop an end-user system but instead task us to execute only part of the product life cycle, such as:

- Develop a technology product for subsequent integration into an end-user system. (A “technology product” is not designed to be used by end users, but instead is intended to be integrated into end-user systems by their developers. An example would be a new type of sensor technology.)

- Assess a specific emerging threat as a prerequisite to requirements development for a system to address the threat. (An example of an “emerging threat” would be a new type of explosive undetectable by current screening systems.)
- Develop a standard to govern the testing, evaluation, and/or use of products or systems by end users, or to govern the application of grants programs. (Standards are adopted by industry groups, for example, to facilitate or ensure standardization of product features, interfaces, or test methods. They may also be used by DHS to aid in the implementation of grants programs.)

Each of these project variants has a specific product to be delivered to specific customers. Accordingly, it is appropriate to start project planning by considering the generic product life cycle (shown again below as Figure 12) and tailoring it to the specific product type to be developed.

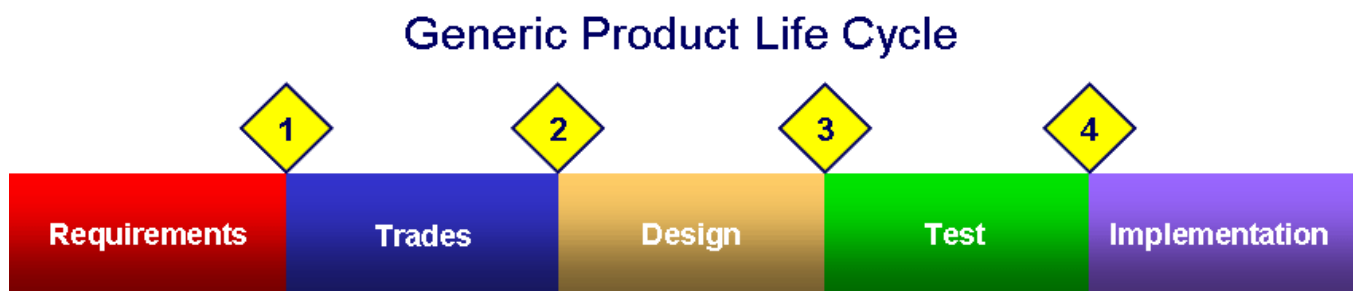


Figure 12. The generic product life cycle (revisited again)

- Requirements Phase
 - Regardless of the type of product, it will have requirements of some sort (though not “operational requirements” if it’s not a product which will be “operated”). These requirements should be elicited, analyzed, and documented in the Requirements Phase. As with operational requirements, these requirements (whatever form they take) are “owned” by S&T’s customer, who should play the principal role in their development.
- Trades Phase
 - Regardless of the type of product, there are likely to be several alternative ways of realizing it. These should be analyzed in the Trades Phase and the optimum approach chosen.
- Design Phase
 - Develop the product
- Test Phase
 - Assess the product’s conformance to its requirements and fitness for use
- Implementation
 - Implementation consists of some form of transition to the customer. Perhaps it’s integration of a technology product into a customer’s Acquisition or Commercialization program, or perhaps it’s simply the delivery of the documented results of a study.

Summary

This document has presented a brief summary of the role of requirements in product and system development, with particular emphasis on operational requirements governing the development of an end-user system. Acknowledging the difficulty of requirements development, it presented nine best practices to elicit requirements from an end-user community and eight criteria to judge the “goodness” of requirements. It also presented a generic product life cycle intended to govern the development of various types of products. It illustrated how this generic life cycle can be tailored in one way to govern an Acquisition program and tailored in another way to govern a Commercialization program. It also considered the development of technology products designed to enable, eventually, a more capable end-user system. Lastly, it considered the development of “knowledge products” such as studies of emerging threats or development of standards, which enables or augments a future Acquisition or Commercialization program.

Additional Requirements Development Readings

AntFarm, Inc. “Uncovering Hidden Customer Needs to Grow Your Services Business”. 2007.

http://www.antfarm-inc.com/docs/Growing_Services.pdf.

Byrd, T.A., Cossick, K.L. and Zmud, R.W. A Synthesis of Research of Requirements Analysis and knowledge Acquisition Techniques. MIS Quarterly, 16 (1). 117-138.

Coplenish Consulting Group. “New Product Best Practices: Over 100 Ideas for Better NPD”. 2004.

<http://www.coplenish.com/FreeStuffPages/npdbp.pdf>.

David. “Undreamt Requirements.” Weblog entry. David’s Software Development Survival Guide. March 12, 2007.

<http://softwaresurvival.blogspot.com/2007/03/undreamt-requirements.html>.

Davis, Alan. “Just Enough Requirements Management, Part I.” CodeGear. November 10, 2004.

<http://conferences.codegear.com/print/32301>.

Derby, Esther. Building a Requirements Foundation Through Customer Interviews. Amplifying Your Effectiveness. 2004.

<http://www.ayeconference.com/buildingreqtsfoundation/>.

Graham, Ian. Requirements Engineering and Rapid Development: An Object Oriented Approach. Addison-Wesley Professional. 1999.

Japenga, Robert. “How to Write a Software Requirements Specification.” Micro Tools, Inc. 2003.

<http://www.microtoolsinc.com/Howsrs.php>.

Korman, Jonathan. “Putting People Together to Create New Products.” Cooper. 2001.

http://www.cooper.com/insights/journal_of_design/articles/putting_people_together_to_cre.html.

- Kotonya, G. and Sommerville, I. Requirements Engineering: Processes and Techniques. John Wiley & Sons, 1998.
- Larson, Elizabeth, and Richard Larson. "Projects Without Borders: Gathering Requirements on a Multi-Cultural Project." The Project Manager Homepage. August 3, 2006.
<http://www.allpm.com/print.php?sid=1587>.
- Miller, Hal. "Customer Requirements Specifications." The Usenix Magazine. Vol. 30, No. 2. 2004.
<http://www.usenix.org/publications/login/2005-04/pdfs/miller0504.pdf>.
- Olshavsky, Ryan. "Bridging the Gap with Requirements Definition." Cooper. 2002.
http://www.cooper.com/insights/journal_of_design/articles/bridging_the_gap_with_requirem_1.html .
- Pande, Peter S., Robert Neuman, and Roland Cavanagh. "Defining Customer Requirements: Six Sigma Roadmap Step 2." *The Six Sigma Way: How GE, Motorola, and Other Top Companies are Honing Their Performance*. McGraw-Hill, New York. 2000.
<http://www.sixsig.info/research/chapter13.php>.
- "Requirements analysis." *Wikipedia, The Free Encyclopedia*. Wikimedia Foundation, Inc. April 8, 2008.
http://en.wikipedia.org/w/index.php?title=Requirements_analysis&oldid=204196812.
- Sehlhorst, Scott. "Elicitation Techniques for Processes, Rules, and Requirements." Weblog entry. Tyner Blain. September 13, 2007.
<http://tynerblain.com/blog/2007/09/13/elicitation-techniques-2/>.
- Sehlhorst, Scott. "Ten Requirements Gathering Techniques." Weblog entry. Tyner Blain. November 21, 2006.
<http://tynerblain.com/blog/2006/11/21/ten-requirements-gathering-techniques/>.
- Silverman, Lori L., "Customers or Consumers? Focus, or Obsession?" Partners for Progress. 2000.
<http://www.partnersforprogress.com/Articles/Customers%20or%20Consumers.pdf>.
- Sisson, Derek. "Requirements and Specifications". Philosophe.com. January 9, 2000.
<http://www.philosophe.com/design/requirements.html>.
- U.S. Department of Defense. Defense Acquisition Guidebook, Chapter 4. Dec. 2004.
https://akss.dau.mil/DAG/TOC_GuideBook.asp?sNode=R&Exp=Y.
- Ward, James. "It Is Still the Requirements: Getting Software Requirements Right." Sticky Minds. June 7, 2005.
http://www.stickyminds.com/s.asp?F=S9150_ART_2.
- Wieggers, Karl E., and Sandra McKinsey. "Accelerate Development by Getting Requirements Right." 2007.

<http://www.serena.com/docs/repository/products/dimensions/accelerate-developme.pdf>.

Wilson, William. "Writing Effective Requirements Specifications." NASA Software Assurance Technology Center. April 1997.
http://satc.gsfc.nasa.gov/support/STC_APR97/write/writert.html.

Winant, Becky. "Requirement #1: Ask Honest Questions." Sticky Minds. April 3, 2002.
http://www.stickyminds.com/s.asp?F=S3264_COL_2.

Glossary

Alternative Systems Review (ASR). The ASR is a multi-disciplined technical review, conducted at the end of the Concept Exploration phase, to ensure that the Operational Requirements Document agrees with the customers' needs and expectations and that the system under review can proceed into the Concept Definition phase. Generally, this review assesses the alternative systems that have been evaluated during the Concept Exploration phase, and ensures that the preferred system alternative is cost effective, affordable, operationally effective and suitable, and can be developed to provide a timely solution to a need at an acceptable level of risk.

Commercial Off-the-Shelf (COTS) Products are products which are commercially available and which can be procured through retail sales channels.

Concept of Operations (CONOPS). Normally a part of the ORD, the CONOPS is a formal document that identifies the end users, describes their skill levels and environment, and describes how the proposed product or system will be used in the field to accomplish the intended mission. The CONOPS may also include relationships with other systems or entities, information sources and destinations, and other relationships or constraints.

Configuration Management (CM). The discipline of identifying the configuration of a hardware/software system at each life cycle phase for the purpose of controlling changes to the configuration and maintaining the integrity and traceability of the configuration through the entire life cycle.

Data Management (DM). The goals of data management include providing accurate, efficient, and effective information and support for resource management and protection. Resource managers need to know: what data are available, in development, or stored; the quality, timeliness, and uses of the data; how to incorporate this data into resource management decisions; and how the data will be managed over time.

Developmental Test and Evaluation (DT&E). Any engineering test used to verify status of technical development, verify that design risks are minimized, substantiate achievement of technical performance and certify readiness for OT&E. Developmental tests generally require instrumentation and measurements and are accomplished by engineers, technicians, or operators in a controlled environment to facilitate failure analysis. One purpose of DT&E is to verify that the test item conforms to its technical requirements, including performance requirements and functional specifications.

End User. The field operator who will actually use the product or system in an operational environment. Examples include border protection agents, firefighters, and Coast Guard sailors.

Initial Technical Review (ITR). The ITR is a multi-disciplined technical review, conducted at the outset of the Concept and Technology Development phase, to assess the mission needs and conceptual approach of a proposed program and to verify that the requisite research, development, test, engineering, logistics, and programmatic bases for the program reflect the complete spectrum of technical challenges and risks. Additionally, the ITR ensures that historical and prospective drivers of system cost have been quantified to the maximum extent and that the range of uncertainty in these parameters has been captured and reflected in the program cost estimates.

Integrated Logistics Support (ILS). The discipline which plans for and provides the infrastructure and material resources needed to support a system in the field.

Key Decision Point (KDP). Critical milestones throughout the DHS Investment Review Process, defined in MD 1400.

Mission Need Statement (MNS). A core DHS document that provides a high-level description of the mission need, whether from a current or impending gap, based on business-case planning. This document, prepared by the Component, outlines only the concept of the solution to fill the gap and does not provide information on expected Acquisitions. [Source: DHS *Investment Review Process*, DHS MD1400.]

Objective. The desired value for a specific requirement. See also “Threshold,” which is the minimum acceptable value.

Operational Requirements Document (ORD). The ORD is a formal document, which describes in detailed quantitative terms what the intended system must be able to do and how it is intended to be used (defined in the CONOPS). The ORD provides a bridge between the high-level operational requirements in the MNS and the detailed system technical specifications. The MNS and ORD are written by the sponsor, whereas the technical specifications are written by the system developer. The ORD establishes absolute minimums (“thresholds”) below, which the mission cannot be successfully performed, and sets goals (“objectives”) to define an operationally effective system.

Operational Test and Evaluation (OT&E). The field-test, under realistic conditions, of any product, system, or key component for the purpose of determining effectiveness and suitability for use by typical users and the evaluation of the results of such a test. One purpose of OT&E is to validate that the test item conforms to a system's ORD.

Quality Assurance. The discipline used by program management to objectively monitor, control, and gain visibility into the development or maintenance process.

Requirement. A condition or capability that must be met or possessed by a system, product, service, result, or component to satisfy a contract, standard, specification, or other formally imposed documents. Requirements include the quantified and documented needs, wants, and expectations of the sponsor, customer, and other

stakeholders. [Source: *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*, Third Edition, 2004.]

Specification. A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system, component, product, result, or service and, often, the procedures for determining whether these provisions have been satisfied. Examples are: requirement specification, design specification, product specification, and test specification. [Source: *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*, Third Edition, 2004.]

Sponsor. The sponsor represents the operational needs of the Component and, ultimately, the end-users of the required system. The sponsor conducts mission analyses, identifies capability gaps, conducts requirements analyses, and participates in the long-range planning process and the prioritization of needs. The sponsor's final requirements are formally documented in an operational requirements document, and the sponsor participates in all phases of the Acquisition to ensure that the item or system being acquired meets operational requirements. [Source: *Investment Review Process*, DHS MD1400.] Typically, the sponsoring organization is a DHS Component with an operational mission. From the perspective of the S&T Directorate, these DHS Components are the customers for S&T's products, so S&T tends to use the terms "sponsor" and "customer" interchangeably.

System Requirements Review (SRR). The SRR, conducted at the end of the Concept Design phase (and therefore at the end of the Concept and Technology Development phase), assesses progress in defining system technical requirements. This review determines the direction and progress of the systems engineering effort and the degree of convergence upon a balanced and complete configuration.

Systems Engineering Management Plan (SEMP). A formal document that describes a project's process and plan for the technical development of a system. It typically includes sections on planning, requirements analysis, functional analysis and allocation, synthesis, systems analysis and systems control.

Test and Evaluation Master Plan (TEMP). A formal document that identifies a project's test and evaluation tasks and activities so that the entire product or system can be adequately tested to assure a successful implementation.

Threshold. The minimum acceptable value for a specific requirement, below which the product is considered a failure. See also "Objective," which is the desired value.

Appendix A: Operational Requirements Document (ORD) Template

1. General Description of Operational Capability

In this section, summarize the capability gap which the product or system is intended to address, describe the overall mission area, describe the proposed system solution, and provide a summary of any supporting analyses. Additionally, briefly describe the operational and support concepts.

1.1. Capability Gap

Describe the analysis and rationale for acquiring a new product or system, and identify the DHS Component, which contains or represents the end users. Also, name the Capstone IPT, if any, which identified the capability gap.

1.2. Overall Mission Area Description

Define and describe the overall mission area to which the capability gap pertains, including its users and its scope

1.3. Description of the Proposed System

Describe the proposed product or system. Describe how the product or system will provide the capabilities and functional improvements needed to address the capability gap. Do not describe a specific technology or system solution. Instead, describe a conceptual solution for illustrative purposes.

1.4. Supporting Analysis

Describe the analysis that supports the proposed system. If a formal study was performed, identify the study and briefly provide a summary of results.

1.5. Mission the Proposed System Will Accomplish

Define the missions that the proposed system will be tasked to accomplish.

1.6. Operational and Support Concept

1.6.1. Concept of Operations

Briefly describe the concept of operations for the system. How will the system be used, and what is its organizational setting? It's appropriate to include a graphic that depicts the system and its operation. Also, describe the system's interoperability requirements with other systems.

1.6.2. Support Concept

Briefly describe the support concept for the system. How will the system (hardware and software) be maintained? Who will maintain it? How, where, and by whom will spare parts be provisioned? How, where, and by whom will operators be trained?

2. Threat

If the system is intended as a countermeasure to a threat, summarize the threat to be countered and the projected threat environment.

3. Existing System Shortfalls

Describe why existing systems cannot meet current or projected requirements. Describe what new capabilities are needed to address the gap between current capabilities and required capabilities.

4. Capabilities Required

4.1. Operational Performance Parameters

Identify operational performance parameters (capabilities and characteristics) required for the proposed system. Articulate the requirements in output-oriented and measurable terms. Use Threshold/Objective format and provide criteria and rationale for each requirement.

4.2. Key Performance Parameters (KPPs)

The KPPs are those attributes or characteristics of a system that are considered critical or essential. Failure to meet a KPP threshold value could be the basis to reject a system solution.

4.3 System Performance.

4.3.1 Mission Scenarios

Describe mission scenarios in terms of mission profiles, employment tactics, and environmental conditions.

4.3.2 System Performance Parameters

Identify system performance parameters. Identify KPPs by placing an asterisk in front of the parameter description.

4.3.3 Interoperability

Identify all requirements for the system to provide data, information, materiel, and services to and accept the same from other systems, and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

4.3.4 Human Interface Requirements

Discuss broad cognitive, physical, and sensory requirements for the operators, maintainers, or support personnel that contribute to, or constrain, total system performance. Provide broad staffing constraints for operators, maintainers, and support personnel.

4.3.5 Logistics and Readiness

Describe the requirements for the system to be supportable and available for operations. Provide performance parameters for availability, reliability, system maintainability, and software maintainability.

4.3.6 Other System Characteristics

Characteristics that tend to be design, cost, and risk drivers.

5. System Support

Establish support objectives for initial and full operational capability. Discuss interfacing systems, transportation and facilities, and standardization and interoperability. Describe the support approach including configuration management, repair, scheduled maintenance, support operations, software support, and user support (such as training and help desk).

5.1 Maintenance

Identify the types of maintenance to be performed and who will perform the maintenance. Describe methods for upgrades and technology insertions. Also address post-development software support requirements.

5.2 Supply

Describe the approach to supplying field operators and maintenance technicians with necessary tools, spares, diagnostic equipment, and manuals.

5.3 Support Equipment

Define the standard support equipment to be used by the system. Discuss any need for special test equipment or software development environment

5.4 Training

Describe how the training will ensure that users are certified as capable of operating and using the proposed system.

5.5 Transportation and Facilities

Describe how the system will be transported to the field, identifying any lift constraints. Identify facilities needed for staging and training.

6. Force Structure

Estimate the number of systems or subsystems needed, including spares and training units. Identify organizations and units that will employ the systems being developed and procured, estimating the number of users in each organization or unit.

7. Schedule

To the degree that schedule is a requirement, define target dates for system availability. If a distinction is made between Initial Capability and Full Operational Capability, clarify the difference between the two in terms of system capability and/or numbers of fielded systems.

8. System Affordability

Identify a threshold/objective target price to the user at full-rate production. If price is a KPP, include it in the section on KPPs above.

Signatures

Sponsor's Acquisition Program Manager [print and sign] Date

Sponsor's Representative [print and sign] Date

S&T Project Manager [print and sign] Date

S&T Division Head [print and sign] Date

Appendix B: Acquisition Mini-Course

The following pages include the slides and slide notes used in teaching the S&T hour-long mini-course on Acquisition.

Slide 1

Acquisition
What it is and how S&T supports it



Sam Francis
samuel.francis@associates.dhs.gov
March 25, 2008



revised 4/1/08

This mini-course is one of a series of about a dozen, sponsored by the S&T Office of Strategy, Planning, and Integration.

The briefing takes an hour, and will start and stop on time, so make sure any questions are for general clarification. The speaker will remain for 30 minutes after the end for discussion, if desired.

Hard copies of the slides will be handed out. The slides are also available from the RDT&E web site (click on Training and follow your nose). To browse the RDT&E web site, double-click on "Shared\RDT&E Process Website\index.htm" (then bookmark). Please sign the sign-in sheet.


Today we'll be talking about Acquisition, which is one of two principal methods by which S&T's technologies can find their way to the user. (The other method is via COTS, enabled by technology transfer, which we'll talk about in another session.)

Acquisition can be confusing because the word is used to mean different things and is often confused with procurement. The next slide addresses this confusion.

Big “A” and Little “a” Acquisition

Big “A” Acquisition (sometimes called “program acquisition”) is a requirements-based process that encompasses everything a program must accomplish from requirements analysis, planning, systems engineering, technology and system development, budgeting, *procurement*, logistics support, testing, system safety, maintenance, *through* production and deployment and plan for disposal.

Little “a” acquisition (also called “stand-alone acquisition”) is, basically, buying stuff. OPO requires an Acquisition Plan for Little “a” (subject to thresholds), but don’t confuse Little “a” with Big “A.”

 2

“Acquisition” is one of those words, like “research”, “transition,” “program,” and “project” which are in the common vernacular and used by different people to mean different things. Where precision is useful, these words have to be defined more precisely. So let’s avoid some confusion by defining the two contexts in which the word “acquisition” is used.

Little “a” acquisition is basically a procurement action to buy existing products or services. OPO requires documentation (e.g., an acquisition plan and/or an alternatives analysis) to demonstrate that you’ve thought through what you’re buying and are making good choices, but it’s a relatively straightforward and low-risk procurement.


Big “A” acquisition is a process to acquire a product or system which must be developed to a set of requirements. It’s much higher-risk than Little “a” acquisition, and requires disciplined program management to manage the risk and assure the outcome.

In short, Little “a” acquisition is buying stuff that exists, and Big “A” acquisition is buying stuff that doesn’t yet exist.


Slide 3

S&T's Role in Acquisition ... Common Questions

- Do we execute any part of Acquisition?
- If so, when and how?
- If not, how can our technologies get to users?
- Does the Capstone IPT diagram refer to Big "A" or Little "a"? Why is S&T on the opposite side of the table?
- What does an EHC "enable?"



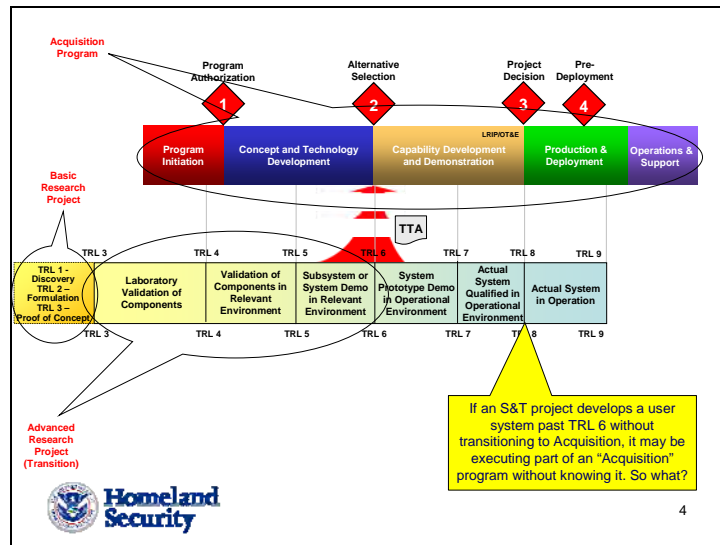
Let's understand the path from invention to the user by starting with Technology Readiness Levels.



3

There are exceptions to all blanket statements regarding RDT&E (which is why the unofficial motto of the Defense Acquisition University is "it depends"). But, here's a blanket statement... Except for COTS, Acquisition is the only path for technology to get to the users. So if we don't execute any part of Acquisition, the only way for our technology to reach the users is through someone else's Acquisition program. Hence, it's critical that S&T be effective in transitioning to Acquisition. Without transition, we cannot influence Homeland Security in any significant way. It's also critical that our customers become expert at Acquisition. If the customer has no effective Acquisition program, there's nothing for S&T to transition to. Even if we aren't executing any part of an Acquisition program, we need to understand Acquisition so we can interface with it (or even know when a customer's Acquisition program doesn't exist or isn't viable). And, by the way, just who does sit in that seat labeled "Acquisition" on the other side of the table? By the end of this hour, we'll come back to these questions and see if we have answers. The next slide will allow us to take a look at the path that technology takes from invention to the users, and note where it leaves the S&T track and enters the Acquisition track.

Slide 4



This slide builds, so it is best viewed in PowerPoint’s “slide-show mode.”

TRL is a 9-point scale measuring technology maturity. For example, a modern cell phone is at TRL 9. In 1975, the prototype cell phone (at TRL 2) was a Ford van with a minicomputer inside and an antenna on top. Mobile phone technology matured through proof of concept (TRL 3), laboratory analyses and experiments, field experiments, etc., to the mature product you use today. There is no way, at TRL 2, to create a program plan through TRL 8 or 9, because there’s too much uncertainty. So you take it a step at a time (Basic Research, then Applied Research, then Acquisition). It’s all about risk reduction.

In interpreting this diagram, don’t forget the unofficial motto of DAU – “It depends.” For example, the TRL at transition could be earlier than TRL 6 if the benefit is worth the added risk.

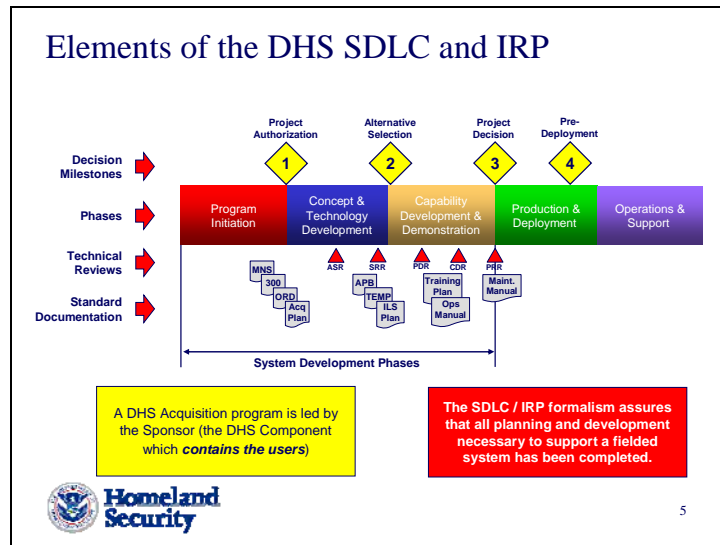
You transition to Acquisition at TRL 6 (roughly) because (a) the risk is low enough, and (b) you haven’t started final system design yet. When you’re doing final system design, you need the planning and controls that the SDLC and IRP include. At TRL 7, by definition, you’ve demonstrated a prototype near or at planned operational system, in an operational environment. If you’re that far along, the system development should be inside the Acquisition program.

Note that there’s “technology development” in the Acquisition program (CTD) phase and also in the Advanced Research project. How do they relate? “It depends.” How does the new technology enter the Alternatives Analysis in CTD? Or does it? “It depends.” Perhaps the technology development by S&T outside the Acquisition program is not on the critical path, and not necessary for the Acquisition (so that if it fails, the Acquisition still proceeds).

Sponsors are responsible for Acquisition programs because 85% of the life-cycle costs are in their domain (Production, Deployment, Operations, and Support). If the Sponsor doesn’t need the system badly enough to pay for these large out-year costs, there’s no point in developing a system.

You don’t develop a production-ready user system without entering the SDLC, and thereby submitting yourself to the IRP. Otherwise, you might end up with a system ready to ship but without any logistics system in the field. No maintenance techs, no spare parts, no manuals, no troubleshooting equipment, no user training. Also no environmental requirements. Even worse, no life-cycle funding! In other words, an Applied Research project developing a “production-ready design” of an operational system is a sneak path to the field, which is generally a bad idea (though, of course, “it depends”).

Slide 5



This chart shows the 4 elements of the SDLC/IRP: decision milestones, phases, technical reviews, and documentation. It's a good example of a phase-gate process (just like DoD 5000, after which it's modeled).

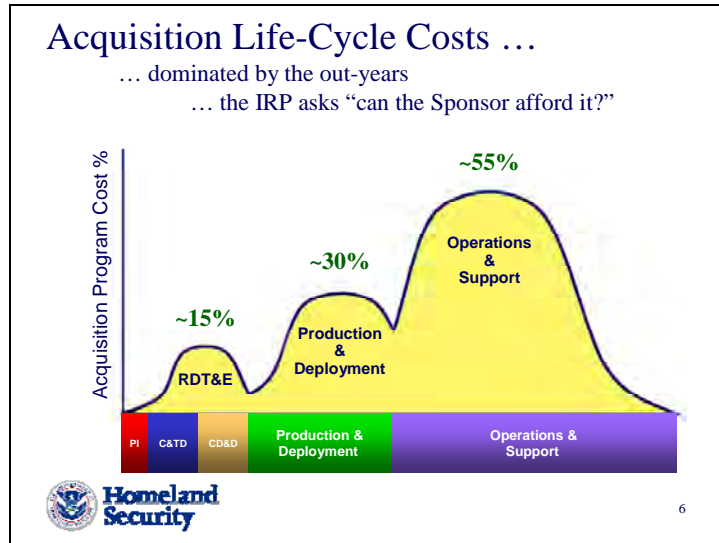
The Sponsor is responsible for Production, Deployment, Operations, Support, since the Sponsor is the DHS Component which contains (or represents) the end users. S&T is almost never the Acquisition Sponsor, because we don't operate systems in the field, and therefore don't fund the big-dollar phases (P&D and O&S). Generally the only Acquisitions for which S&T would be the Sponsor would be acquisition of facilities (such as NBAF, which is to replace Plum Island Animal Disease Center).

We may execute the "System Development Phases" (shown), if the Sponsor asks us to manage that part of the life cycle. But we do that as a "subcontractor" to the Sponsor, who is responsible for the requirements and the out-year funding (even if we budget for design and development). The importance of executing system development INSIDE AN ACQUISITION PROGRAM is that the formalism forces certain best practices, such as operational requirements development, out-year funding, logistics planning, etc. If a system prototype is developed by S&T without linkage to an Acquisition program, the likely outcome is an unsupported system which also may not be compliant with the users' operational requirements.

This is a good time to reflect on the concept of "tailoring." There are almost no hard-and-fast rules in RDT&E management. The caveat to almost every rule or guideline is "it depends." R&D processes are not like manufacturing processes, designed to produce the same output over and over again. On the production line, innovation is anathema, since production processes must be tightly controlled. But R&D is different. Unlike a production process, which must produce the same thing many times, an R&D process must produce the same thing ONCE. Thus, there aren't really R&D processes, which dictate what you must do, but R&D management frameworks, providing guidelines within which projects are planned and executed. The framework provides a structure, a common vocabulary, checklists, templates, and best practices, but it's not intended to be prescriptive. The project manager must be expected to have the wisdom and experience to decide what elements of the framework are appropriate for his/her project. For example, if the project doesn't require configuration management (CM), then tailor out the CM Plan, but be prepared to defend that decision. Or if an alternatives analysis isn't felt to be necessary, then tailor out the concept exploration phase, and be prepared to defend *that* decision when someone asks "why didn't you consider this alternative approach?"

Acronyms: ASR = Alternative Systems Review, SRR = System Requirements Review, PDR = Preliminary Requirements Review, CDR = Critical Design Review, PRR = Production Readiness Review

Slide 6

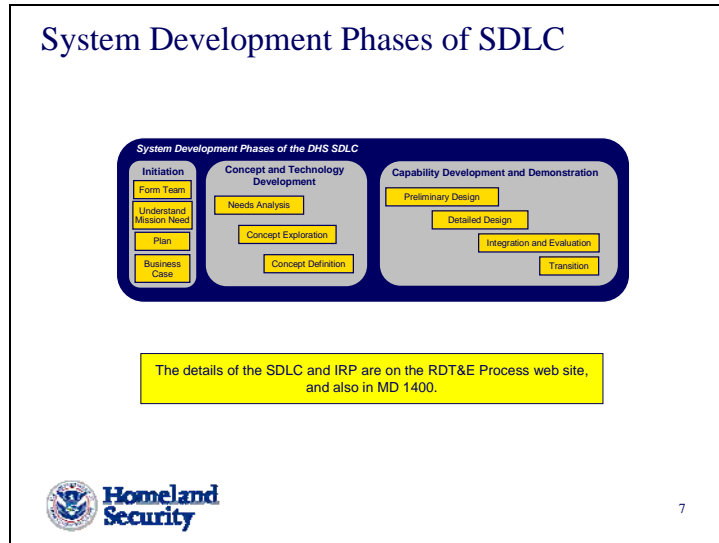


There's little point doing RDT&E to develop a system if the Sponsor can't afford the life-cycle costs. For most systems the majority of cost is incurred in O&S.

In Program Initiation, the IRP requires the Sponsor to create a Business Case (typically, an Exhibit 300), forcing the Sponsor to consider the entire life cycle. If S&T is responsible for the RDT&E phases, the Sponsor needs S&T's help in estimating the life-cycle costs.

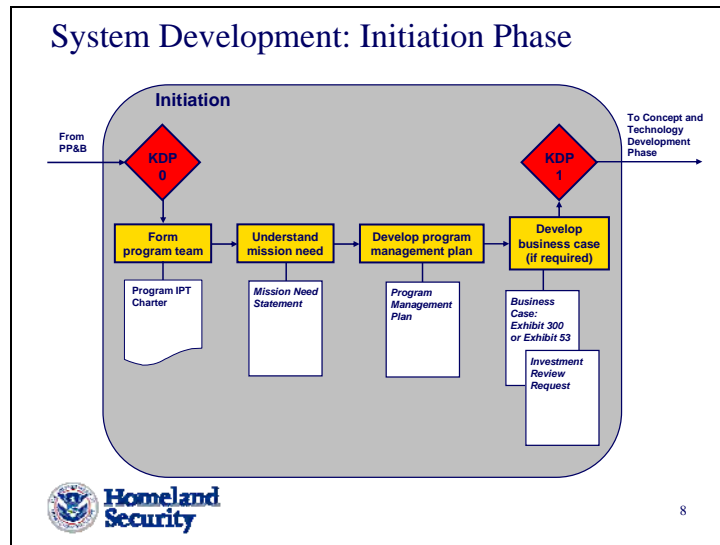
The DHS system development life cycle doesn't explicitly include disposal costs, but they may be sizeable and should not be ignored.

Slide 7



This slide is the first one to show a graphic from the RDT&E web site, and therefore is a good segue to the site. Note that the three phases shown here (“Initiation,” etc.) are the first three phases of SDLC shown on the previous slide, and that on the web site you find more explanation and detail by drilling down. Down to a certain level of detail, the web site simply provides a user-friendly version of the DHS SDLC and MD 1400, “Investment Review Process”. Below that level of detail, standard systems engineering best practices are included. (For example, the three sub-phases of C&TD – “Needs Analysis” etc. – are not part of the SDLC but are simply textbook systems engineering, integrated with the SDLC.)

Much of the textbook systems engineering on the web site is taken from Kossiakoff and Sweet, *Systems Engineering Principles and Practice*, but any good systems engineering text will serve, if more details are desired. Another standard text is Blanchard and Fabrycky, *Systems Engineering and Analysis*.



This graphic will be discussed when viewing it on the web site. "Initiation" is the first phase of system development. The red diamonds are the IRP's decision milestones, called "Key Decision Points." The identification of the decision authority depends on the size (i.e., Level) of the investment. Show the table which defines the levels, by clicking on the "Acquisition" link and scrolling down.

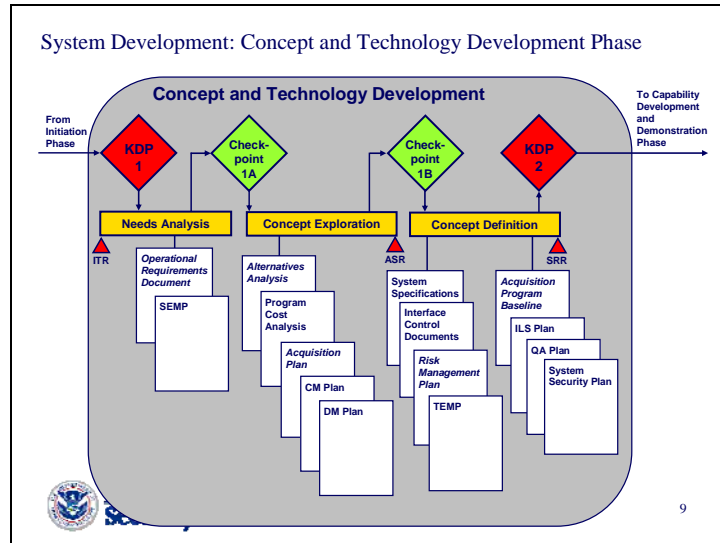
The program team is really an IPT, representing all important functional disciplines and stakeholders (including, as appropriate, representation from program management, engineering, T&E, users, contracting, procurement, production, logistics, etc.).

Obviously, representatives from industry join the IPT after award.

The top-level statement of the need is in a Mission Need Statement, for which a template is provided.

A business case is required for large investments, typically an Exhibit 300 generated by the Sponsor (with support from S&T if involved in system development). Then, at KDP 1, triggered by an Investment Review Request, the milestone decision authority reviews the business case to verify the need for the system as well as the availability of out-year funding for the life-cycle costs.

Slide 9



This graphic will be discussed when viewing it on the web site. C&TD consists (in S&T's version) of three sub-phases:

Needs Analysis develops an Operational Requirements Document (including a CONOPS) and assesses the feasibility of developing a compliant system. Titles in italics are required by the IRP; other titles (e.g., SEMP) have been added by S&T and are optional. The program manager tailors the phases, reviews, and documentation to suit the size, importance, and risk of the program.

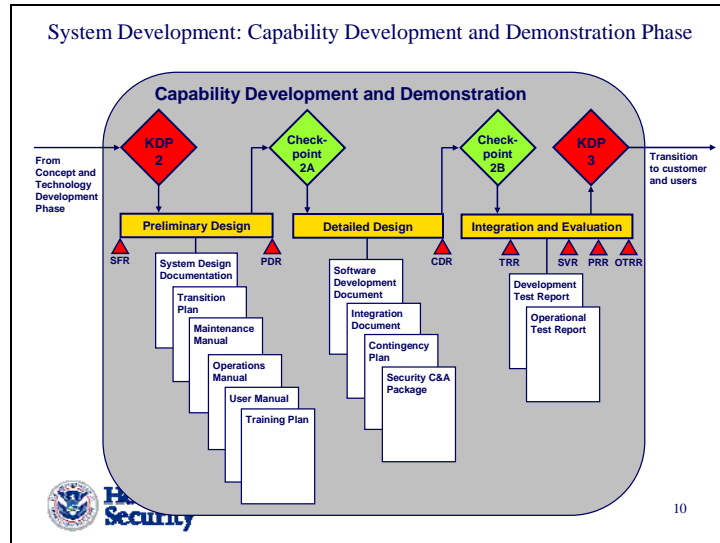
Concept Exploration explores alternative concepts and chooses the best one, documented in an Alternatives Analysis. Typically, system concepts are defined only down to the subsystem level during Concept Exploration. An Acquisition Plan is developed, documenting the acquisition strategy.

Concept Definition accomplishes the systems engineering necessary to define subsystems and components, flow down functional requirements, and define interface requirements. Test planning is started (in the form of a draft TEMP) and logistics planning (in the form of a draft ILS Plan).

Note the green diamonds between sub-phases, called "checkpoints." These are milestones at which the project/program manager looks back and looks ahead. Looking back, he/she verifies, by means of checklist reviews, that all necessary activities and documentation have been completed in the preceding sub-phase. Looking ahead, he/she reviews the plans, activities, and deliverables during the next phase to ensure that these are planned and understood, and that there are adequate resources (funding, facilities, and people) to execute.

The C&TD phase ends at Key Decision Point 2, at which the milestone decision authority verifies that the program team has accomplished and documented the necessary activities and produced the necessary work products. The milestone decision authority ensures that any process tailoring done by the program team has not increased program risk unduly. (For example, did the program team "tailor out" the concept exploration and alternatives analysis? If so, why?)

Acronyms ITR = Initial Technical Review, ASR = Alternative Systems Review, SRR = System Requirements Review



This graphic will be discussed when viewing it on the web site. CD&D consists of three sub-phases:

Preliminary Design (sometimes called “Advanced Development”), is that part of the SDLC in which the great majority of the uncertainties inherent in the selected system concept are resolved through analysis, simulation, development, and prototyping. Its goal is to develop and validate a sound technical approach and demonstrate it during PDR to those who must authorize the full-scale development of the system. System requirements are flowed down through subsystems, components, and sub-components, and functional allocation is adjusted as the capabilities of the system elements are proven (or not).

Detailed Design (sometimes called “Engineering Design”) is that part of the SDLC in which all the component parts of the system are designed so that they will fit together as an operating whole that satisfies the ORD. Detailed internal and external interfaces are established and confirmed, and the design is first fully implemented in hardware and software. This phase culminates in a CDR.


Integration and Evaluation is that part of the SDLC in which the engineered components of the new system are assembled and integrated into an effectively operating whole, which undergoes DT&E (to verify compliance with technical specifications) and OT&E (to verify compliance with the operational specifications in the ORD when the system is operated in the field by its intended users). During this phase, Low-Rate Initial Production (LRIP) may be authorized, so that the OT&E is conducted on a production unit (often the first article). OT&E should be conducted by a testing agent independent of the development team.

At the end of this phase, the milestone decision authority at KDP 3 authorizes the release of the design to full production, after verifying successful DT&E and OT&E by reviewing test plans and test reports.

Acronyms SFR = System Functional Review, PDR = Preliminary Design Review, CDR = Critical Design Review, TRR = Test Readiness Review, SVR = System Verification Review, PRR = Production Readiness Review, OTRR = Operational Test Readiness Review

Recapping the Process

- Simply stated, system development for an Acquisition program is a 6-step process:
 - Requirements
 - Concept exploration
 - Concept selection and refinement
 - Preliminary design
 - Detailed design
 - Test and evaluate
- Generically, almost every R&D project executes these steps in some form
 - More formal in Acquisition programs (higher TRLs), to reduce risk
 - Less formal for early TRLs, to provide flexibility



11

Having shown and discussed details of the system development phases of an Acquisition program, we'll step back and recap.

System development consists of 6 steps, which actually aren't specific to Acquisition but are executed in one form or another in almost all R&D.

Define the requirements. There are requirements, of a sort, in almost all projects, even as early as TRL 1. For example, the Wright brothers' requirements were twofold: It has to be heavier than air, and it has to get off the ground.

Explore alternative concepts, to make sure that you aren't jumping to a preconceived solution and missing a better one.


Choose the favored concept (best balance of cost, schedule, risk, performance) and, if appropriate, do the system design (identify subsystems and components, and flow down requirements).

Execute preliminary design, emphasizing the immature technologies to reduce risk.

Execute detailed (final) design.

Integrate and test against the requirements, making sure that the relationship between the developers and the testers isn't cozy.

Review of Earlier Questions	
Question	Answer
Does S&T execute any part of Big "A" Acquisition? If so, when and how?	Commonly, no, but occasionally, yes, we may manage the system development (the C&TD and CD&D phases) if requested to do so by the Sponsor, subject to the availability of adequate funding. In such cases, we follow DHS's SDLC, and the Sponsor is responsible for compliance with the IRP.
If we don't execute Acquisition, how can our technologies get to users?	By executing an Advanced Research project and transitioning the product to a customer's Acquisition program, subject to a Technology Transition Agreement. To create a good TTA we must understand the Acquisition process in general and the customer's Acquisition program in particular.
Does the Capstone IPT diagram refer to Big "A" or Little "a"?	Big "A" (because if it were Little "a," the customer would simply execute a procurement without the need for S&T involvement).
Why is S&T on the opposite side of the table from Acquisition?	Because Acquisition is the Sponsor's responsibility, not S&T's. At most, S&T executes the system development phases of Acquisition, if requested.
What does an EHC "enable?"	An EHC, consisting of one or more technology products from S&T Applied Research projects, "enables" the customer's Acquisition program to produce a more capable system.


12

These are the questions first posed on slide 3. Below are some amplifying comments for each Q&A (numbered 1 to 5 to correspond with the 5 questions).

Since the only way that technology can get to the user, it's critical that effective Acquisition programs be executed (by somebody). However, since Big "A" Acquisition is expensive, S&T's budget typically is inadequate to fund a full-fledged system development leading to a fully sustainable and production-ready design. This is an issue which must be addressed case by case, realizing that if an effective Acquisition program is not executed, no technology can improve Homeland Security.

The transition of our product to a customer's Acquisition program is very difficult, and requires us to understand the customer's program and what they need, in depth. What are the complete requirements (not just functionality, but also interface requirements, environmental requirements, and ilities)? Do they need a production-ready design? If so, how will production-readiness be demonstrated? Do they need S&T to develop a supplier who can be integrated into their Acquisition program? Or will the product be handed off to a system prime by S&T's supplier, in which case can it be effectively integrated and manufactured?

This one is pretty self-explanatory, once you understand Big "A" Acquisition.

So is this one.

The subtleties of EHCs will be addressed in another mini-course. Suffice it to say that the term "enabling" is intended to imply that S&T's product augments the customer's system development some important way, providing an important increment of capability which would be otherwise unachievable. It's important to understand whether S&T's technology development is on the customer's critical path (in which case "enable" may mean that the EHC makes the customer's system development possible) or whether S&T's technology development is supplementary (in which case S&T's technology development will allow the customer's system to be more capable than it otherwise would be, but if S&T's development fails or is late, the customer's system development will still proceed, resulting in less capability but still providing a useful performance increment).

Appendix C: Commercialization Mini-Course

The following pages include the slides and slide notes used in teaching the S&T hour-long mini-course on Technology Commercialization.

Slide 1

Technology Commercialization

The other path to the user



Sam Francis
samuel.francis@associates.dhs.gov
March 25, 2008

revised 4/1/07

This mini-course is one of a series of 14, sponsored by the S&T Office of Strategy, Planning, and Integration (Mitch Crosswait, Director).

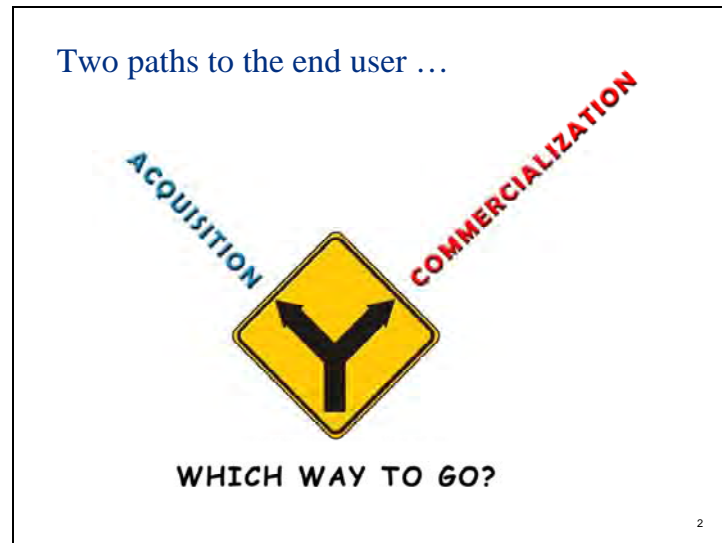
The briefing takes an hour, and will start and stop on time, so make sure any questions are for general clarification. The speaker will remain for 30 minutes after the end for discussion, if desired.

Hard copies of the slides will be handed out. The slides are also available from the RDT&E web site. To reach this web site, browse to the S&T Shared drive, find the folder "RDT&E Process Website," then double-click on the filename index.htm to browse the home page. To find the slides for all of the mini-courses in this series, click on Training in the bottom navigation bar and follow your nose.

Please sign the sign-in sheet. Also, fill out and leave behind the feedback form.

Today we'll be talking technology commercialization, which is one of two methods by which new products and systems can be put into the hands of users. (The other method is Acquisition.)

Slide 2

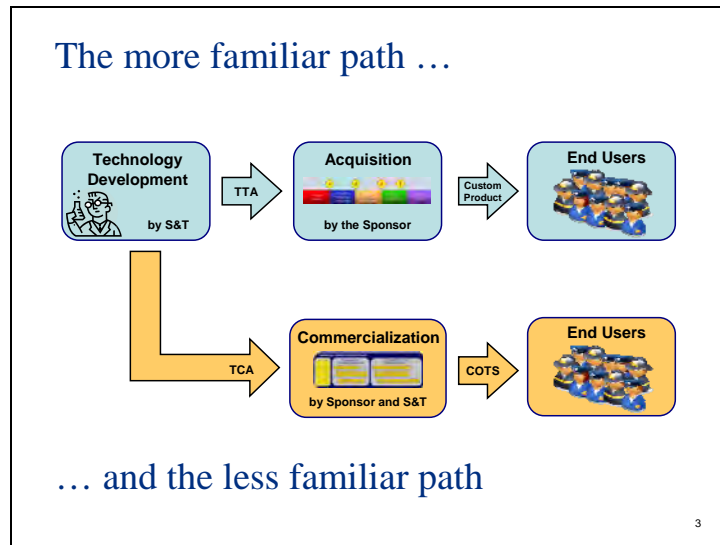


Acquisition and Commercialization are very distinct processes. Accordingly, the project manager reaches a fork in the road right at the beginning of the project. Which way to go?

Acquisition and Commercialization aren't mutually exclusive, of course, in the sense that elements of each can be blended, depending on the needs of the project. However, they are distinctly different models, and therefore it's important to understand both models before you try to combine elements of each.

In this mini-course, whenever we mention "Acquisition," we're talking "big 'A' Acquisition, not "little 'a' acquisition." In other words, we're talking about acquiring products which don't exist, rather than procuring or purchasing products which do exist. Those who are unfamiliar with the distinction between big 'A' Acquisition and little 'a' acquisition are referred to two other mini-courses in this series: "Acquisition" and "Procurement Requisitions."

We will also use the terms "product" and "system" interchangeably.



This slide depicts the two alternative paths to the end users.

The blue path, Acquisition, is the methodology which seems most familiar to S&T project managers, for two reasons:

It is the methodology which is used by most other major Federal Government agencies, such as the Department of Defense and NASA, because of their high-technology requirements and limited market size. Thus, it is the only methodology with which S&T project managers with Government experience are likely to be familiar.

It is the methodology which has been emphasized by the S&T Under Secretary and the Director of Transition, in their implementation of the Capstone IPT approach to engaging our internal DHS customers. The emphasis on “transition to Acquisition” governed by “Technology Transition Agreements” (TTAs) is, by now, familiar across S&T.

In contrast, the beige-colored path, Commercialization, is much less familiar to most S&T project managers, for two reasons:

This methodology has no close analog widely used in any other Government agency.

Consequently, there is no proven management framework for this methodology, as there is for Acquisition. True, our National Laboratories have a commercialization process which is executed by their Offices of Research and Technology Application (ORTAs) in compliance with technology transfer statutes, but this process lacks important features needed by S&T. Specifically, the ORTA’s process is not driven by capability gaps of government end users, nor does it make provision for the use of grants and standards.

The purpose of this mini-course is to familiarize you with the beige-colored path by describing a methodology which S&T has put forward for executing Commercialization projects. This methodology cannot be said to be proven, since it has not been applied widely. However, it has benefited from adoption of the best practices of the ORTAs, where they apply, and it’s a good starting place for the project manager who is wondering what to do next.

The two paths are extraordinarily different

- Acquisition
 - A **government contractor** executes design, development, and production, driven by **DHS requirements**, using **DHS funding**, under **contract** to DHS. The product is then **deployed to captive users**. Product unit price is determined by **cost-based** pricing. The contractor's customer is **DHS**, not the end-user community.
- Commercialization
 - A **private-sector enterprise** executes design, development, and production, driven by **market requirements**, using **private funding**, perhaps assisted by DHS technology **licenses, standards, and grants**. The product is then **sold as COTS directly to end users**. Product unit price is determined by **market-based** pricing. The vendor's customer is the **end-user community**, not DHS.

4

Although the two paths are extraordinarily different, they are often confused. Let's highlight the differences.

Who develops the product?

In Acquisition, the developer is a government contractor (often called a prime contractor or a system integrator to make clear their responsibility for the total product or system.)

In Commercialization, the developer is a private-sector enterprise.

Where do the requirements come from?

In Acquisition, the government specifies the requirements, based on information from its captive end users.

In Commercialization, the developer determines the requirements from the marketplace. The government may assert that it knows the marketplace requirements, but the developer is unlikely to invest scarce resources until they have at least validated those requirements.

Where does the funding come from?

In Acquisition, from the government.

In Commercialization, from the developer.

What are the formal, legal agreements between the Government and the developer?

In Acquisition, the relationship is governed by contracts.

In Commercialization, the relationship may require no legal agreements, or it may require licenses, CRADAs (Cooperative R&D Agreements), or Memoranda of Understanding.

(continued in the slide notes on the next page)

Highlighting the differences ...

Typically ...

	Acquisition	Commercialization
Product type	Custom	COTS
Users	Federal agency	State, local, private sector
Channel to users	Deployment	Sales
Designer & manufacturer	Gov't contractor	Private sector
Formal agreements	Contracts	Licenses, CRADAs, or none
Developer's customer	DHS	Marketplace
Design funder and owner	DHS	Private sector
Pricing	Cost-based	Market-based
Standards development	Possible	Likely
Grants	None	If needed
The bottom line ...		
DHS relationship to developer	Control	Influence

5

(notes continued from previous page)

What are the channels by which the products reach the end users?

In Acquisition, by deployment to captive end users.

In Commercialization, by sales channels such as catalog sales, e-commerce, or direct sales. The product is referred to as COTS (Commercial Off-the-Shelf), implying that it is readily available for sale.

How is the unit price determined?

In Acquisition, by a cost-type contract specifying a price determined by the cost of goods sold marked up by a fixed percentage.

In Commercialization, by price-based pricing, sometimes called market-based pricing, which means that the vendor charges what the market will bear. The market price is conventionally determined by a combination of a product's value, its manufacturing cost, and the competitive situation.

Who does the developer consider to be their customer?

In Acquisition, the developer's customer is the government agency with which they have contracted.

In Commercialization, the developer's customer is the marketplace.

The fundamental difference between the two approaches is the question of who has control. Acquisition allows total control by the government, because the government is paying the bills. In contrast, the best the government can hope for in Commercialization is to influence the private sector, by informing them of the market and perhaps by judicious use of standards and grants programs.

Slide 6

How to choose between Commercialization and Acquisition?

It's all about control (or lack of it)

<ul style="list-style-type: none">• How much control do you need?<ul style="list-style-type: none">– If the private sector can't be influenced to fund product development, or– If DHS can't wait for the private sector to develop the product, then <p>Acquisition is necessary to force product development</p>	<ul style="list-style-type: none">• How much control can you have?<ul style="list-style-type: none">– If DHS can't afford to fund product development, manufacturing, and deployment, or– If DHS has no authority over the users, then <p>Commercialization is necessary to get the product to the users</p>
---	---

Note that if the product is commercialized, DHS has no control over product price. The market-based commercial unit price will be higher than the cost-based Acquisition unit price. Thus, although DHS saves money up front if the product is commercialized, total cost of ownership may be higher ("pay me now or pay me later").

6

The choice between Acquisition and Commercialization may boil down to two questions of control:

How much control is needed? (Perhaps none, if the private sector can be influenced to commercialize the product in a timely manner.)

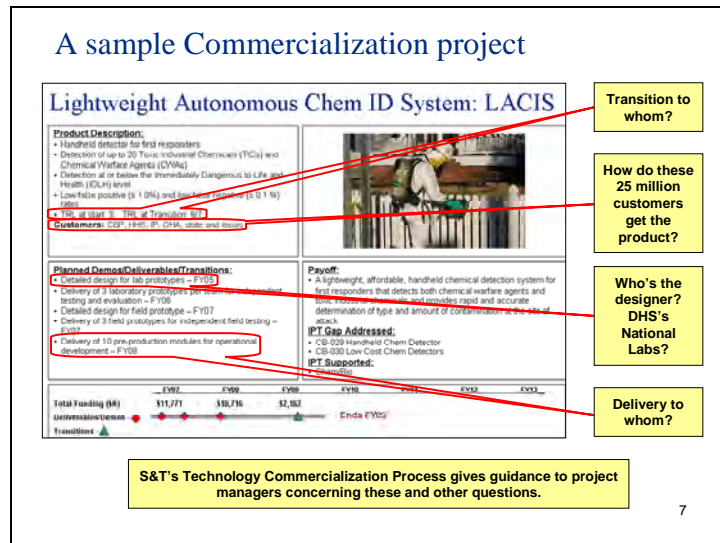
How much control is achievable? (Perhaps none, if the end users are not under the authority of a DHS agency, and therefore make their own buying decisions.)

Note that the ultimate unit price of the product will be price-based if commercialized and cost-based if acquired under contract. One can expect that market-based pricing will be higher than a cost-based pricing, because the vendor will recover the R&D costs in the market-based price of the product.

So if the ultimate users are in a DHS agency, the choice may very well be between (a) a higher up-front cost and a lower unit purchase price (in an Acquisition program), or (b) a lower up-front cost and a higher purchase price (in a Commercialization program).

In short, if the users are in a DHS agency, the choice may be "Pay me now or pay me later." If indeed both the Acquisition and Commercialization paths are feasible for the desired product, total cost of ownership should be considered as a significant factor in the decision.

Slide 7



Here is a sample Commercialization project quad chart, chosen at random from the many S&T projects whose goal is to put a commercial product into the hands of users over whom DHS has no authority.

The call-outs ask questions which might be prompted by any S&T quad chart for a Commercialization project. Specifically:

This is a Transition project, in that it is part of the portfolio of S&T's Transition Office. But to whom will it transition?

The customers include some DHS agencies with authority over end users (such as border-protection agents), but other agencies over which DHS has no authority (such as State and local agencies). How will all these end users have access to the product?

The quad chart asserts that the first major milestone is detailed design of a laboratory prototype. But what Laboratory will do the design? If the manufacturing will ultimately be done in the private sector, shouldn't the designing Laboratory be the R&D Division of the enterprise whose factory will ultimately manufacture the product? After all, their profits will depend on whether the product can be produced in *their* factory at a cost consistent with a competitive price point?


But perhaps the private sector doesn't have the technology? This is where licensing may enter the picture.

The quad chart describes the last milestone as "delivery of pre-production modules for operational development." Delivery to whom? Does "pre-production" imply that there is or is not yet a production-ready design? If there is a production-ready design, whose factory has it been designed for, and by whom?

Of course, the quad chart format is not designed to answer detailed questions such as these. Presumably the project's documentation, such as its Project Management Plan and its Transition Plan, have specified answers to these questions.

Two interlocking processes ...

- Every private-sector enterprise has their own product development process.
- S&T's goal, in partnership with our Sponsor, is to influence the private sector to develop a product satisfying a prescribed need (to fill an identified capability gap).
- To do that effectively, S&T needs its own process, called the Technology Commercialization Process.

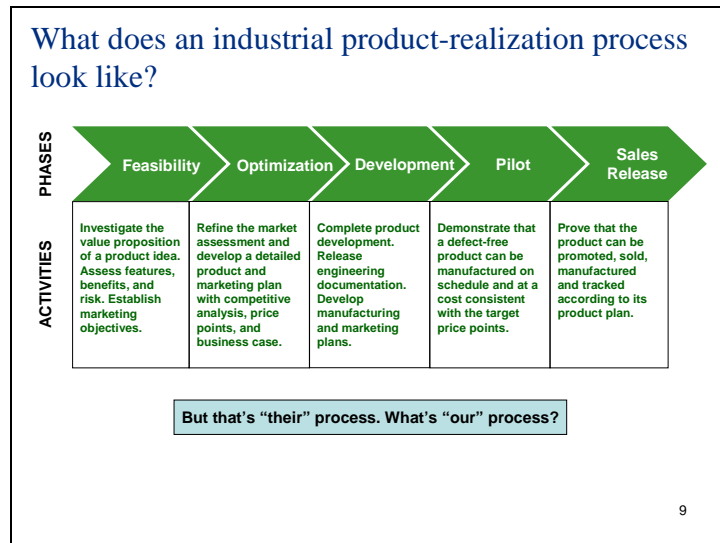


8

Let's be clear that we're talking about two interlocking processes here: Each private sector enterprise has its own product development process. Of course, S&T does not execute **this** process, and cannot specify it or control it, but needs to understand it in order to influence its outcome.

S&T has its own Technology Commercialization process. The private sector will not execute any part of **our** process, but will need to understand certain aspects of it in order for S&T to be able to influence the private sector. For example, if S&T asserts that there is a strong market for a new product satisfying certain requirements, the credibility of this assertion may depend on the private sector's visibility into how the market size and the requirements were determined.

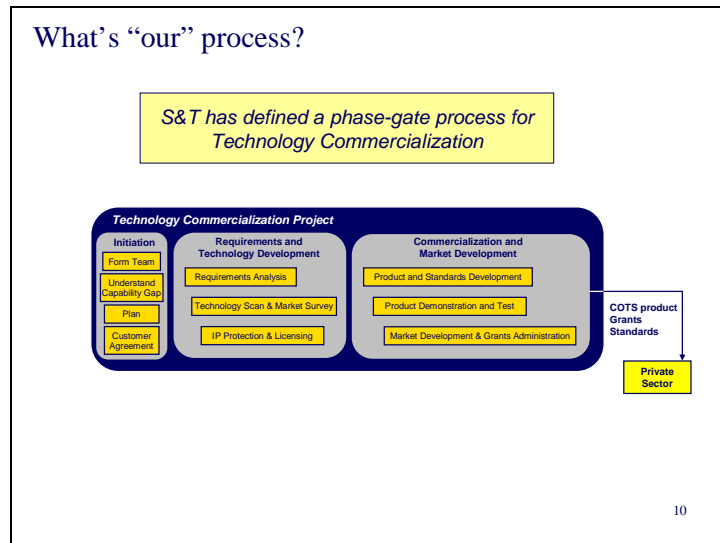
This mini-course will not go into detail concerning the private sector's product development process. We will touch on it, but spend most of our time talking about **our** process.



Most industrial product-development processes are structured as phase-gate frameworks, since the phase-gate paradigm is the best way to organize a series of activities with periodic event-driven management reviews.

The product-development process depicted here is a top-level description of a detailed product-development process used by S&T's Chief Commercialization Officer, Tom Cellucci, when he was a CEO and later a management consultant in the private sector. This phase-gate process uses a different vocabulary than any of S&T's processes, including terms such as "value proposition," "marketing," "competitive analysis," "price points," and "sales." One difficulty faced by S&T project managers of Commercialization projects is bridging the communications gap between the typical S&T technology-focused terms and the private sector's product-focused terms.

S&T's technology focus reveals itself in the use of terms (such as Technology Readiness Levels) which are generally unknown in the private sector. If you plan to partner with the commercial sector, you've got to learn their language, because (unlike government contractors) they won't learn yours.

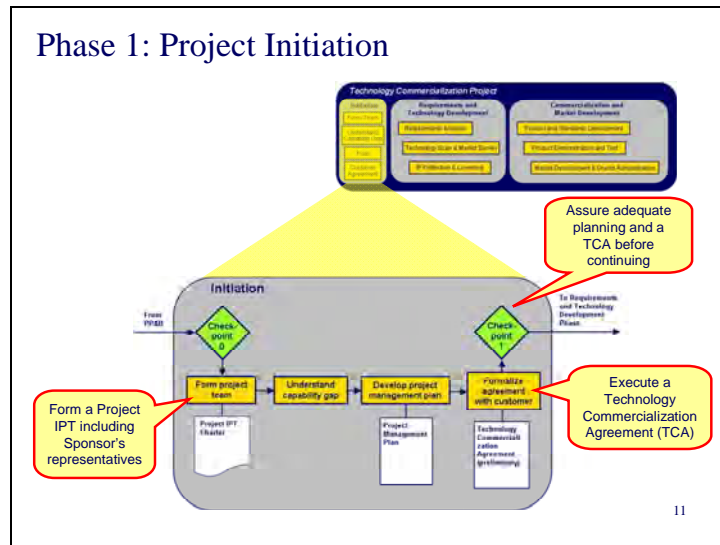


S&T has developed a phase-gate process to govern Technology Commercialization, as a way of providing guidance to project managers as they navigate unfamiliar waters. S&T has discovered no analogous process anywhere else, because no other government agency have a proven requirements-driven process to influence the private sector to develop a new product for a specific set of users.

This process contains elements of the commercialization process used by the Offices of Research and Technology Application (ORTAs) in DHS's National Laboratories to manage technology transfer to the private sector. However, the goal of the ORTAs is simply to transfer the technology to private-sector partners for whatever commercial purpose the private sector chooses, regardless of any connection with the Laboratory's mission. In contrast, the purpose of S&T's Technology Commercialization process is mission-driven, specifically to fill capability gaps relating to homeland security. This objective is much more difficult.

Accordingly, this process cannot be said to be proven, but is offered as a prototype process to be used and improved.

The process is documented on S&T's RDT&E web site, a disk-based web on the S&T Shared drive. Find the file "index.htm" in the folder "RDT&E Process Website" and double-click it to reach the home page. Then click on "Transition" in the main graphic, and then on "Technology Commercialization," and you'll see the phase-gate graphic reproduced in this slide.



Form project team

Name the project manager, who will lead the formation of a project integrated product team (IPT) whose members include all important skill sets and constituencies, including the Sponsor, who is S&T's customer internal to DHS who will represent the interests of the end users.

Understand capability gap

Establish knowledge of and rapport with the Sponsor and, through him, the end-user community. Define precisely the capability gap to be filled, and validate this requirement with the Sponsor and, through him, the end-user community.

Develop project management plan

Revisit and validate the initial decision to address the capability gap via Commercialization versus Acquisition.

Develop a specific commercialization strategy for this project, to be executed jointly by the S&T project team and the Sponsor's organization.

Document the project plan, defining the project team, project schedule, project budget, major milestones, and major reviews and checkpoints, all of which are consistent with the project's commercialization strategy.

Formalize agreement with the customer

Execute a Technology Commercialization Agreement (TCA) with the Sponsor. See the next slide for details.

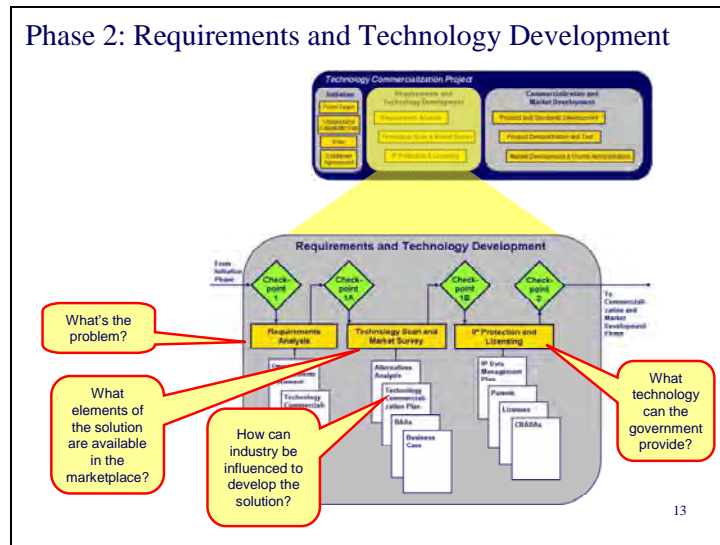
Technology Commercialization Agreement

- Analogous to a Technology Transition Agreement (TTA).
- Agreement between S&T and a sponsoring DHS agency representing the target user community.
- Defines roles and responsibilities for both S&T and the Sponsor during technology commercialization.
- Specifies:
 - Capability gap
 - Product to be developed
 - Commercialization strategy
 - Technologies to be transferred
 - Standards to be developed
 - Grant programs to be initiated
 - S&T funding
 - Sponsor funding



12

It is fundamental principle of S&T project management that all Transition projects must have written agreements with their internal DHS customers, documenting mutual expectations and signed by both parties. If a project can't reach a written agreement with its DHS customer (its Sponsor), then it probably doesn't have a real customer at all. For Advanced Research projects, which develop technology and transition it to an Acquisition program, the form of the agreement is the by-now familiar Technology Transition Agreement (TTA). For Technology Commercialization projects, the TTA template is inappropriate, and it is replaced by a template for a Technology Commercialization Agreement. The TCA specifies what responsibilities will be fulfilled by S&T (generally those that require technology expertise), and what responsibilities will be fulfilled by the Sponsor (generally those requiring familiarity with the end users and their operations). Funding by both parties is also specified. Specifically, if the Sponsor is expected to develop and administer a grants program, this fact is documented in the TCA.



Requirements Analysis

Develop a set of operational requirements to govern subsequent product development

Make an initial assessment of technological feasibility

Technology Scan and Market Survey

Conduct a technology scan, spanning all potential sources of technology (private sector, DHS laboratories, national laboratories, and other Government agencies such as the Department of Defense).

The purpose of the scan is to assess whether there exist technologies and/or products which address the documented operational requirements, and to identify the preferred technology or product.

Conduct a market survey, to ensure that no products exist which address the capability gap addressed in the ORD, and to identify which vendors are best positioned to reach the target marketplace with a new product based on the identified technology

Conduct a commercialization assessment, to assess the potential of the identified technology for successful commercialization and marketing

IP Protection and Licensing

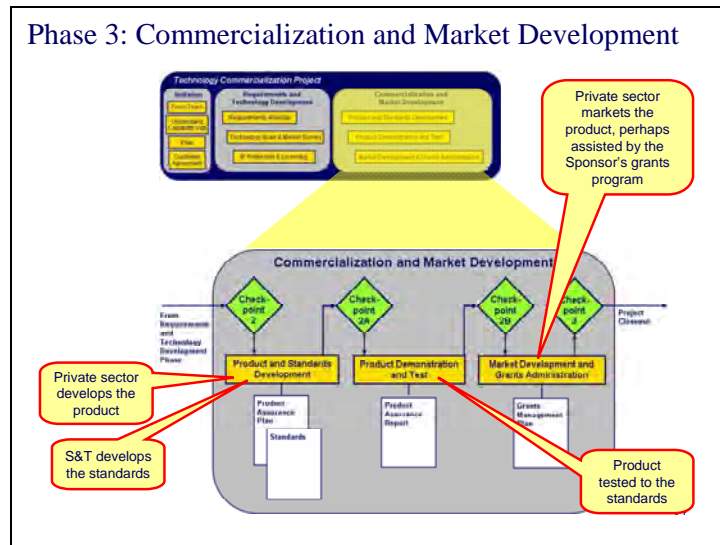
Develop the technology, if necessary, to the point of reduction to practice and therefore patentability

Ensure that the Government's intellectual property rights are secured

Identify the best partner in the private sector for commercialization of the technology

Enter into an appropriate licensing agreement with a chosen partner in the private sector

Manage the license during its effective term



Product and Standards Development

- Follow and, if appropriate, oversee the product development by the licensee
- Develop any necessary new standards to govern the product under development

Product Demonstration and Test

- Ensure that the commercial product, if successfully marketed, will meet the original requirements documented in the ORD.
- Influence the test and certification plan to ensure that a properly conducted test program will validate the product's performance against the original operational requirements document (ORD).



- Assure that tests and certifications are conducted properly, to the degree possible under the terms of the license and consistent with any standards which apply.

Market Development and Grants Administration

- Add the product, once certified, to the authorized equipment list on the website Grants.gov.
- Administer the grants program (as defined in the Technology Commercialization Plan and subsequently amended) to help develop the market for the product

Summary

- Technology Commercialization is the "other" path to the users (distinct from Acquisition).
- To cause a new COTS product to be developed and purchased by end users directly from a vendor, Commercialization (not Acquisition) is executed.
- Like S&T's Advanced Research projects, governed by TTAs, Technology Commercialization projects require agreements (TCAs) with DHS Sponsors (representing the users).
- Commercialization requires S&T and the Sponsor to exercise "influence," not "control," over the private sector.
- Grants, governed by Standards, may be required to enhance the market.
- An S&T phase-gate management framework provides guidance for project managers.



15

This slide summarizes the main points of this mini-course.

Appendix D: Requirements Mini-Course

The following pages include the slides and slide notes used in teaching the S&T two-hour mini-course on Requirements.

Slide 1

Requirements

Types of requirements and their development



Sam Francis
samuel.francis@associates.dhs.gov
March 26, 2008

revised 4/1/07

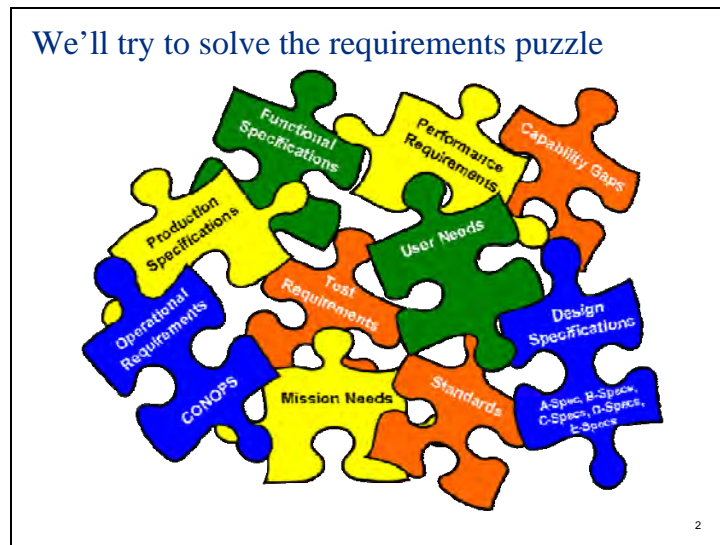
This mini-course is one of a series of more than a dozen, sponsored by the S&T Office of Strategy, Planning, and Integration.

The briefing takes an hour, and will start and stop on time, so make sure any questions are for general clarification. The speaker will remain for 30 minutes after the end for discussion, if desired.

Hard copies of the slides will be handed out. The slides are also available from the RDT&E web site. It's on the S&T Shared drive, in the folder "RDT&E Process Website." Double-click the filename index.htm and you'll be browsing the home page. Click on Training in the links at the bottom of any page and you'll be able to find the slides.

Please sign the sign-in sheet.

Today we'll be talking about Requirements, which is a critical topic for S&T if we hope to satisfy our customers.



The vocabulary relating to requirements is broad and not standardized. Different communities use different definitions.

The Project Management Institute, in its bible titled *Project Management Book of Knowledge*, includes the following definitions:

Requirement: A condition or capability that must be met or possessed by a system, product, service, result, or component to satisfy a contract, standard, specification, or other formally imposed documents.

Requirements include the quantified and documented needs, wants, and expectations of the sponsor, customer, and other stakeholders.

Specification: A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system, component, product, result, or service and, often, the procedures for determining whether these provisions have been satisfied. Examples are: requirement specification, design specification, product specification, and test specification.

Other communities use the term “requirement” to refer to a definition of the problem, and “specification” to refer to a definition of the solution. For example, Kossiakoff and Sweet (Systems Engineering Principles and Practice) define:

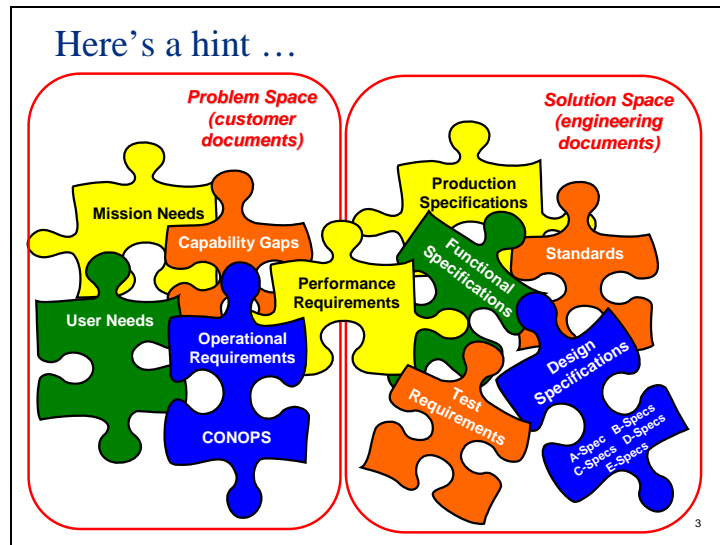
Requirement: (1) A characteristic that identifies the accomplishment levels needed to achieve specific objectives under a given set of conditions; (2) A binding statement in a document or in a contract.

Specification: A document intended primarily for use in procurement, which clearly and accurately describes the essential technical requirements for items, materials, and services including the procedures by which it will be determined that the requirements have been met.

Nor does DHS have a standard vocabulary, with the exception of “mission need” and “operational requirement” (two terms inherited from DoD by way of the Coast Guard).

This mini-course will use the terms carefully, adopting a set of definitions which should be clear by the end, but don’t assume that these terms mean the same to everyone. You will have to negotiate a common vocabulary with each of your customers (or suppliers) to be sure of your terms.

By the way, the acronym CONOPS stands for Concept of Operations.



In systems engineering, an “operational requirement” is generally a description of *what* a system must do. It is generally written in the language of the operator (the end user), not the engineer. In contrast, a “performance requirement” specifies something about the system itself, and how well it performs its functions. It is generally written in the language of the engineer. Performance requirements are a bridge from the operational world to the engineering world. Examples of performance requirements include availability, testability, maintainability, and ease-of-use. Other system-specific performance requirements include detection probability, false-alarm probability, and similar technical performance measures (TPMs).

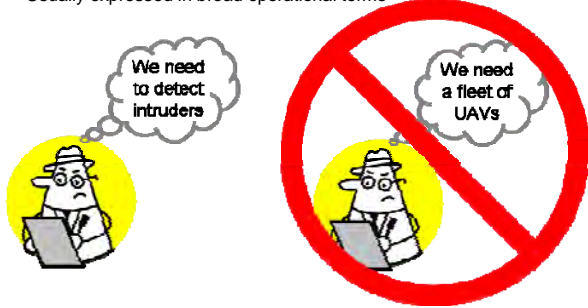
A “good” list of requirements generally avoids saying *how* the system should implement the requirements, leaving such decisions to the system designer.

Once the system designer has decided how the system implements the requirements, this solution is documented in the design specifications. In short, “requirements” can be thought of as statement of the problem, and “specifications” are a statement of the solution.

Step 1: Define the problem (not the solution)

The Sponsor (an operational DHS Component) identifies a capability gap

- Can be identified in partnership with (or independent of) S&T and the Capstone IPT
- Must be expressed as a needed capability, not a needed product or system
- Usually expressed in broad operational terms



4

We'll start by describing how requirements of various types relate to a standard product or system development. Then we'll be in a position to understand how they relate to an S&T technology development or a commercialization project.

In DHS, a product or system development is conventionally accomplished by an Acquisition program, led by a Sponsor.

The term "Sponsor" is formally defined by DHS's Investment Review Process, documented in MD1400. The Sponsor is a designated executive in the DHS Component which contains or represents the end users (the "boots on the ground") who need the capability. It is the Sponsor's responsibility to ensure that the end users have the capabilities they need.

At this early stage, there is an almost irresistible temptation to specify the solution rather than the problem. However, it's important to resist that temptation so as not to preclude possible solutions which may be optimal but haven't been considered. Force the problem statement to be a need for a "capability to be able to do something" rather than a "need to have something." This is called capabilities-based planning.

To identify the capability need seems basic or self-evident. However, a design project is often initiated as a result of a personal interest or a political whim, without first having adequately defined the requirement. Defining the problem is the most difficult part of the system engineering process. This objective is most likely to succeed if the ultimate users are involved in the process from the beginning.

Step 2: Document the need

- The Sponsor documents the need in a *Mission Needs Statement*
 - MNS template is prescribed by MD1400
- MNS approval is the first step in an Acquisition program to fill the capability gap

The diagram illustrates two stick figures representing the 'Sponsor' and the 'Acquisition Program Manager'. They are standing on either side of a document titled 'MNS Mission-Based Statement of Needed Capability'. The document features a blue arrow pointing downwards. The 'Sponsor' is on the left, and the 'Acquisition Program Manager' is on the right. A small number '5' is located in the bottom right corner of the slide frame.

Note that, so far, all these activities have taken place in the Sponsor's organization, not in the S&T Directorate. The only role played by S&T so far is, perhaps, to act as a catalyst in identifying the capability gap (through S&T's sponsorship of the Capstone IPTs).

Said another way, the S&T Directorate plays little role in identifying the problem. S&T's role begins (if asked) when it comes time to identify the solution.

As an aside, the *Mission Need Statement* was initially used in the Department of Defense, but was subsequently changed in DoD to the *Initial Capability Document* to emphasize capability-based planning (i.e., identify the problem, not the solution). DHS also emphasizes capability-based planning, but has not changed the title of the document.

To originate a program, the Sponsor documents the mission need in an MNS, stating the operational needs (i.e., capability gaps) written in broad operational terms and not in terms specific to any system or system concept. For example, a checked-baggage mission need could be that a new type of explosive must be detected during airport baggage handling, or that an increase in air travel requires that baggage throughput be doubled within 5 years.

It's not uncommon for the creation of the MNS to be delegated to an Acquisition program manager, but this practice violates the principle that the solution developer should not be the same as the problem specifier. It's very tempting for solution developers to solve problems that they prefer, rather than solving problems of importance to operators.

What a MNS is (and is not)


A MNS is a high-level document describing:

- a capability gap which needs to be filled
- the link to the Sponsor's mission
- the Authority which specifies the mission
- the link to DHS and Sponsor's strategic plans
- why the capability is not more suitably provided by another Federal agency or the private sector
- why the gap cannot be filled by a non-materiel solution (i.e., a solution which doesn't involve new product or system development)

A MNS is not a proposal for:

- a specific or preferred solution
- the establishment of an Office or Directorate

MNS
Mission-Based
Statement of
Needed
Capability



The purpose of the
MNS is to make the
case for an
Acquisition program.

MNS example: CBP needs improved control over shipping containers by detecting anomalous contents, detecting unauthorized intrusion, and tracking movements.

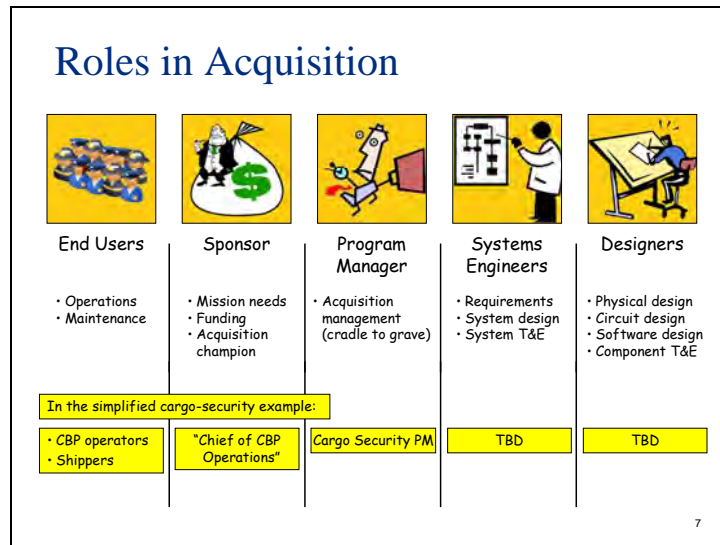
6

The purpose of the Mission Need Statement (MNS) is to synopsize at a high level (i.e., two to five pages) specific functional capabilities required to accomplish the DHS mission and objectives. MNS submissions that go beyond the scope of this guidance and include detailed costs or solution-based requirements normally contained in other planning documents will be rejected. The MNS is a qualitative communication vehicle both within a program and between the program and DHS HQ to provide a strategic framework for Acquisition planning and development.

Approval of the MNS provides formal DHS executive-level acknowledgment of a justified and supported need for allocation of scarce resources to resolve a mission deficiency with a material solution. In the broader view of the investment lifecycle, it represents the initiation of formal acquisition program management and the beginning of the investment process.

The MNS should describe specific functional and architectural capabilities required to perform the DHS mission, concisely but in sufficient detail for reviewers to understand the need for the investment within the context of the DHS portfolio. It should provide critical insight into mission capabilities and should provide the basis on which the reviewers can render an investment decision with an initial authorization to proceed within an acquisition project. Later documents, such as the Operational Requirements Document, will take the concepts outlined in the MNS and begin decomposing the gap requirements in detail.

The MNS requires approval by the Milestone Decision Authority, depending upon the level of the investment (see the MD 1400, Investment Review Process, for a description of the levels), before the investment can proceed.



The goal of Acquisition is to provide a material system or product to the end users to enhance Homeland Security.

Any product development by S&T is useless unless, sooner or later, it finds its way to the end users through the Acquisition process (or the Commercialization process). It's important that S&T managers understand where they fit in and what responsibilities are fulfilled by others. Their impact on the end users may be direct or indirect, depending on where their products fit in the value chain.

For example, if the role of a particular S&T project is to transition a product to Acquisition, but the Acquisition program does not exist or is not viable, S&T will have no impact on Homeland Security.

The roles and responsibilities may be articulated as follows:

The End Users have the responsibility to operate and maintain the systems in the field. They have no responsibility to identify capability gaps or requirements.

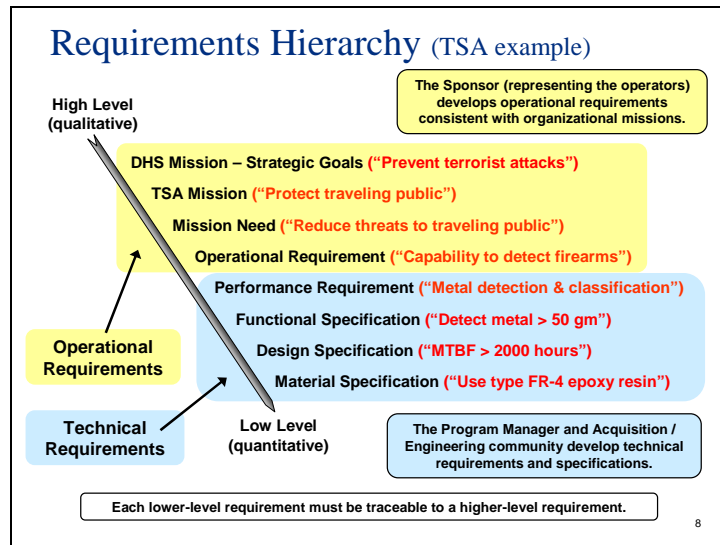
The Sponsor is an executive in DHS agency which contains or represents the end users. The Sponsor's responsibility is to identify mission needs (or, equivalently, capability gaps), perhaps inside the Capstone IPT process; to be a champion for Acquisition programs to address the mission needs; and to provide funding and other resources to facilitate the success of such Acquisition programs.

The Acquisition Program Manager is responsible for managing the Acquisition from beginning to end, from needs assessment at the front end to system deployment, operation, maintenance, and ultimately disposal at the back end.

The Systems Engineers guide the engineering of the system, from requirements development to test and evaluation, including the development of the system architecture.

The Design Engineers design and develop the components of the system.

Slide 8



The requirements hierarchy is naturally divided into two domains, operational and technical. The Sponsor, representing the operators, is responsible for all operational requirements. The technical system developer is responsible for all technical requirements.

The Mission Needs Statement is the entry point to Acquisition.

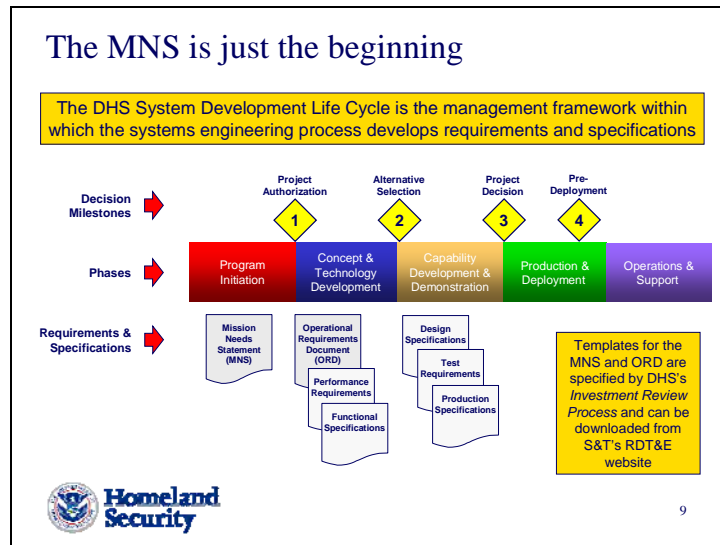
During an Acquisition program, requirements and specifications of increasing detail will ultimately specify the materiel solution. All lower-level requirements must be traceable to higher-level requirements. If not, why are they required?

The development of these requirements and specifications is governed by the systems engineering process.

Attention to detail, and disciplined adherence to process, is required for a successful Acquisition program. Counter-examples are legion.

Incidentally, the acronym MTBF signifies Mean Time Between Failures, a principal measure of reliability.

Slide 9

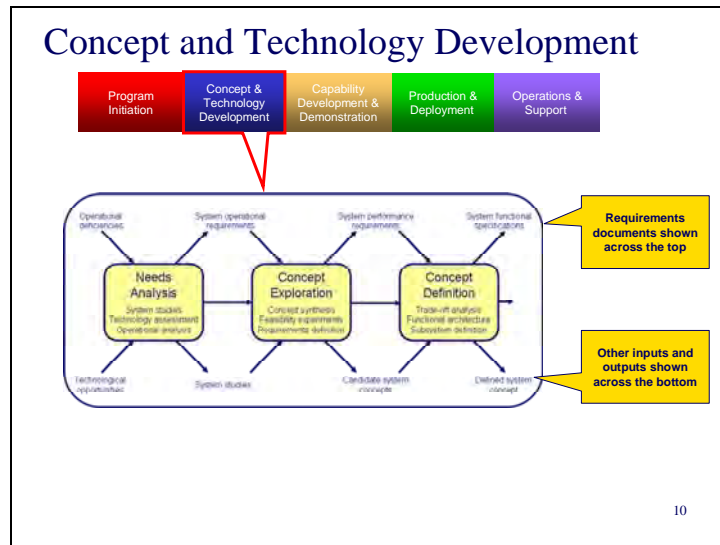


The System Development Life Cycle (SDLC) is DHS's management framework to provide structure and discipline for Acquisition programs. Its 5 phases are a relatively standard structure for a system life cycle.

DHS mandates the use of MNSs and ORDs, and provides templates for these documents. However, the downstream requirements and specification documents are not prescribed.

The decision milestones, known as Key Decision Points and numbered from 1 to 4, are the gates in the phase-gate process at which the program is reviewed by its Acquisition Authority (whose level depends on the size of the Acquisition, as prescribed in MD1400). We will use the SDLC to provide the context in which requirements and specifications evolve as a new system goes through design and development.

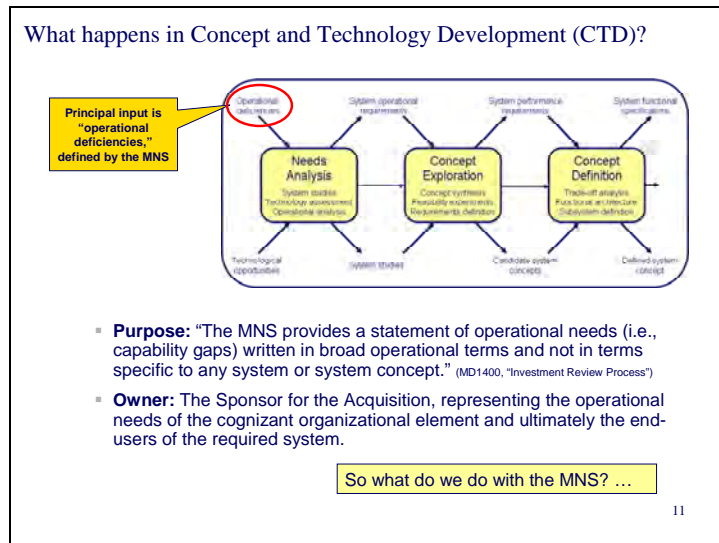
More details can be found on S&T's RDT&E website. Browse to the "RDT&E Process Website" folder on S&T's Shared drive, then open index.htm in your browser.



We will expand the SDLC's second phase (Concept and Technology Development) and its third phase (Capability Development and Demonstration) into three sub-phases each, to describe the activities within each phase and the resulting requirements and specifications.

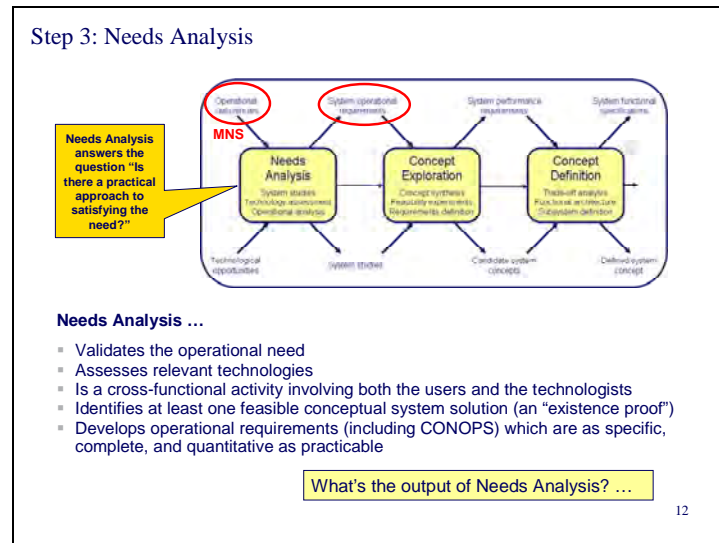
This expansion derives from relatively standard textbook expositions of systems engineering. Reference may be had to *Systems Engineering: Principles and Practice* by Kossiakoff and Sweet, or to any standard systems engineering text.

Slide 11



The entry criteria for Concept and Technology Development are:
 An approved Mission Needs Statement, stating operational deficiencies
 An approved preliminary business plan, typically in the form of an Exhibit 300
 A successful completion of Key Decision Point 1
 The next step (on the next slide) is Needs Analysis.

Slide 12



Needs Analysis consists of the following activities:

Conduct Operations Analysis

Analyze projected needs (Identify deficiencies in current systems)

Define operational approach (CONOPS) and operational objectives

Conduct Functional Analysis

Translate into functions, analyzing functional capabilities necessary for the system to perform the desired operational actions.

Allocate functions to subsystems and identify all interactions and interfaces

Establish Feasibility

Envision subsystem technology

Define feasible concept

Validate Needs

Design an operational effectiveness model, including "measures of effectiveness," to assess the degree to which a given system concept may be expected to meet a postulated need.

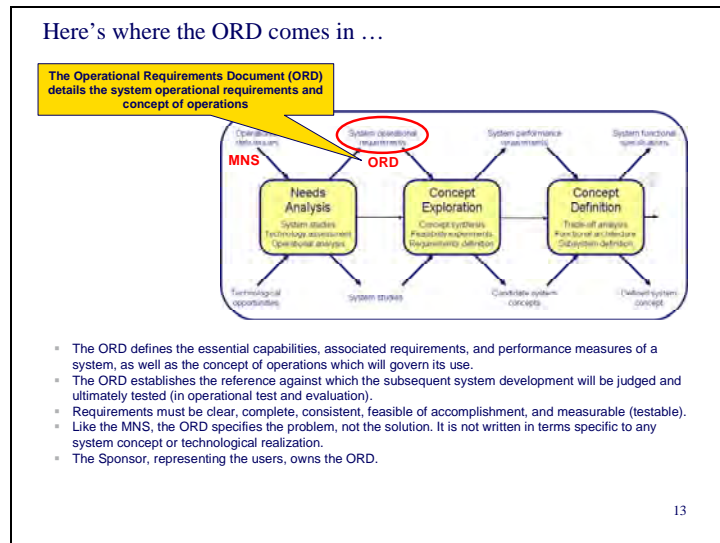
Validate feasibility and needs

Develop System Operational Requirements

Develop operational scenarios spanning the expected range of operational situations

Develop operational requirements statements (described in terms of operational outcomes rather than system performance). They must not be stated in terms of implementation, nor biased toward a particular conceptual approach.

All requirements should be expressed in measurable (testable) terms. The rationale for all requirements must be stated or referenced, so that the systems engineers can understand the requirements in terms of user needs.



After needs analysis and the selection of a feasible technical approach (though not, at this point, necessarily the optimum one), one is ready to project the relevant information to derive anticipated operational requirements. These requirements include the following considerations:

Operational distribution or deployment – the number of customer sites where the system will be used, the geographical distribution and deployment schedule, and the type and number of system components at each location. This responds to the question: where is the system to be used?

Mission profile or scenario – identification of the prime mission for the system, and its alternative or secondary missions. What is the system to accomplish and what functions must be performed in responding to the need? This may be defined through a series of operational profiles, illustrating the “dynamic” aspects required in accomplishing a mission. An aircraft flight path between two cities, an automobile or a shipping route, and the number of products to be produced in a factory are examples.

Performance and related parameters – definition of the basic operating characteristics or functions of the system. This refers to parameters, such as range, accuracy, rate, capacity, throughput, power output, size, and weight. What are the critical system performance parameters needed to accomplish the mission at the various sites? How do these parameters relate to the mission profile(s)?

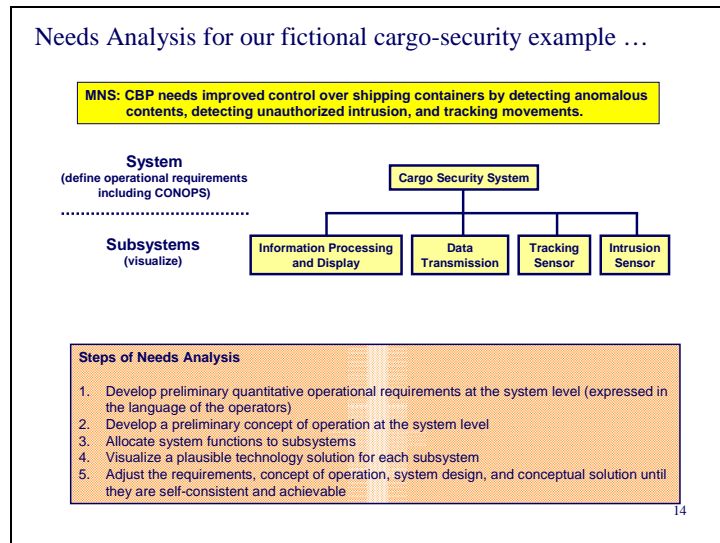
Utilization requirements – anticipated usage of the system (and its components), in accomplishing the mission. This refers to hours of equipment operation per day, the duty cycle, on-off cycles per months, percentage of total capacity used, facility loading, and so forth. To what extent will the various system components be used? This leads to a determination of some of the stresses imposed on the system by the operator.

Effectiveness requirements – system requirements (specified quantitatively as applicable) to include cost/system effectiveness, operational availability, dependability, reliability mean time between failure (MTBF), failure rate, readiness rate, maintenance downtime, mean time between maintenance (MTBM), facility use (percentage), personnel quantities and skill levels, cost, and so on. Given that the system will perform, how effective or efficient must it be?

Operational life cycle (horizon) – the anticipated time duration that the system will be operational. How long will the system be in use by the consumer? What is the total inventory profile for units of the system and its components, and where is this inventory to be located? One needs to define the system life cycle. Although this may change (i.e., the life cycle of a system may be extended or reduced), a “baseline” needs to be established at the beginning.

Environment – definition of the environment in which the system is expected to operate in an effective manner. Examples are temperature, shock and vibration, noise, humidity, arctic or tropics, mountainous or flat terrain, airborne, ground, and shipboard. Following a set of mission profiles may result in specifying a range of values. To what will the system be subjected during its operational use and for how long? In addition to system operations, environmental considerations should address transportation, handling, and storage modes. It is possible that the system (or some of its components) will be subjected to a more rigorous environment when being transported than during operation.

The establishment of operational requirements forms the basis for system design. Be careful not to presuppose a specific technical solution. For example, if an operational requirement is that a vehicle be capable of traveling 600 miles on a tank of gas, such a requirement might be met by a larger gas tank, a lighter vehicle, or a more efficient engine. Thus, the ORD would specify the 600 miles/tank requirement, but be silent on tank size, vehicle weight, and engine efficiency, each of which presupposes a specific technical approach to solving the problem.



Start by writing down draft operational requirements at the system level. For example (to cite some made-up requirements for pedagogical purposes):

If a shipping container is tampered with, CBP shall know within 24 hours if at sea or on arrival at the port of entry.

CBP shall be able to determine the geographical position of each shipping container on demand, to an accuracy of one nautical mile.

CBP's ability to monitor each container shall commence when the container leaves its port of departure.

If a shipping container at sea is bound for a U.S. port which is not a port of entry, CBP shall have at least one day's notice of this fact.

CBP shall know within one day when its ability to monitor a particular shipping container is compromised.

Also write down a CONOPS.

CBP shall maintain an operations center where shipping container status is monitored. (Or, alternatively, each port of entry shall maintain such an operations center.)

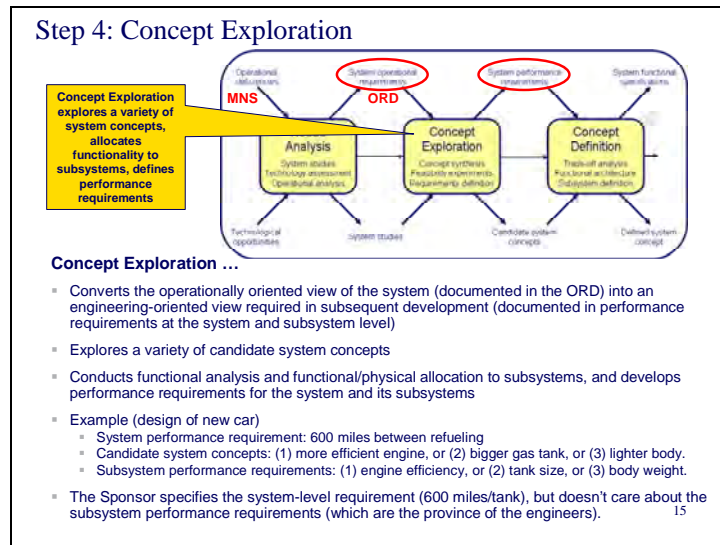
When tampering is detected on a container at sea, CBP will ...

When a shipping container is bound for a U.S. port which is not a port of entry, CBP will ...

If CBP loses the ability to monitor a particular shipping container, CBP will ...

Visualize a potential system decomposition into subsystems and visualize how the functionality of the system is distributed among the subsystems. Is there a plausible technology solution for each subsystem?

For example, is the signal processing done in the sensor (of which there may be 100,000) or the Info Processing and Display subsystem (of which there may be one)? If in the sensor, the sensor may become unaffordable for the shippers to purchase. If centralized in the Info Processing and Display subsystem, great demands are placed on the Data Transmission subsystem and the Info Processing subsystem.



Concept Exploration consists of the following activities:

Operational Requirements Analysis

Define and analyze at least 3 alternative concepts, starting with an existing (predecessor) system as a baseline, if possible, and varying one or more subsystems or considering modified architectures

Develop a CONOPS, expressing the customer's expectation for system use. The CONOPS is a constraint on the system concept and therefore is, effectively, an addition to the operational requirements.

Performance Requirements Formulation

Derive subsystem functions

Formulate performance parameters

Implementation Concept Exploration

Explore alternative technologies and architectures

Define performance characteristics of each candidate system concept

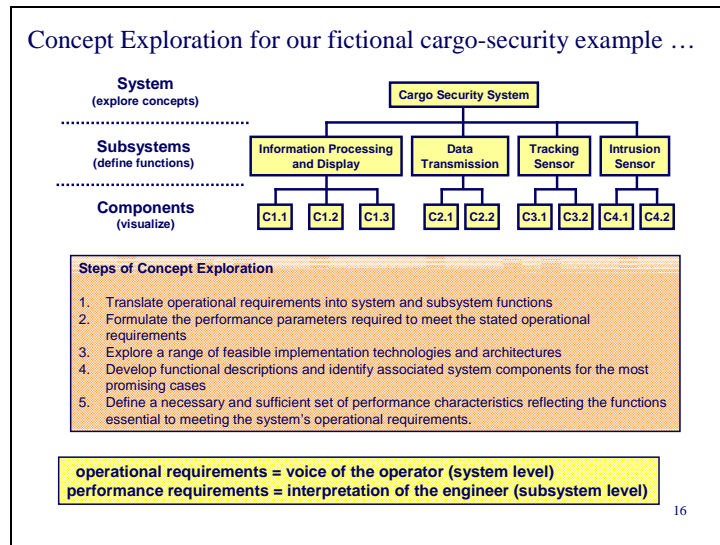
Performance Requirements Validation

Integrate performance characteristics, selecting those characteristics of the different system concepts that are necessary and sufficient to define a system possessing the essential operational characteristics

Validate performance requirements against operational requirements, and create the performance-requirements document. These requirements define:

What the system must do, and how well, but not how the system should do it.

Characteristics in engineering terms that can be verified by analytical means or experimental tests.



Now we define the functionality of the subsystems and visualize the components necessary to implement these subsystems. We do this for a range of feasible implementation technologies and architectures.

For example, two competing concepts might be to implement signal processing in the Intrusion Sensor subsystem or to centralize signal processing in Info Processing and Display subsystem. We would visualize the components necessary to implement each of these approaches, and compare the system performance, cost, schedule, and risk for the competing approaches.

We then define a necessary and sufficient set of performance characteristics reflecting the functions necessary to meet the operational requirements.

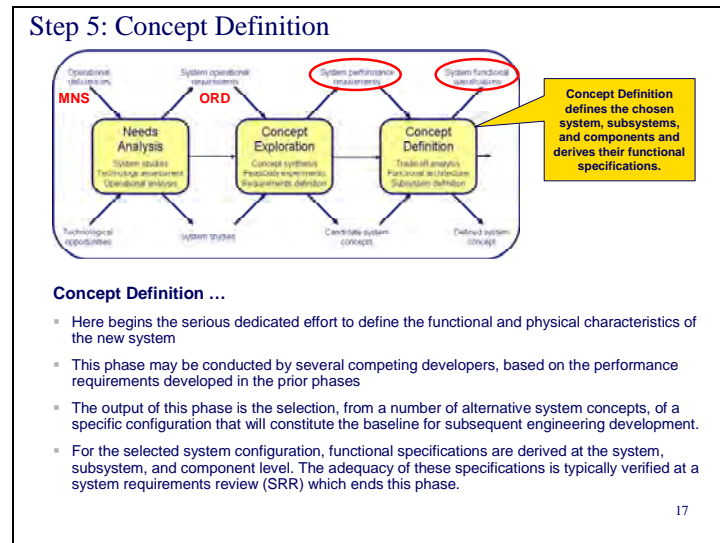
These performance characteristics, derived for the system and subsystem levels, are called “performance requirements” and are the engineer’s interpretation of the operational requirements.

Examples of performance requirements for this system might include “probability of detection of an intrusion,” “probability of false alarm,” “system availability,” “system geographical coverage.”

These are performance requirements at the system level. Requirements at the subsystem level might include the bandwidth of the Data Transmission system, shock and vibration resistance of the Intrusion Sensor subsystem, or the accuracy of the Tracking Sensor subsystem.

To tell whether a particular requirement is an operational requirement or a performance requirement, ask yourself whether the operator could (a) articulate the requirement, and (b) measure compliance with the requirement during an operational test at the system level.

Slide 17



Concept Definition consists of the following activities:

Performance Requirements Analysis

Analyze performance requirements

Each phase of development must begin with a detailed analysis of all of the requirements on which the ensuing program is to be predicated. Even though the previous phase may have been thoroughly carried out, the derivation of a set of performance requirements for a complex system is necessarily an imprecise and often subjective process. It is therefore essential that both the basis for the requirements and their underlying assumptions be clearly understood.

Refine performance requirements as necessary

Functional Analysis and Formulation

Define component functions, by allocating subsystem functions to the component level

Formulate functional requirements for each assigned function

Concept Selection

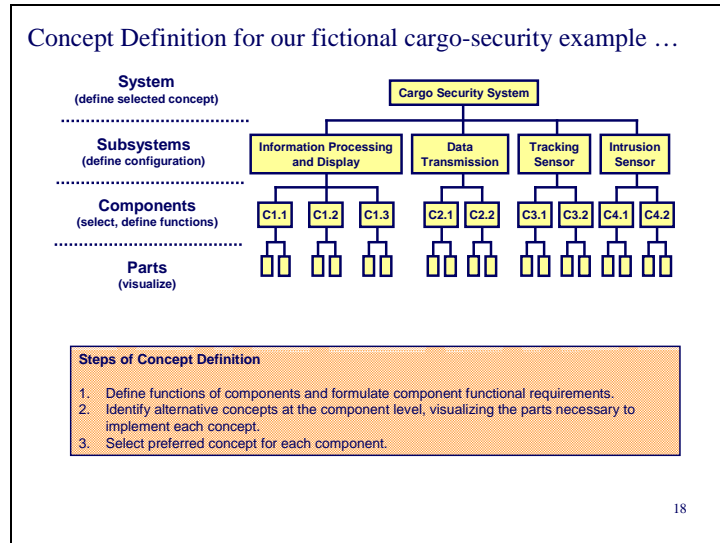
Synthesize alternative technological approaches and component configurations designed to meet the system performance requirements

Select preferred concept after trade-off studies

Concept Validation

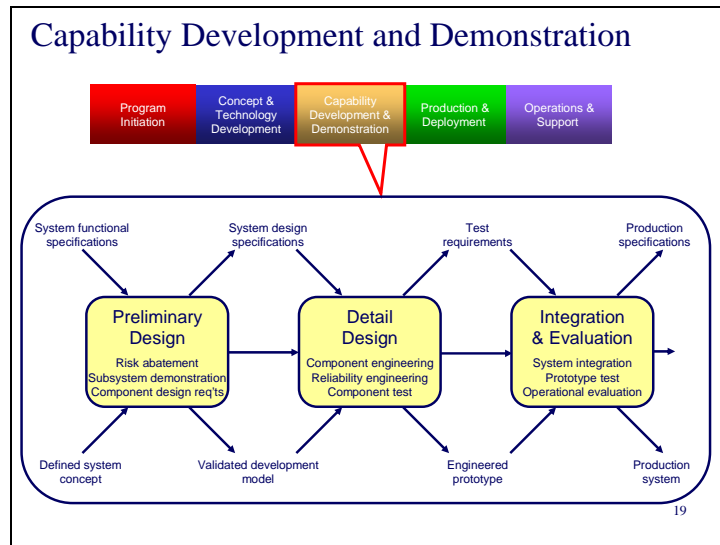
Conduct system simulation using system effectiveness models. Conduct critical experiments where necessary to demonstrate feasibility where modeling is inadequate.

Validate selected concept (Does it meet requirements? Is it the superior alternative?)

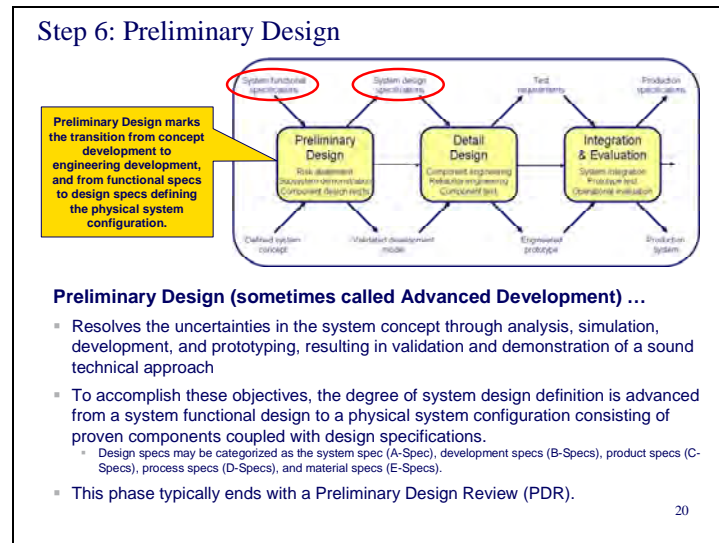


After the optimum system concept has been selected in the Analysis of Alternatives (AoA), complete the system design by flowing down functional requirements from the subsystem level to the component level, and visualizing the implementation of these components using standard parts.

Select a preferred concept for each component (a sort of mini-AoA).



We expand the System Development Life Cycle's third phase (Capability Development and Demonstration) into three sub-phases, to describe the activities within this phase and the resulting requirements and specifications, listed across the top. This expansion derives from relatively standard textbook expositions of systems engineering. Reference may be had to *Systems Engineering: Principles and Practice* by Kossiakoff and Sweet, or to any standard systems engineering text.



Preliminary Design consists of the following activities:

Requirements Analysis

Analyze system functional specs, validating their traceability to operational and performance requirements and the validity of their translation into subsystem and component functional requirements

Identify immature components requiring development

Functional Analysis and Design

Identify functional performance issues

Resolve issues (by analyses and simulations), design software

Prototype Development

Identify unproven technology

Design and build critical components (hardware and software)

Development Testing

Build test set-up, conduct tests of critical components

Evaluate test results and feed back design deficiencies or excessively stringent requirements as necessary for correction.

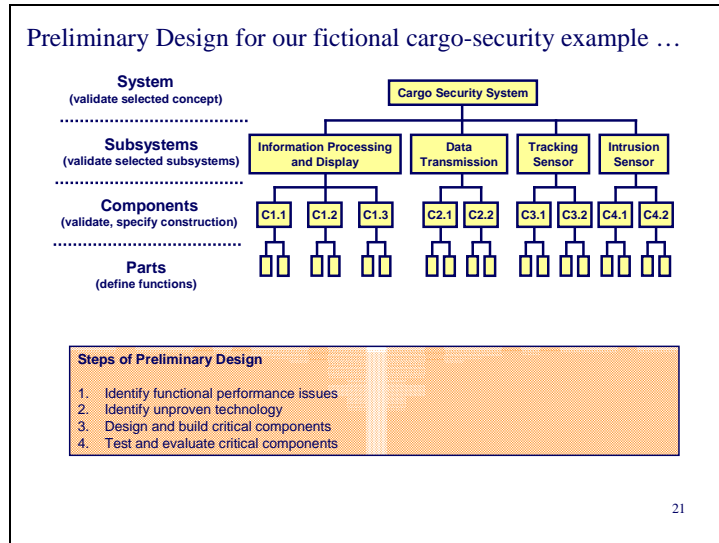
Perform preliminary product design

Create mockups, models, and breadboards as necessary.

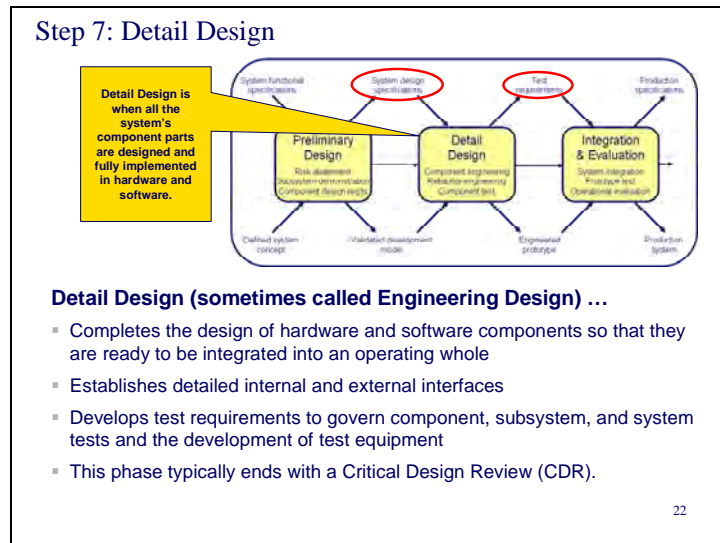
Create design and interface specifications (B specs)

Conduct a PDR

Slide 21



Note that, in Preliminary Design, functional requirements are flowed down to the Parts level, and critical components using unproven technology are designed, built, and tested.



Detail Design consists of the following activities:

Requirements Analysis

Analyze system design requirements for relevance, completeness, and consistency

Identify and analyze external interface requirements

Since the whole system has not been physically assembled in previous phases, it is likely that the design of its external interfaces has not been rigorous.

Functional Analysis and Design

Analyze component interactions (which may not have been done rigorously in preliminary design)

Maximize system modularity, by definitizing the interactions of components with one another and with the system environment to maximize their mutual independence

Execute detailed design of components

Produce a complete description (the product baseline) of the end items constituting the total system, including specifications (C, D, E), interface control drawings, detailed engineering drawings, configuration control plan, detailed test plans and procedures, QA plans, ILS plans, and other documentation

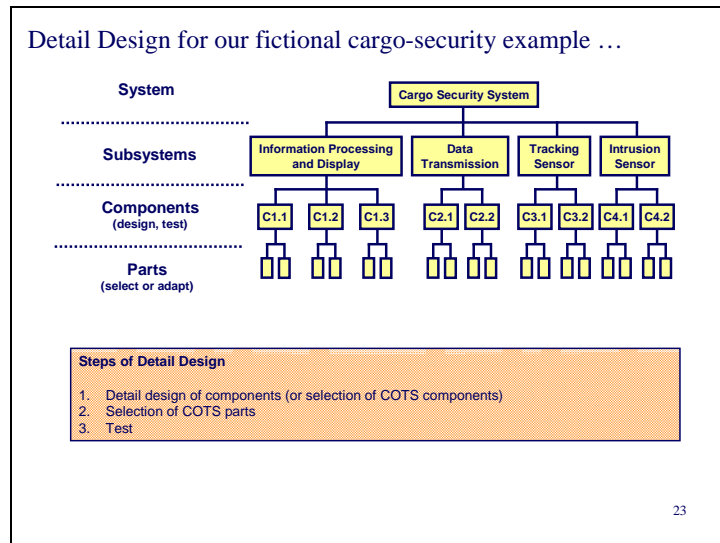
Produce prototype hardware and software

Conduct a CDR

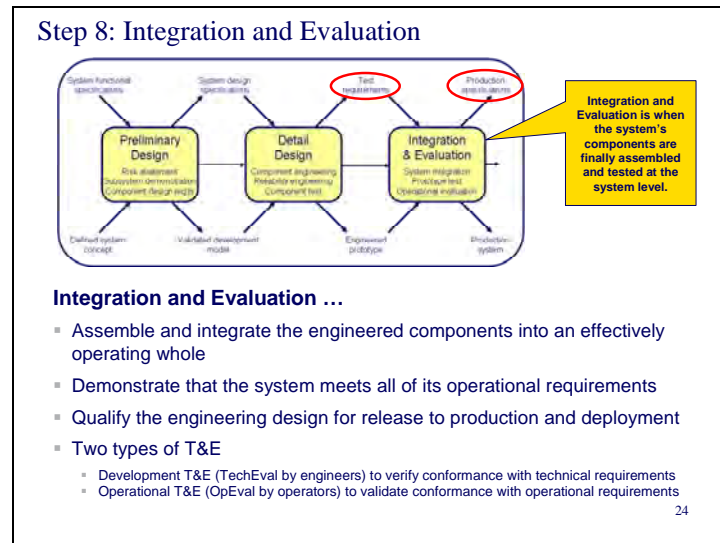
Design Validation

Design and build test equipment

Test components to validate design, correcting design discrepancies if necessary



In detail design we complete the design down to the Parts level, by selecting or adapting existing COTS parts which can be used with acceptable risk to implement the functionality at the Component level.



Integration and Evaluation phase consists of the following activities:

Test Planning and Preparation

Review system requirements to ensure that no changes have occurred during the engineering design phase which may impact the system T&E process.

Define test requirements for integration testing and performance testing

Design/build system/subsystem test equipment (including capability to stimulate the element under test and measure system response)

System Integration

Integrate tested components into subsystems

Test subsystems

Integrate tested subsystems into an operational system

Developmental System Testing

Perform system-level tests

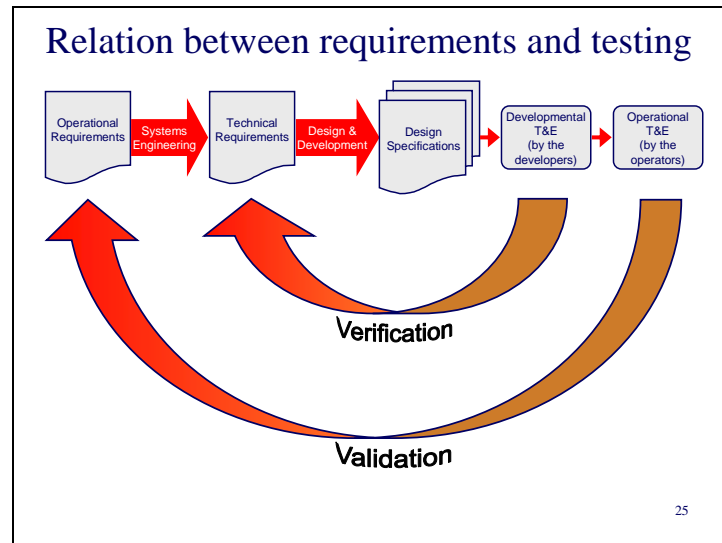
Eliminate all performance deficiencies

Operational Test and Evaluation

Test system performance with real users, under the cognizance of an independent test agent

Compare test results to the operational requirements themselves, rather than to their translation into performance requirements.

Evaluate system readiness for transition to the Production and Deployment Phase



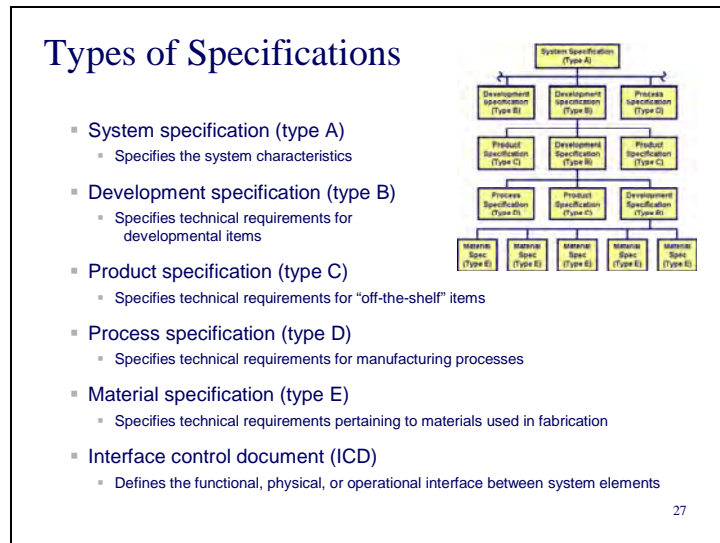
T&E comes in two flavors: Developmental T&E and Operational T&E. Developmental T&E is sometimes called Technical Evaluation (or TechEval) or, in the software world, alpha testing. Operational T&E is sometimes called OpEval or, in the software world, beta testing. DT&E serves the purpose of verifying that the final system design conforms to its technical requirements. OT&E serves the purpose of validating that the final system design satisfies its operational requirements **when operated by its intended users**. Involving the system designers in OT&E represents a conflict of interest, since the designers have a vested interest in proving that the system satisfies its operational requirements. This consideration motivates the requirement for an independent test agent when conducting OT&E.

What makes a good requirement?

Criterion	Description
Necessary	Can the system meet prioritized, real needs without it? If yes, the requirement isn't necessary.
Verifiable	Can one ensure that the requirement is met in the system? If not, the requirement should be removed or revised.
Unambiguous	Can the requirement be interpreted in more than one way? If yes, the requirement should be clarified or removed. Ambiguous or poorly worded requirements can lead to serious misunderstandings and needless rework.
Complete	Are all conditions under which the requirement applies stated? Also, does the specification include all known requirements?
Consistent	Can the requirement be met without conflicting with any other requirement? If not, the requirement should be revised or removed.
Traceable	Is the origin (source) of the requirement known, and is there a clear path from the requirement back to its origin?
Concise	Is the requirement stated simply and clearly?
Standard constructs	Requirements are stated as imperative needs using "shall." Statements indicating "goals" or using the words "will" or "should" are not imperatives.

26

This list of criteria for good requirements was taken from a publication of INCOSE, the International Committee on Systems Engineering. It is pretty much self-explanatory.



System specification (type A)

Includes the technical, performance, operational and support characteristics for the system as an entity. It includes the allocation of requirements of functional areas, and it defines the various functional-area interfaces. The information derived from the feasibility analysis, operational requirements, maintenance concept, and the functional analysis is covered.

Development specification (type B)

Includes the technical requirements for any item below the system level where research, design, and development are accomplished. This may cover an equipment item, assembly, computer program, facility, critical item of support, and so on. Each specification must include the performance, effectiveness, and support characteristics that are required in the evolving of design from the system level and down.

Product specification (type C)

Includes the technical requirements for any item below the top system level that is currently in the inventory and can be procured "off the shelf." This may cover standard system components (equipment, assemblies, units, cables), a specific computer program, a spare part, a tool, and so on. These are sometimes called "non-developmental items," or NDIs.

Process specification (type D)

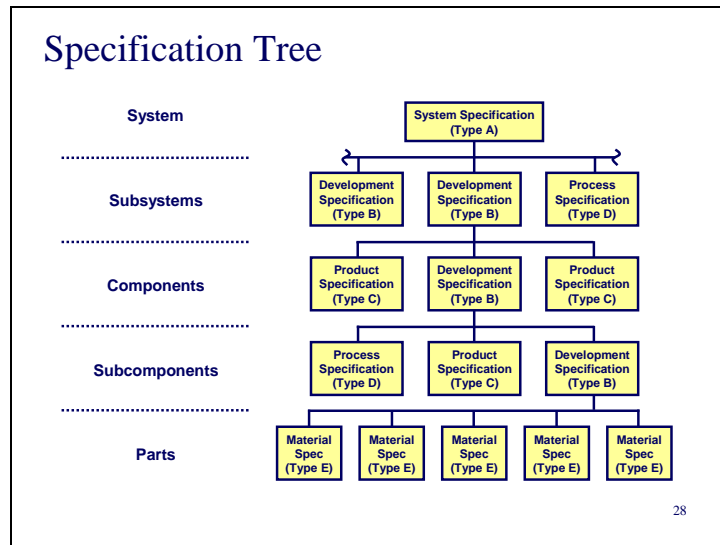
Includes the technical requirements that cover a service that is performed on any component of the system (e.g., machining, bending, welding, plating, heat treating, sanding, marking, packing, and processing).

Material specification (type E)

Includes the technical requirements that pertain to raw materials, mixtures (e.g., paints, chemical compounds), or semi-fabricated materials (e.g., electrical cable, piping) that are used in the fabrication of a product.

Interface control document

Describes the complete interface protocol from the lowest physical elements (e.g., the mating plugs, the electrical signal voltage levels) to the highest logical levels (e.g., the level 7 application layer of the ISO model), or some subset thereof. The purpose of the ICD is to communicate all possible inputs to and all potential outputs from a system element.



The specification tree shows the relationships among all the system's specifications, related to the system/subsystem/component hierarchy.

At the highest level is the system spec. Any path down through the hierarchy must end in a product or material that can be procured "off the shelf."

The system integrator, normally a prime contractor, is responsible for the system specification and for integrating the subsystems.

The subsystems themselves might be developed by the integrator, by a subcontractor to the integrator, or by separately contracted developers providing the subsystems as Government-furnished equipment (GFE).

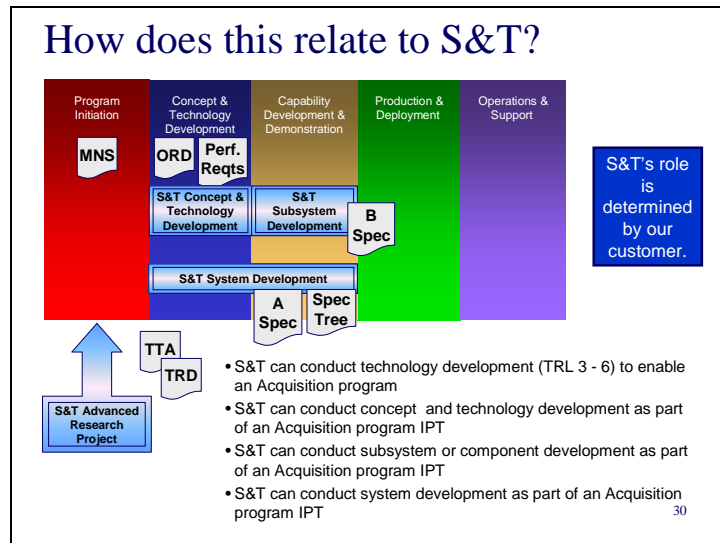
S&T's engagement with this specification tree depends on whether S&T is responsible for delivering a system, a subsystem, or a component. If delivering a subsystem or component, S&T would execute to a development specification (type B).

Sample System Specification (A-Spec)	
1.0 Scope	
2.0 Applicable Documents	
3.0 Requirements	
3.1 System Definition	
3.1.1 General Description	
3.1.2 Operational Requirements	
3.1.3 Maintenance Concept	
3.1.4 Functional Analysis & System Definition	
3.1.5 Allocation of Requirements	
3.1.6 Functional Interfaces and Criteria	
3.2 System Characteristics	
3.2.1 Performance Characteristics	
3.2.2 Physical Characteristics	
3.2.3 Effectiveness Requirements	
3.2.4 Environmental Requirements	
3.2.5 Reliability	
3.2.6 Maintainability	
3.2.7 Usability (Human Factors)	
3.2.8 Supportability	
3.2.9 Transportability / Mobility	
3.2.10 Other	
3.3 Design and Construction	
3.3.1 CAD/CAM Requirements	
3.3.2 Materials, Processes, and Parts	
3.3.3 Mounting and Labeling	
3.3.4 Electromagnetic Radiation	
3.3.5 Safety	
3.3.6 Interchangeability	
3.3.7 Workmanship	
3.3.8 Testability	
3.4 Documentation / Data	
3.5 Logistics	
3.5.1 Maintenance Requirements	
3.5.2 Supply Support	
3.5.3 Test and Support Equipment	
3.5.4 Personnel and Training	
3.5.5 Facilities and Equipment	
3.5.6 Packaging, Handling, Storage, Transport	
3.5.7 Computer Resources (Software)	
3.5.8 Technical Data	
3.5.9 Customer Services	
3.6 Producibility	
3.7 Disposability	
3.8 Affordability	
4.0 Test and Evaluation	
5.0 Quality Assurance	

This sample system specification is intended to illustrate the range of requirements which govern a system development (and, by extension, the development of subsystems or technologies).

Engineers tend to focus on functionality, but only a subset of the requirements relates to the functionality of the system (which of course is of direct interest to the operators). Other requirements address logistical concerns, such as maintainability, supportability, producibility, and affordability.

B-Specs and C-Specs are similar in nature to A-Specs, though with more emphasis on interface requirements and less emphasis (if any) on operational requirements (since subsystems and components are generally not “operated” in the same sense that systems are operated).



We've shown how the world of requirements relates to the world of Acquisition. But in almost all cases the S&T Directorate is not the Acquisition Sponsor and may not play a direct role in the Acquisition program. So how does all of this relate to S&T? There are several alternative roles for S&T.

S&T can execute an Advanced Research project intended to provide an Enabling Homeland Capability (EHC) to an Acquisition program. The EHC may in fact be necessary to make the Acquisition program possible, in which case it would execute before the initiation of Acquisition. Or the EHC may provide an enhancement to an existing Acquisition program, in which case it may transition its technology product into the Concept and Technology Development phase, to be included as part of the Alternatives Analysis.

OR

S&T can be tasked by an Acquisition program manager to conduct the technical aspects of the Concept and Technology Development phase.

OR

S&T can be tasked by an Acquisition program manager to execute the preliminary and detail design of a subsystem or component, as part of the Capability Development and Demonstration phase.


OR


S&T can be tasked by an Acquisition program manager to execute the technical aspects of the entire system development.

In the last three alternatives, where S&T is executing inside the Acquisition program, S&T would be a full member of the Acquisition program's Integrated Product Team (IPT).

How does this relate to Technology Commercialization?

- We've framed this discussion of requirements in the context of an Acquisition program. But what about commercialization?
- The goal of an S&T technology commercialization project is to induce the development and marketing of a COTS product.
- The principles of requirements development are the same for commercialization as for Acquisition though the commercial development is done by the **private sector**, using their own product-development process
- S&T might help stimulate technology commercialization via:
 - Operational requirements development (e.g., starting with a first-responder capability gap)
 - Performance requirements development (if the COTS product is a subsystem)
 - Market surveys
 - Private-sector partner(s)
 - Technology transfer
 - Grants
 - Standards



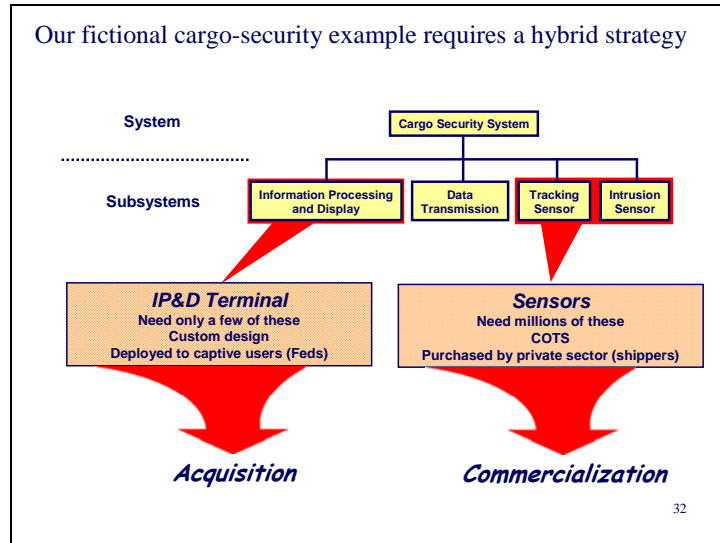


A DHS Acquisition program typically results in a DHS-funded DHS-owned product or system, manufactured and integrated by a prime contractor and deployed to a DHS workforce. But what if the goal is the realization of a Commercial Off-the-Shelf (COTS) product, to be made available to non-DHS users (State, local, and/or private sector) via normal commercial channels (such as catalog sales)?

Such a product development is not governed by DHS's System Development Life Cycle, but instead by S&T's Technology Commercialization framework (described in other mini-courses in this series).

How is the world of requirements different in this case?

The principles are the same, though very little of the product-realization process is under the direct control of DHS. Instead, the product or system is developed by the private sector, using their product-realization process. DHS's requirements role is limited to the development of operational requirements to address a capability gap (e.g., pertaining to first responders), and to the development of standards to govern the acceptance of the resulting product.



Our fictional cargo-security system has an awkward aspect when it comes to Acquisition. It is a distributed system whose sensors must be procured and installed by the private sector.

Thus, the development, deployment, operations, and support of its Information Processing and Display Terminal can be accomplished by a classical Acquisition program. But the implementation and distribution of its distributed sensors cannot be managed in that way, because the users of the sensors are not under CBP control, and therefore CBP cannot “deploy” to them.

The implementation of a commercialization program to create the necessary COTS sensors must address the following questions, among others:

What private-sector enterprise will develop and market the product?

What are the performance requirements which the product must satisfy, and how will compliance with these requirements be assured? (Note that “operational requirements” are not relevant here, since the sensors are subsystems which are not “operated”.)

Is there government-owned intellectual property which must be transferred to the private sector?



What will cause shippers to purchase and install the sensors? Grants? Regulation? Dual use? If dual use, how will the shippers interrogate the sensors?

Are new standards required?

How are the answers to these questions documented in an agreement with S&T's DHS customers, and who must be party to the agreement? CBP, certainly, but also Policy (to address regulation) and FEMA (to address grants)?

Speaking of Standards ...

We haven't said much about this puzzle piece ...



- Standards are "technical documents intended to establish common solutions to repetitive requirements."
- Congress and OMB require the use of technical standards from voluntary consensus standards bodies (replacing the pre-1995 reliance on government standards such as MIL-STDs)
- Some standards are commonly used as plug-ins to product or system specs to specify common performance requirements and test methods (e.g., to quantify shock and vibration resistance)
- In S&T's technology commercialization projects, standards can be developed to govern grants administration for products on the Authorized Equipment List
- Within S&T, consult the Office of T&E and Standards for further information

33

Most organizations use the generic term "standard" to refer to a wide variety of technical documents intended to establish common solutions to repetitive requirements. OMB Circular A-119 defines a standard as "common and repeated use of rules, conditions, guidelines, or characteristics for products or related processes and production methods and for related management systems practices." According to OMB, a standard can be "definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality or quantity in describing materials, processes, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength."

Congress passed the National Technology Transfer and Advancement Act of 1995 to promote the commercialization of technology and industrial innovation. The Act requires all federal agencies and departments to use technical standards that are developed or adopted by voluntary consensus standards bodies, unless such use is impractical or inconsistent with law.

The use of technical standards as plug-ins to product or system specifications is a powerful labor-saving tactic for developers. Why develop your own environmental requirements, for example, if someone else has already done it for you?

The use of product performance standards is a powerful incentive to private-sector product developers to develop products to conform to homeland-security needs as perceived by DHS, in cases where product marketing relies on DHS acceptance (as with the use of grants programs coupled with the Authorized Equipment List).

time →

Phase →		Concept and Technology Development			Capability Development and Demonstration		
		Needs Analysis	Concept Exploration	Concept Definition	Preliminary Design	Detail Design	Integration and Evaluation
Requirements output →		Operational requirements	Performance requirements	Functional specs	Design specs (A, B, C, D, E)	Test requirements	Production specs
Level →	System	Define operational objectives	Explore concepts	Define selected concept	Validate concept		Test and evaluate
	Subsystem	Visualize	Define functions	Define configuration	Validate selected subsystems		Integrate and test
	Component		Visualize	Select and define functions	Validate and specify construction	Design and test	Integrate
	Sub-component			Visualize	Define functions	Design	
	Part				Visualize	Select or adapt	

34

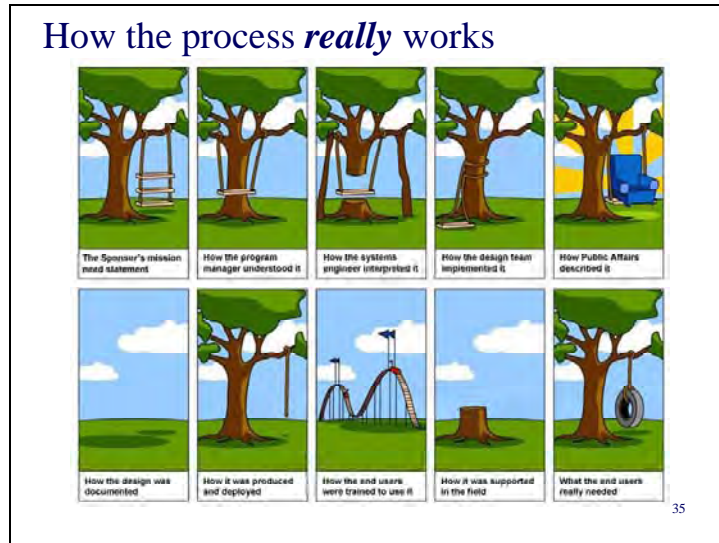
This slide summarizes the parallel evolution of requirements and designs to deeper and deeper levels in the system/subsystem/component hierarchy as time progresses and the design matures. The framework is DHS’s System Development Life Cycle.

Technical requirements are derived from operational requirements, and lower-level requirements from higher-level requirements, always maintaining traceability so that systems engineers and design engineers don’t lose sight of why a lower-level requirement is important to the customer.

At each phase and sub-phase, the higher-level requirements are re-validated before lower-level requirements are developed, to ensure that the link to customer needs is never broken.

The final design is verified against its technical requirements, to ensure that it conforms to all specifications. Then it is validated against operational requirements, to ensure that it addresses all customer needs.

The details of this requirements development differ depending on whether the development is a DHS Acquisition program or an S&T Technology Commercialization project, and the level of DHS control is radically different in these two types of product or system development. But the principles are the same.



Appendix E: Commercialization Briefing to Industry

The following pages include the slides used in briefing the private sector on business opportunities in DHS and ancillary markets.

Slide 1

Opportunities for the Private Sector



Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Department of Homeland Security
Science and Technology
Email: Thomas.Cellucci@dhs.gov

Slide 2

Discussion Guide

- Overview of Department of Homeland Security
- Commercialization initiatives at DHS
- Capstone Integrated Product Teams (IPTs)
- Market Potential is Catalyst for Rapid New Product Development
- Getting on the Same Page
- SECURE Program
- Safety Act Protection
- Tech Clearing House
- SBIR Opportunities
- Getting Involved
- Summary



Slide 3

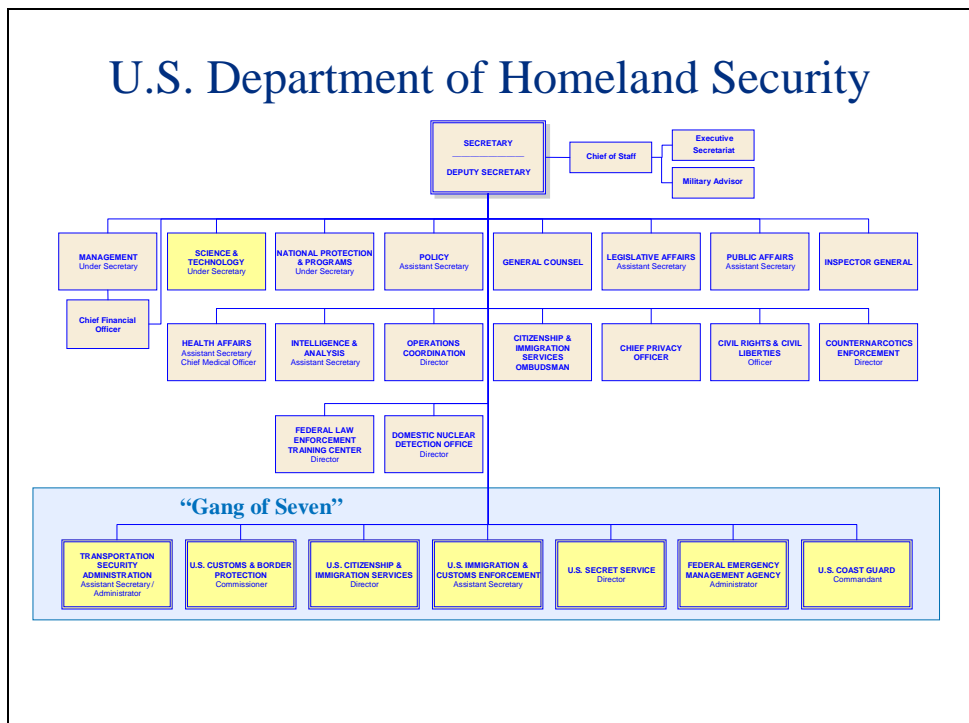
Homeland Security Mission



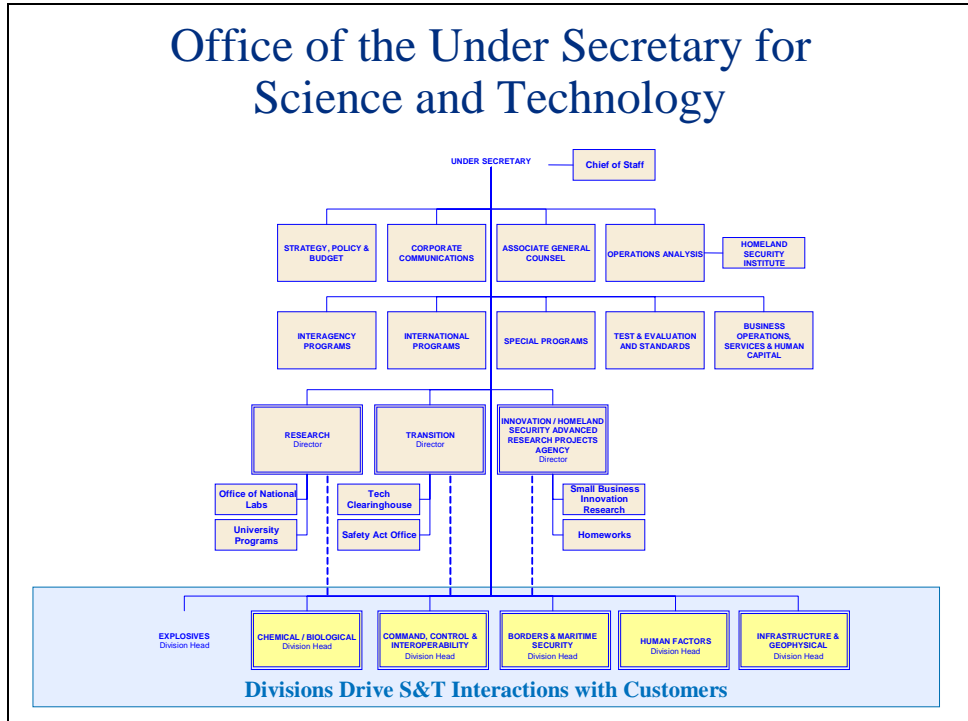
- Lead Unified National Effort to Secure America
- Prevent Terrorist Attacks Within the U.S.
- Respond to Threats and Hazards to the Nation
- Ensure Safe and Secure Borders
- Welcome Lawful Immigrants and Visitors
- Promote Free Flow of Commerce



Slide 4



Slide 5



Slide 6

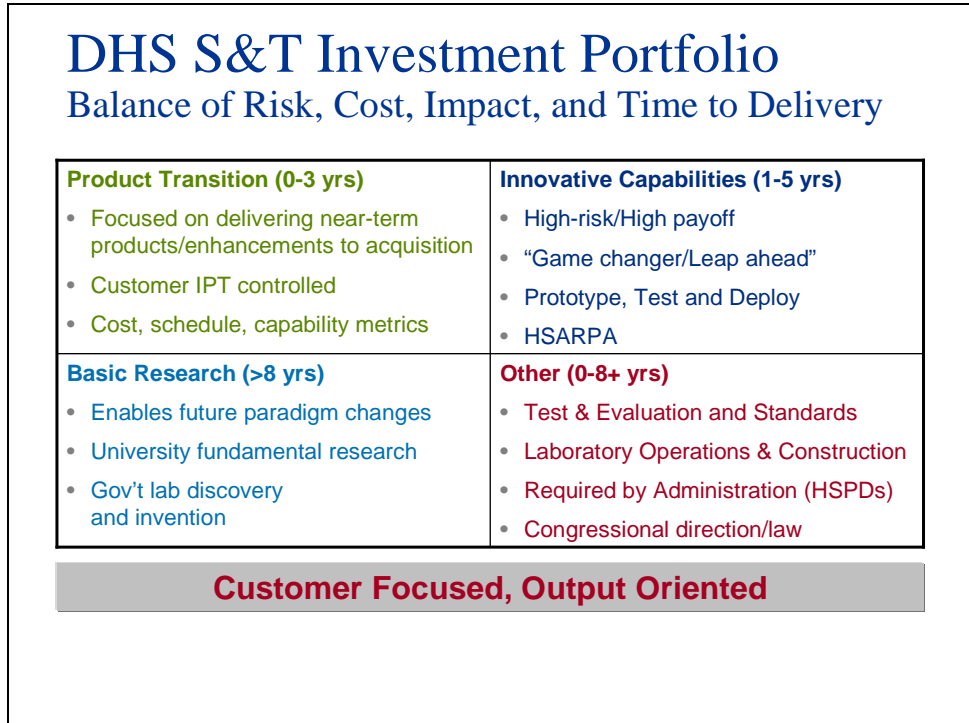
S&T Goals

Consistent with the Homeland Security Act of 2002

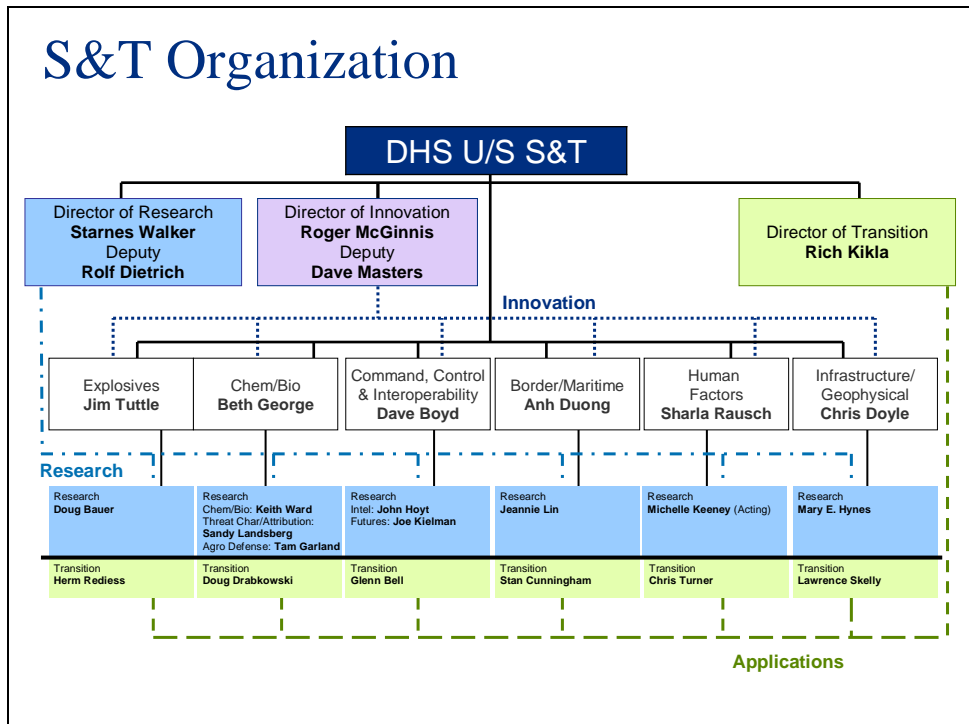
- **Accelerate the delivery of enhanced technological capabilities** to meet the requirements and fill capability gaps to support DHS agencies in accomplishing their mission.
- Establish a lean and agile world-class S&T management team to deliver the technological advantage necessary to ensure DHS Agency mission success and prevent technological surprise.
- Provide leadership, research and educational opportunities and resources to develop the necessary intellectual basis to enable a national S&T workforce to secure the homeland.



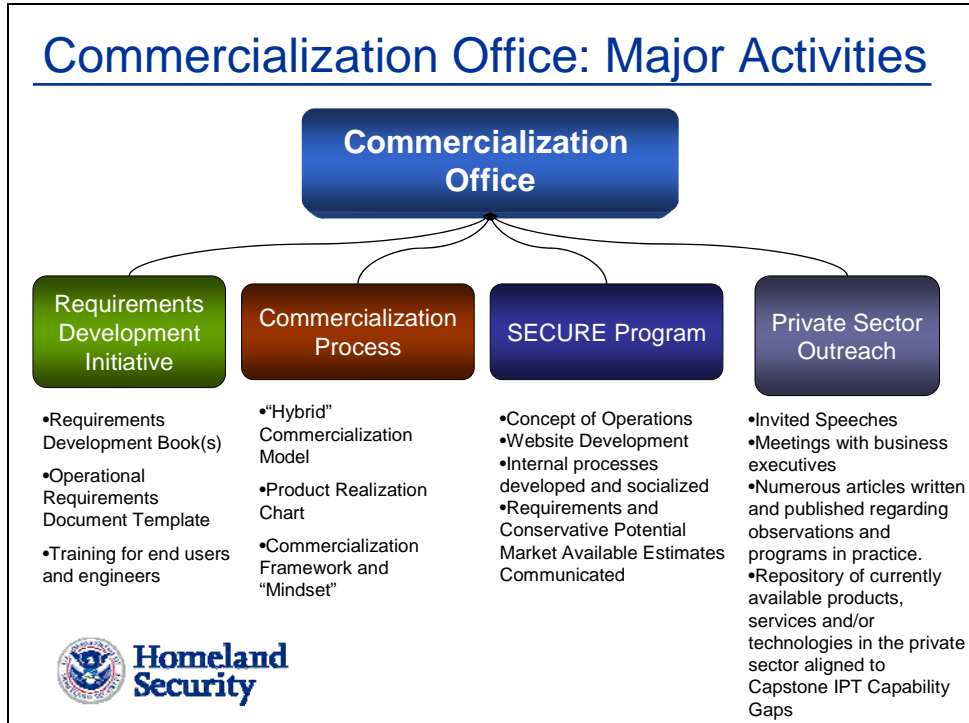
Slide 7



Slide 8



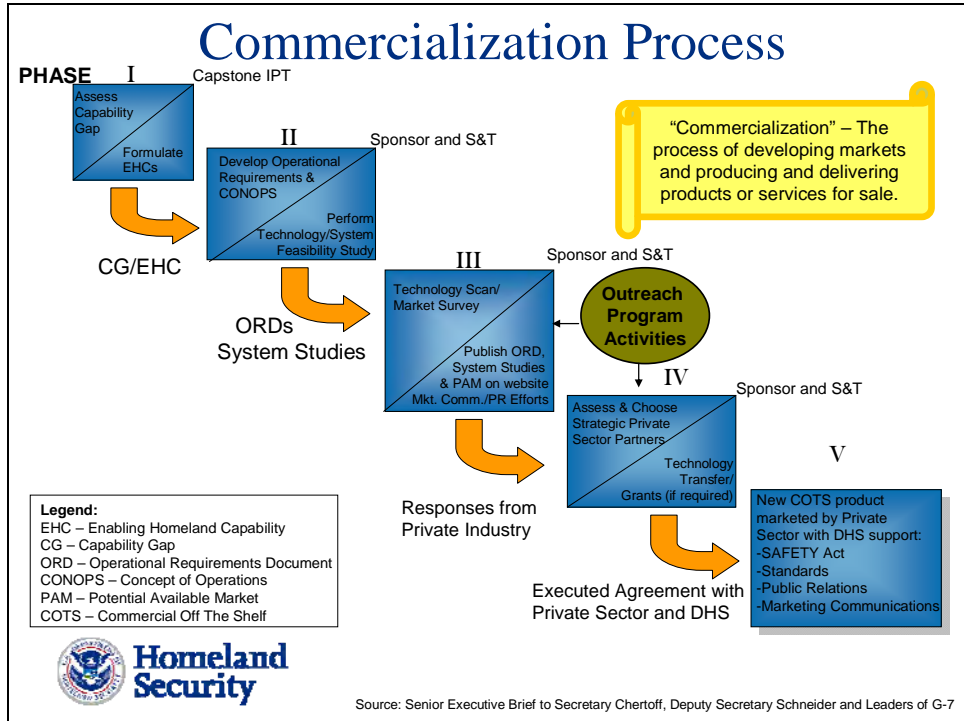
Slide 9



Slide 10



Slide 11



Slide 12

10 Reasons to Partner with DHS Science & Technology

Reasons Color Legend:

Economics-based

Public Relations-based

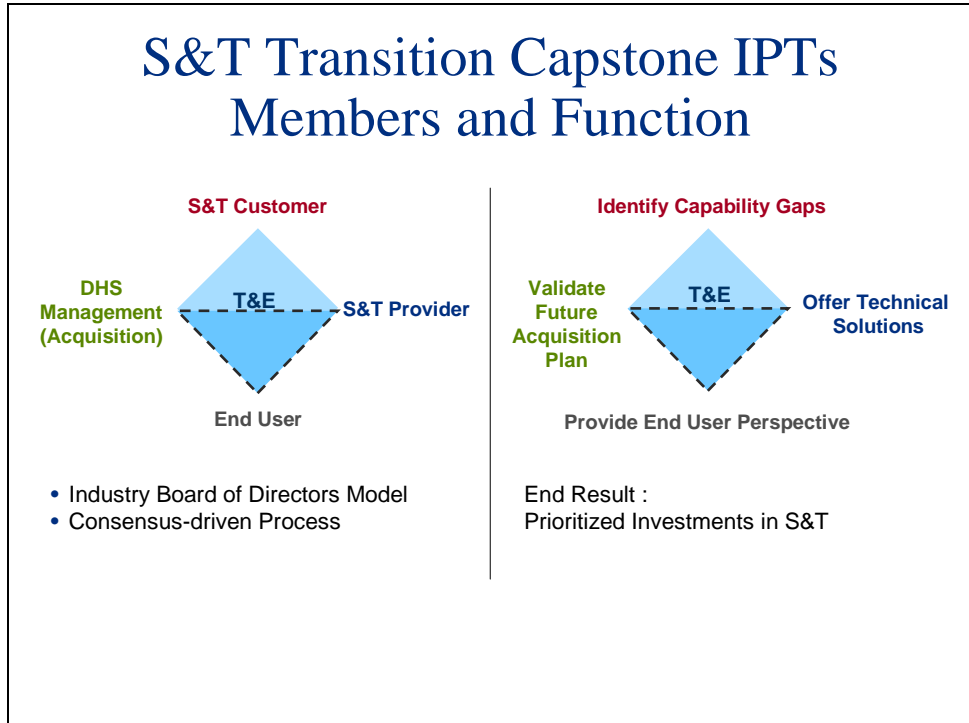
Business Development-based

Strategic Marketing-based

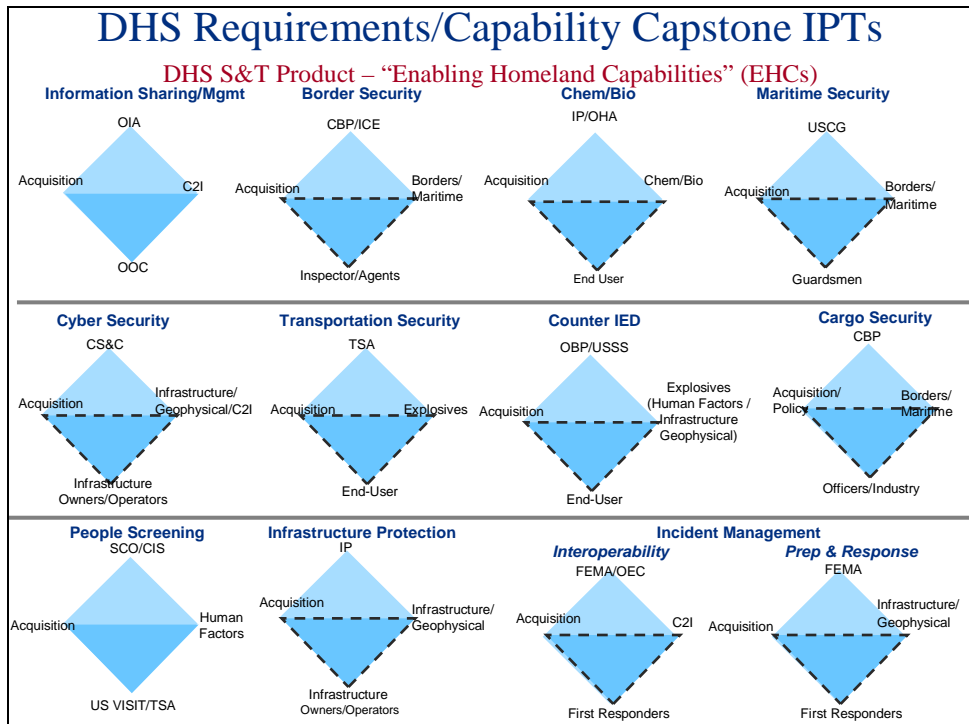
Technical Resources-based

1. Access to Sizeable DHS Market and Ancillary Markets
2. Leverage the Financial Strength/Stability of DHS and offset R&D costs through participation in mutually beneficial cost-sharing Programs
3. Utilize the SAFETY Act to gain liability protection and access DHS' array of PR and Market Communications services
4. Effectively reach the First Responders Market through FEMA-sponsored grant programs, the AEL (Approved Equipment List), other sponsored equipment lists and fast-track programs
5. Team with Science & Technology Personnel to leverage a vast Network of Laboratory Facilities for Technology and Product Development
6. Gain access to Test and Evaluation (T&E) Facilities for Product Development and actively participate in the generation of Standards, T&E methods and Regulations used at the tribal, local, state, and federal levels
7. Meet and establish Partnerships with others in the University, Business, and National Lab Communities
8. Potentially generate Licensing revenue and capture potential Derivative Product revenue
9. Leverage SBIRs, HITS and HIPS to gain experience with homeland security applications
10. Make a Real Difference by Developing Products to Defend the Homeland for Generations to come as well as gain recognition as a Corporate Citizen contributing to the Security of our Homeland

Slide 13

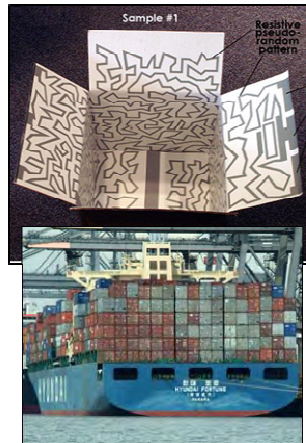


Slide 14



Cargo Security

Representative Technology Needs

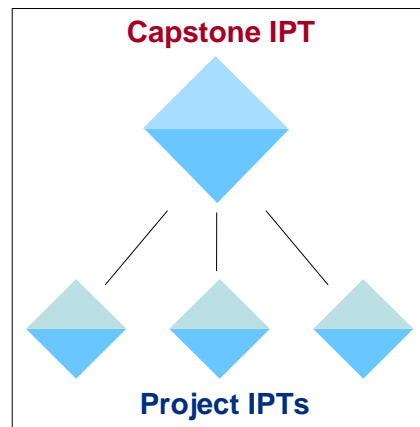


- Enhanced screening and examination by non-intrusive inspection
- Increased information fusion, anomaly detection, Automatic Target Recognition capability
- Detect and identify WMD materials and contraband
- Capability to screen 100% of air cargo
- Test the feasibility of seal security; detection of intrusion
- Track domestic high-threat cargo
- Harden air cargo conveyances and containers
- Positive ID of cargo and detection of intrusion or unauthorized access

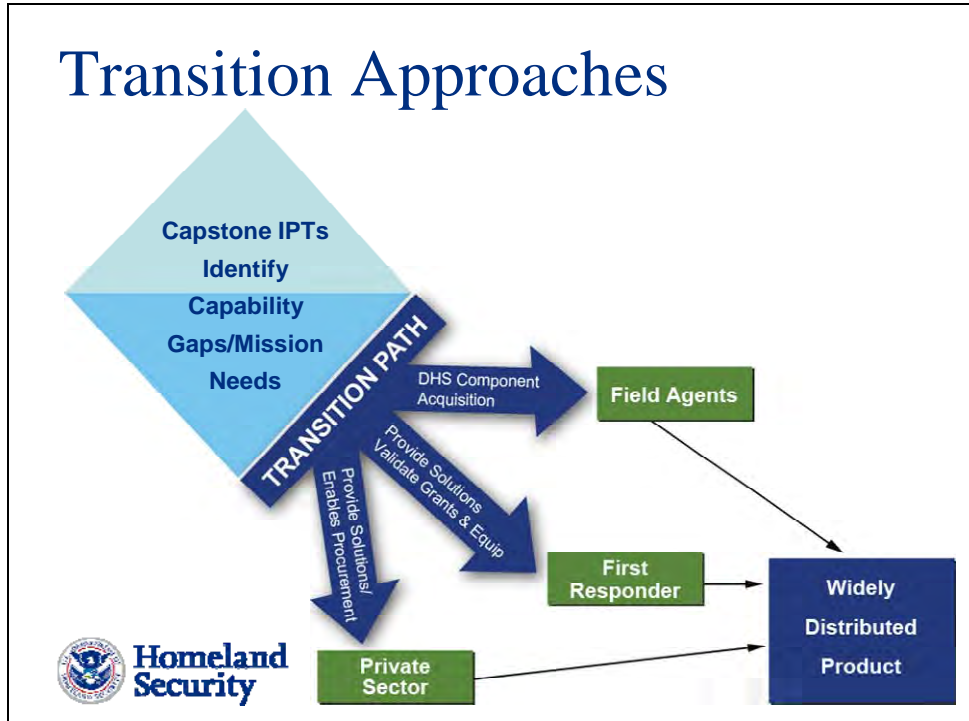
Source: S&T High Priority Technology Needs, May 2007

Establishment of Project IPTs: Detailed Specifications/Requirements

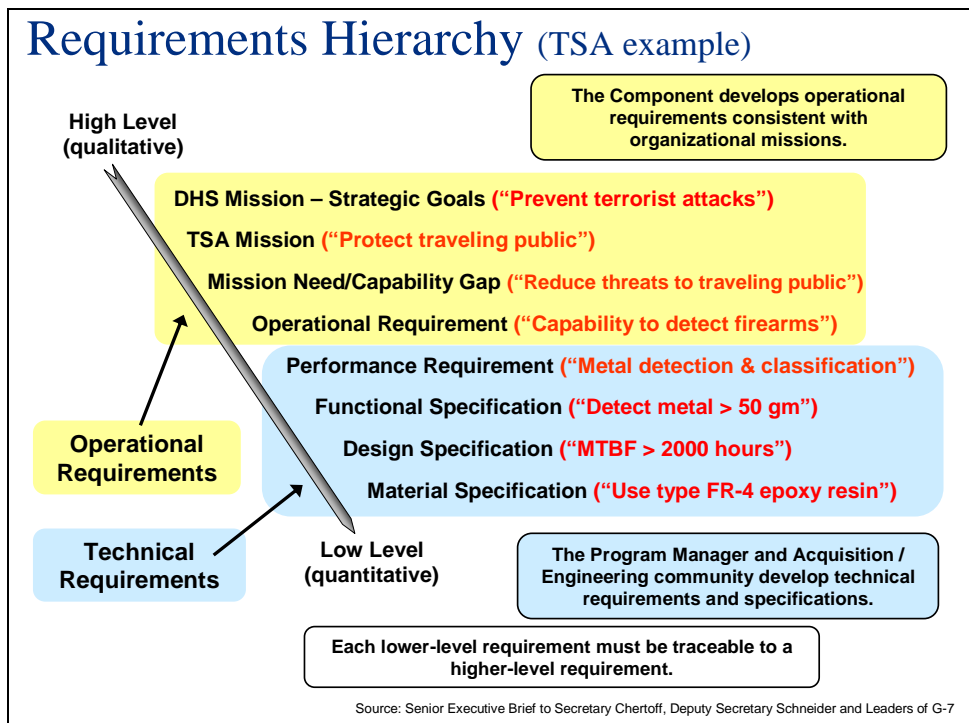
- Members:
 - S&T Program Manager(s)
 - Operating Component's Program Manager(s)
 - End-User(s)
 - Supplier/Provider
- Meet at Least Monthly
- Report to Capstone IPT Quarterly



Slide 17



Slide 18



ORD: Operational Requirements Document

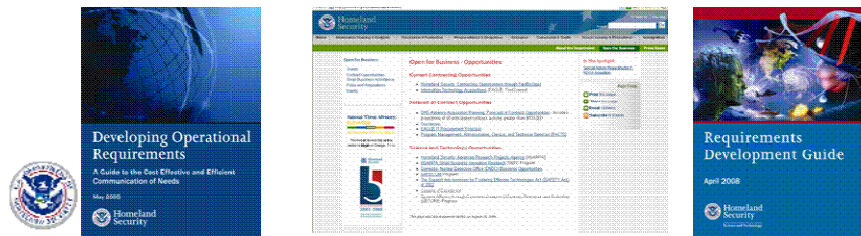
What: ORDs provide a clear definition and articulation of a given problem.

How: Training materials have been developed to assist drafting an ORD.

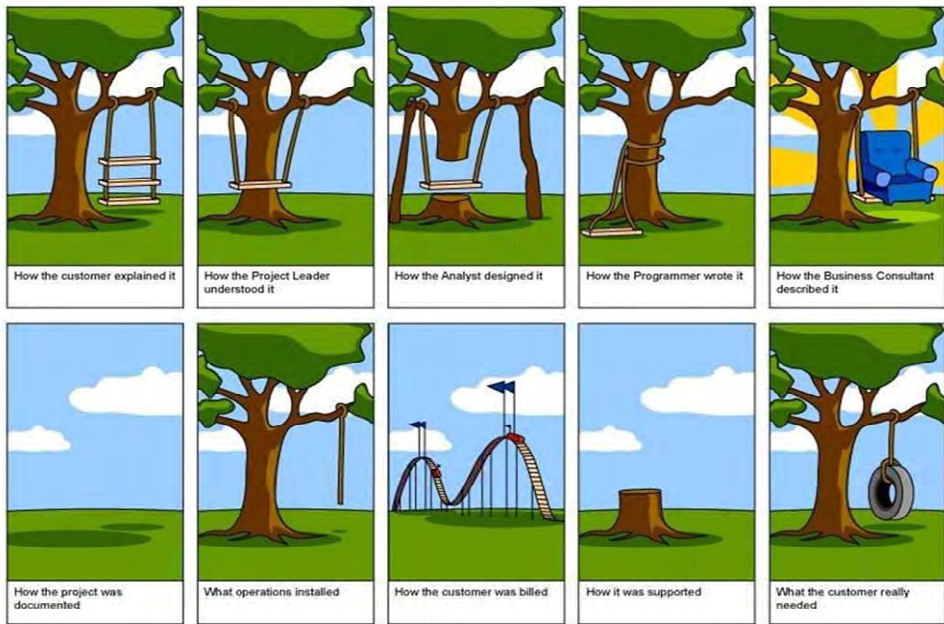
- *Developing Operational Requirements*, 194pp. Available online: http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf

When: For Use in Acquisition, Procurement, Commercialization and Outreach Programs –Any situation that dictates detailed requirements (e.g. RFQ, BAA, RFP, RFI, etc.)

Why: It's cost-effective and efficient for both DHS and all of its stakeholders.



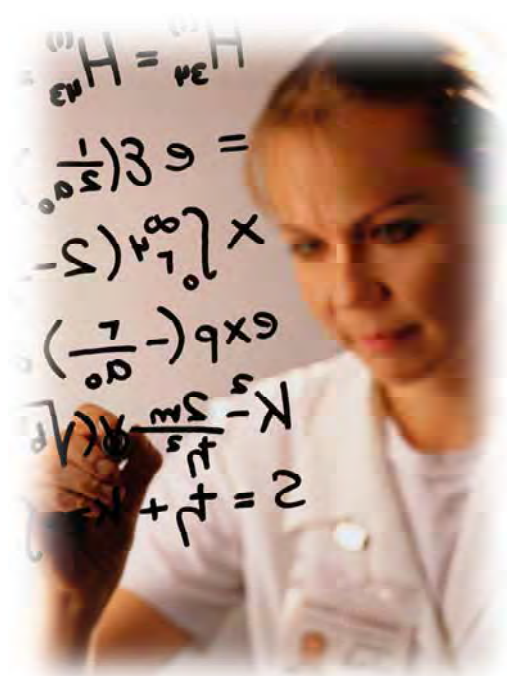
Does this look familiar?!



Author Unknown

Getting on the “Same Page”

- Historical Perspective
- Language is Key
- Communication is Paramount




Technology Readiness Levels (TRLs): Overview

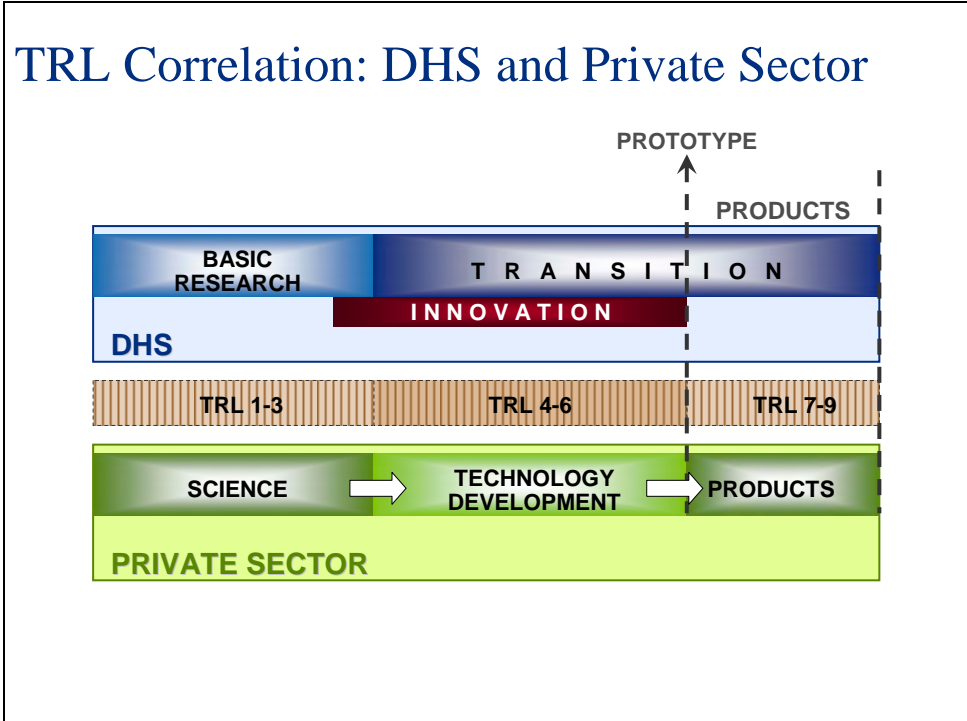
TRLs are NASA-generated and Used Extensively by DoD

Basic principles observed and reported	1	Basic
Technology concept and/or application formulated	2	
Analytical and experimental critical function and/or characteristic	3	
Component and/or breadboard validation in laboratory environment	4	Applied
Component and/or breadboard validation in relevant environment	5	
System/subsystem model or prototype demonstration in a relevant environment	6	Advanced
System prototype demonstration in a operational environment	7	
Actual system completed and 'flight qualified' through test and demonstration	8	
Actual system 'flight proven' through successful mission operations	9	

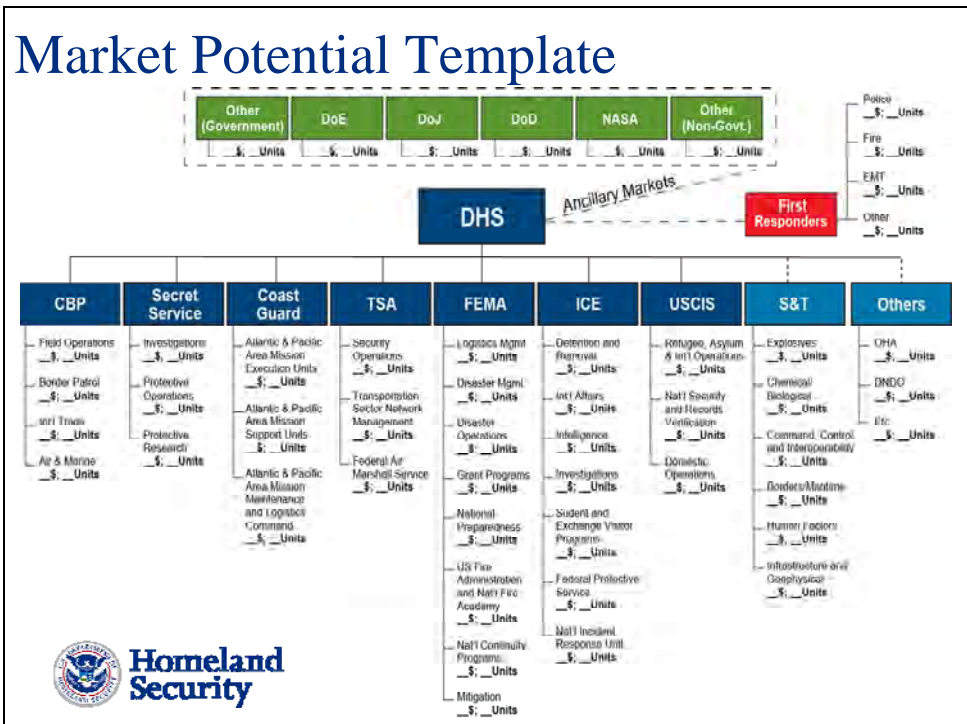
TECHNOLOGY MATURITY



Slide 23



Slide 24



Slide 25

Conservative Estimate: Number of First Responders in the US

- Homeland Security Presidential Directive 8
- Steve Golubic (FEMA)

Total: > 25.3 Million Individuals

Front Line > 2.3 Million

Support to Front Line > 23 Million

- Port Security
- Public Health
- Hospitals
- Transportation
- Emergency Management
- Clinics
- Venue Security
- Public Works/Utility
- School Security
- Response Volunteers

Slide 26

Call to Action: Mutual Benefits Create “Win-Win-Win” Relationships

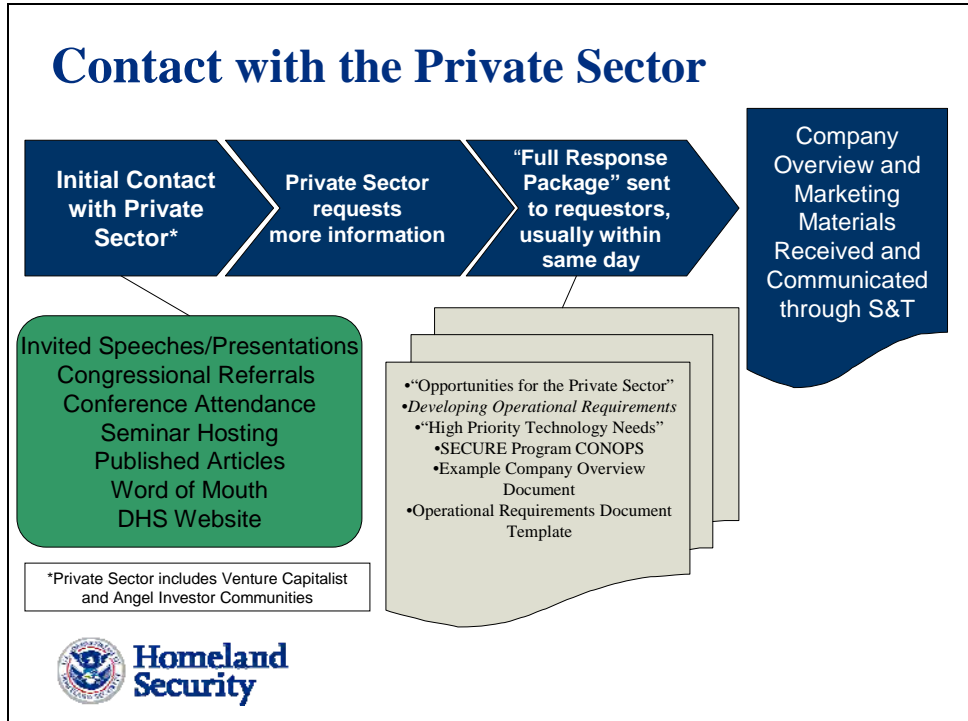
```
graph TD; A((1. Learn Current DHS Needs  
Visit www.FedBizOpps.gov  
and www.hsarpabaa.com  
for current solicitations)) --> B((2. Inform DHS of Products/Capabilities  
Request DHS – S&T Full Response Package at thomas.cellucci@dhs.gov)); B --> C((3. Establish Mutually-beneficial Relationship)); C --> A;
```

1. Learn Current DHS Needs
Visit www.FedBizOpps.gov and www.hsarpabaa.com for current solicitations

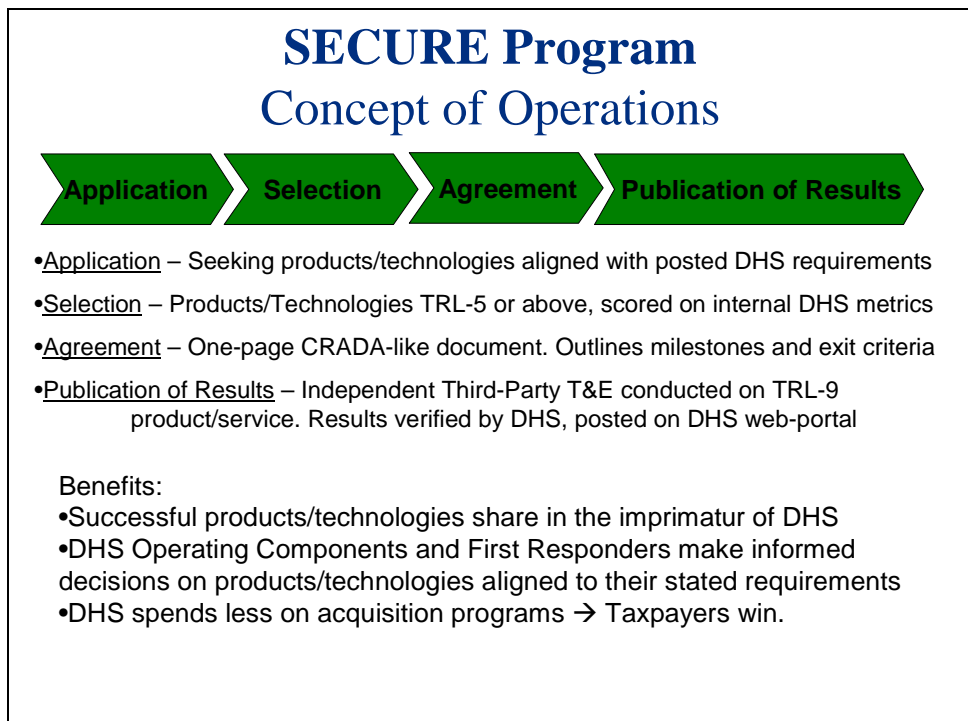
2. Inform DHS of Products/Capabilities
Request DHS – S&T Full Response Package at thomas.cellucci@dhs.gov

3. Establish Mutually-beneficial Relationship
Interact with DHS

Slide 27



Slide 28



Slide 29

SECURE Program Benefit Analysis “Win-Win-Win”

Taxpayers	Private Sector	Public Sector
1. Citizens are better protected by DHS personnel using mission critical products	1. Save significant time and money on market and business development activities	1. Improved understanding and communication of needs
2. Tax savings realized through Private Sector investment in DHS	2. Firms can genuinely contribute to the security of the Nation	2. Cost-effective and rapid product development process saves resources
3. Positive economic growth for American economy	3. Successful products share in the “imprimatur of DHS”; providing assurance that products really work	3. Monies can be allocated to perform greater number of essential tasks
4. Possible product “spin-offs” can aid other commercial markets	4. Significant business opportunities with sizeable DHS and DHS ancillary markets	4. End users receive products aligned to specific needs
5. Customers ultimately benefit from COTS produced within the Free Market System – more cost effective and efficient product development	5. Commercialization opportunities for small, medium and large business	5. End users can make informed purchasing decisions with tight budgets

Slide 30

The screenshot shows the DHS Open for Business website. The address bar displays <http://www.dhs.gov/xopnbiz/>. The page features a navigation menu with categories like Home, Information Sharing & Analysis, and Preparedness & Response. The main content area is titled "Open For Business" and includes sections for "Spotlight" (Information Technology Acquisitions, E-Verify Program), "Programs and Services" (Acquisition Policies and Regulations, Opportunities, Small Business Procurement Assistance, Grants, Reports and Notices, Forms), and "Resources" (SAFETY Act, System Efficacy through Commercialization, Utilization, Relevance and Evaluation (SECURE) Program resources for SECURE).

Federal Business Opportunities

Sites where the Office of Procurement Operations (OPO) posts opportunities for prospective suppliers to offer solutions to DHS – S&T's needs:

- www.FedBizOpps.gov
- www.HSARPAbaa.com
- www.SBIR.dhs.gov
- www.Grants.gov

take advantage of...

- **Vendor Notification Service:** Sign up to receive procurement announcements and solicitations/BAA amendment releases, and general procurement announcements.
<http://www.fedbizopps.gov>
- **S&T's HSARPA website:** Register to join the HSARPA mailing list to receive various meeting and solicitation announcements. Link to Representative High Priority Technology Areas, where DHS areas of interest can be found.
<http://www.hsarpabaa.com>
- **Truly Innovative and Unique Solution:** Refer to Part 15.6 of the Federal Acquisition Regulation (FAR) which provides specific criteria that must be met before a unsolicited proposal can be submitted to Kathy Ferrell.
<http://www.acquisition.gov/far/current/html/Subpart%2015.6.html>

Contact Information:
 Kathy Ferrell
 Department of Homeland Security
 Office of the Chief Procurement Officer
 245 Murray Dr., Bldg. 410
 Washington, DC 20528
unsolicited.proposal@dhs.gov
 202-447-5576

Show Us the Difference...

Hall's Competitive Model

As a function of:

- Market
- Application
- Technology

Differentiation = (A+B)C/(D+E)



SAFETY Act

Support Anti-Terrorism by Fostering Effective Technologies Act of 2002

- Enables the development and deployment of qualified anti-terrorism technologies
- Provides important legal liability protections for manufacturers and sellers of effective technologies
- Removes barriers to industry investments in new and unique technologies
- Creates market incentives for industry to invest in measures to enhance our homeland security
- The SAFETY Act liability protections apply to a vast range of technologies, including:
 - Products
 - Services
 - Software and other forms of intellectual property (IP)

Examples of eligible technologies:

- Threat and vulnerability assessment services
- Detection Systems
- Blast Mitigation Materials
- Screening Services
- Sensors and Sensor Integration
- Vaccines
- Metal Detectors
- Decision Support Software
- Security Services
- Data Mining Software

Protecting You, Protecting U.S.

Criteria as stated in the SAFETY Act

- Is it an Anti-Terrorism Technology?
- Is it effective and available?
- Does it possess large potential third party liability risk exposure?
- Does Seller need SAFETY Act?
- Does it perform as intended?
- Does it conform to Seller's specifications?
- Is it safe for use as intended?

Addition SAFETY Act information...

Online: www.safetyact.gov Email: helpdesk@safetyact.gov

Toll-Free: 1-866-788-9318

Award Criteria

	Developmental Testing and Evaluation (DT&E)	Designation	Certification
Effectiveness Evaluation Conclusion	Needs more proof, has potential	Demonstrated effectiveness, i.e. Developmental testing (with confidence of repeatability)	Consistently proven effectiveness, i.e. operational performance (with high confidence of enduring effectiveness)
Protection	Liability cap • only for identified test event(s) and for limited duration (=3yrs)	Liability cap • for any and all deployments in 5-8 year term	Government Contractor Defense (GCD) • for any and all deployments in 5-8 years term
Examples	• EDS not yet TSL Certified • Novel incident pattern matching service	• Radiological detector with <u>laboratory</u> success Opt-out screeners, only similar projects completed	• EDS TSL Certified • Well-documented infrastructure protection service with history of excellent performance and meeting DoE standards

EDS=Explosive Detection System TSL=Transportation Security Laboratory (TSA)

Slide 37

The screenshot shows the Department of Homeland Security SBIR Program website. A yellow box highlights the URL <https://www.sbir.dhs.gov>. Three red callout boxes with arrows point to specific content: 'Safety Act' points to the 'SAFETY Act' link in the navigation bar; 'Other Funding Opportunities' points to the 'Topic Recommendations' link in the left sidebar; and 'Topic Recommendations' points to the 'Topic Recommendations' link in the main content area.

Slide 38

Tech Clearinghouse Mission

To rapidly disseminate technical information concerning existing and desired products and services to/between Federal, State, Local, and Tribal Government and the Private Sector in order to encourage technological innovation and facilitate the mission of the Department of Homeland Security.

- Establishes Central Federal Technology Clearinghouse
- Issues Announcements for Innovative Solutions
- Establishes S&T Technical Assessment Team
- Provides guidance for the evaluation, purchase, and implementation of homeland security enhancing technologies
- Provides users with information to develop or deploy technologies that would enhance homeland security
- Enables technology transfer

Improved Knowledge Sound Acquisition Decisions

TechSolutions

The mission of TechSolutions is to rapidly address technology gaps identified by Federal, State, Local, and Tribal first responders

- Field prototypical solutions in 12 months
- Cost should be commensurate with proposal but less than \$1M per project
- Solution should meet 80% of identified requirements
- Provide a mechanism for Emergency Responders to relay their capability gaps
 - Capability gaps are gathered using a web site (www.dhs.gov/techsolutions)
- Gaps are addressed using existing technology, spiral development, and rapid prototyping
- Emergency Responders partner with DHS from start to finish

Rapid Technology Development
Target: Solutions Fielded within 1 year, at <\$1M

TechSolutions Investments

Seatbelt Safety for
Emergency Vehicles



Next Generation
Breathing Apparatus



Fire Ground Compass



----- Under Consideration -----

Vehicle Mounted Chem/Bio
Sensor Detection



Slide 41

Getting Involved: S&T Contacts

Division	Email
Jim Tuttle	S&T-Explosives@dhs.gov
Beth George	S&T-ChemBio@dhs.gov
David Boyd	S&T-C2I@dhs.gov
Anh Duong	S&T-BordersMaritime@dhs.gov
Sharla Rausch	S&T-HumanFactors@dhs.gov
Chris Doyle	S&T-InfrastructureGeophysical@dhs.gov
Rich Kikla	S&T-Transition@dhs.gov
Starnes Walker	S&T-Research@dhs.gov
Roger McGinnis	S&T-Innovation@dhs.gov

Slide 42

Summary

Detailed Requirements
Sizeable Market Potential
Delivered Products – PERIOD!

How Can You Afford NOT to Partner with DHS S&T?

Questions/Comments:
Thomas A. Cellucci, Ph.D., MBA
thomas.cellucci@dhs.gov

Slide 43

U.S. Department of Homeland Security: Science and Technology Directorate's Chief Commercialization Officer

Thomas A. Cellucci, PhD, MBA was recently appointed Chief Commercialization Officer for the Department of Homeland Security's Science and Technology (S&T) Directorate. The Chief Commercialization Officer (CCO) is responsible for initiatives that identify, evaluate and commercialize technology for the specific goal of rapidly developing and deploying products and services that meet the specific operational requirements of the Department of Homeland Security's Operating Components and its end users. The CCO also develops and drives the implementation of DHS-S&T's outreach with the private sector to establish and foster mutually-beneficial working relationships to facilitate cost-effective and efficient product/service development efforts.



Cellucci is an accomplished serial entrepreneur, seasoned senior executive and Board member possessing extensive corporate and VC experience across a number of worldwide industries. Profitably growing high technology firms at the start-up, mid-range and large corporate level has been his trademark. In 1999, he founded a highly successful management consulting firm--Cellucci Associates, Inc. -- that raises capital and provides strategic business services to top-tier global high technology firms. He serves on both public and private Boards and has authored or co-authored over 120 articles on Nanotechnology, Laser physics, Photonics, Environmental disturbance control, MEMS test and measurement, Mistake-proofing enterprise software, and Sales & Marketing. He has also held the rank of Lecturer or Professor at institutions like Princeton University, University of Pennsylvania and Camden Community College. Cellucci also co-authored ANSI Standard Z136.5 "The Safe Use of Lasers in Educational Institutions".

As a result of his consistent achievement in the commercialization of emerging technologies, Cellucci has received numerous awards and citations from industry, government and business. Cellucci earned a PhD in Physical Chemistry from the University of Pennsylvania, an MBA from Rutgers University and a BS in Chemistry from Fordham University. He has also attended and lectured at executive programs at the Harvard Business School, MIT Sloan School, Kellogg School and others. Dr. Cellucci is regarded as an authority in rapid time-to-market new product development and is a frequent public speaker.

Slide 44



Homeland Security

Appendix F: SECURE Program Concept of Operations

The following pages include the overview and Concept of Operations for the SECURE (System Efficacy through Commercialization, Utilization, Relevance and Evaluation) Program.

SECURE Program: Concept of Operations



Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Department of Homeland Security
Science and Technology Directorate
Email: Thomas.Cellucci@dhs.gov



**Homeland
Security**

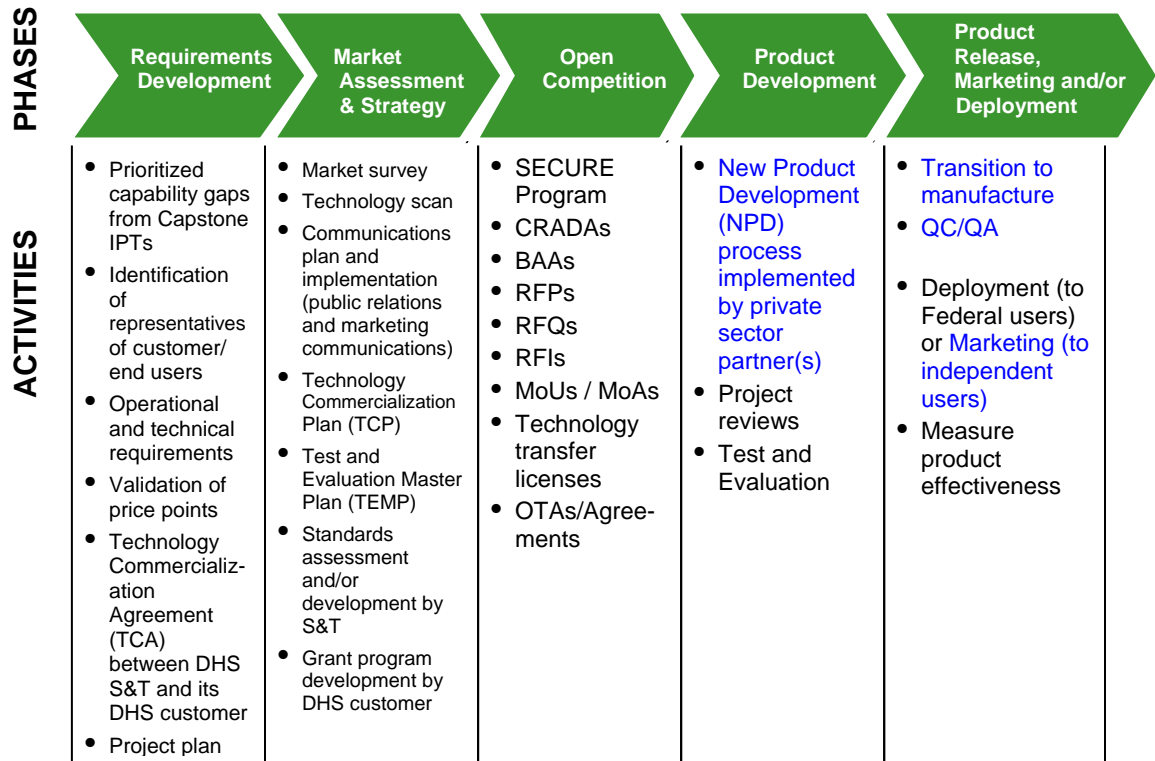
SECURE Program: System Efficacy through Commercialization, Utilization, Relevance and Evaluation

Scope:

We have developed a comprehensive program to enable DHS-S&T to efficiently and cost-effectively leverage the resources, skills, experience and productivity of the Private Sector to develop technologies and products in alignment with specific requirements obtained from DHS Components, the First Responder Community and other End-Users involved in Homeland Security applications.

Overall Process:

Below is a graphical representation of the overall outreach process we have implemented to stimulate and engage the Private Sector to use its resources to rapidly develop technology, products and services that can yield significant benefits for DHS-S&T with a speed-of-execution not typically observed in the Public Sector.



Legend: Black text = Typical Government activities
 Blue text = Typical Private-Sector activities

Outreach to the Private Sector



Program Process:

In order to provide DHS Operating Components, the First Responder Community and other End-Users with products that meet their specific requirements, DHS-S&T will provide a vehicle by which Private Sector entities can offer products and/or conduct product development geared specifically toward meeting those needs. Private Sector entities currently possessing a technology/product/system rated at a Technology Readiness Level TRL-5 (i.e. applied or advanced R&D) or above that potentially closes a defined DHS capability gap by addressing detailed operational requirements supplied by DHS-S&T will have the opportunity to continue development of their technology/product/system to TRL-9 (i.e. fully field deployable product) at the expense of the Private Sector entity with the assurance that DHS-S&T will verify their independent third-party test(s) of a given technology/product/system.

Only when TRL-9 is achieved, will Private Sector entities be assured that their testing and evaluation (T&E) of the fully deployable technology/product/system (performed by an independent third-party) is verified by a DHS-S&T assessment of a given third party, independent T&E. DHS-S&T will publish its assessment on the DHS' public website as validation of the success (or failure) to meet the Private Sector entity's own established specifications. This approach enables DHS-S&T to review several highly developed technologies/products/systems in an open and fair manner while successful Private Sector entities will share in the imprimatur of DHS-S&T. DHS Operating Components, the First Responder Community and other End-Users are enabled to make informed purchasing decisions for necessary technologies/products/systems to enhance their capabilities through meeting their detailed requirements. In addition, these solutions are excellent candidates for liability protection under the provisions of the DHS SAFETY Act.



Application:

In the spirit of open and free competition, and in order to capitalize on the free-market system, DHS-S&T intends to publish this program and all ancillary requirements documents/information on the DHS-S&T website. These materials will be accessible by all businesses. Given this information, Private Sector entities may file an application to develop or enhance their technology/product/system in cooperation with DHS-S&T that will improve upon currently fielded DHS technologies. We envision a simple application for this program that can be completed via the internet. The contents of the application will include basic, non-proprietary business information, contact information, alignment to widely available DHS-S&T capability gaps and ancillary requirements documents we choose to offer such as ORDs (Operational Requirement Documents), etc.



Selection:

In order to be fully considered by DHS-S&T for cooperative development:

The company entity must demonstrate they possess technology at TRL-5 (i.e. applied or advanced R&D) or above and possess the resources to invest in the commercialization of its technology to TRL-9 (i.e. fully field deployable product)

The company entity must propose a technology/product development effort that has clear and substantial alignment with published DHS-S&T capability gaps and other announced requirements

A DHS selection committee will be established to review applications and monitor the mutually-agreed-upon roles and responsibilities of the partnership.

The selection committee will consider these and other DHS proprietary metrics for selection consideration.



Agreement:

The Private Sector entity and DHS-S&T will execute a simple, straightforward and binding agreement whereby the Private Sector entity details milestones with dates and agrees to bear full and total financial responsibility to develop its technology/product/system to a TRL-9 state (if not already at that level). DHS-S&T will publish on the DHS-S&T website the factual findings of such assessment. DHS-S&T has the right to cancel an agreement if the Private Sector entity does not fulfill/achieve any of its milestones by the mutually-agreed-upon dates.



Publication of Results:

It is apparent that the Private Sector highly values DHS-S&T’s potential assessment of a given product’s independent third-party test and evaluation. DHS-S&T will openly publish these T&E results on the DHS public web portal for review by the DHS Operating Components, First Responder communities and other end users.

SECURE Program: System Efficacy through Commercialization, Utilization, Relevance and Evaluation

Appendix G: DHS Management Directive 1400

The following pages include the Investment Review Process – DHS Management Directive 1400. *Note, at the time of publication DHS Management Directive 1400.1, which will update MD 1400, is in its final review stages.

INVESTMENT REVIEW PROCESS

1. Purpose

To establish an Investment Review Process (IRP) that will:

- A. Integrate capital planning and investment control (CPIC), budgeting, acquisition, and management of investments (both Information Technology (IT) and non-IT) to ensure scarce public resources are wisely invested and the requirements of the authorities listed below are achieved.
- B. Ensure that spending on investments directly supports and furthers DHS's mission and provides optimal benefits and capabilities to stakeholders and customers.
- C. Identify poorly performing investments that are behind schedule, over budget, or lacking in capability so corrective actions can be taken.
- D. Identify duplicative efforts for consolidation and mission alignment when it makes good sense or when economies of scale can be achieved.
- E. Improve investment management in support of the President's Management Agenda (PMA).

2. Scope

This Management Directive (MD) applies to all Departmental offices, directorates, agencies, and sub-elements within DHS (hereafter referred to as Organizational Elements), unless specifically exempted by statutory authority. Additionally, this MD applies to the acquisition of all capital assets, including services. Joint agency initiatives will follow the IRP of the designated lead agency (or managing partner).

3. Authorities

- A. Office of Management and Budget (OMB) Circular A-11, Preparing, Submitting and Executing the Budget, June 2002.
- B. Public Law 107-296, the Homeland Security Act of 2002.
- C. Clinger-Cohen Act

D. OMB Circular A-130, Management of Federal Information Resources, Nov 2001.

E. OMB Circular A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs, Jan 2002.

4. Definitions

For detailed definitions and applicable terms, reference Enclosure (1).

5. Policy and Procedures

The management of Departmental investments is a key strategic function of DHS. Proper management also warrants a structured program management program, a systematic process for review and approval, visibility, and accountability to senior management.

There are two distinct objectives of the IRP: 1) acquisition oversight of new investments throughout their life cycle, and 2) portfolio management to achieve budget goals and objectives. The guiding principles for this process provided in Enclosure (2) should be used to further these objectives.

DHS investments are categorized in four levels based on defined criteria. These levels determine the documentation required for review as well as the approval levels. Threshold criteria will be reevaluated 6 months after the directive is issued and annually thereafter.

Threshold	Review/ Approval	Document Required	Criteria ¹	Additional IT Criteria ¹
Level 1	Investment Review Board (IRB) / Deputy Secretary	Exhibit 300	<ul style="list-style-type: none"> Contract cost exceeds \$50M Importance to DHS strategic and performance plans High development, operating, or maintenance cost High risk High return Significance in resource administration 	<ul style="list-style-type: none"> Life-cycle cost exceeds \$200M
Level 2	Management Review Council (MRC) / Directorate Head or Under Secretary	Non-IT: Exhibit 300 Light IT: Exhibit 300 Light	<ul style="list-style-type: none"> Contract cost \$5M - \$50M Impacts more than one DHS component Significant program or policy implication High executive visibility 	<ul style="list-style-type: none"> Life-cycle cost \$20M - \$200M Financial system with operation cost exceeding \$500K Was major in FY04 budget submission Meets following criteria: E-Gov related, FEA, DHS EA, Strategic Data/Information sharing, DHS utility services and infrastructure, new technology initiatives, and sensitive initiatives (for definitions see Enclosure (1))
Level 3 (IT Only)	Enterprise Architecture Board (EAB) / CIO	Exhibit 300 Light		<ul style="list-style-type: none"> Annual costs \$1M - \$5M annually Life-cycle costs \$5M - \$20M Falls in one of the E-Gov transformation focus areas (e.g. financial management, data and statistics, human resources, monetary benefits, criminal investigations, public health monitoring, etc.)

Level 4	Directorates or Organizational Elements	IT: Exhibit 53 Information	<ul style="list-style-type: none"> Total acquisition cost less than \$5M 	<ul style="list-style-type: none"> Does not meet Level 3 criteria IT service contract Total acquisition costs between \$100,000 and \$5M, and involves modifications / revisions to the existing IT infrastructure or security, with no new technology involved
<ul style="list-style-type: none"> General Notes: Level 1, 2, and 3 IT investments require review by the DHS CIO and the EAB. Exhibit 300 Light is a DHS designation, not an official OMB Exhibit. Note 1: Threshold levels are determined based on one or more of listed criteria. 				

For Level 1 programs the Deputy Secretary is the acquisition executive who has final decision authority at a program’s Key Decision Point (KDP). For Level 2 programs and below, the Under Secretary for the program’s sponsoring directorate, the Commandant of the Coast Guard, or the Director of the Secret Service is the acquisition executive and decision authority. The Under Secretary for Management supports the acquisition executives by conducting formal, comprehensive investment reviews of acquisition programs through various boards and councils established by this directive.

6. Roles and Responsibilities

A. Investment Review Board (IRB).

The IRB is the executive review board that provides acquisition oversight of DHS Level 1 investments and conducts portfolio management. As the chair of the IRB, the Deputy Secretary is the Department’s senior acquisition executive. The structure of the board follows:

Chair: Deputy Secretary
Vice Chair: Under Secretary of Management
Membership: Under Secretary, Border and Transportation Security
Under Secretary, Emergency Preparedness and Response
Under Secretary, Science and Technology
Under Secretary, Information Analysis and Infrastructure Protection
Deputy Chief of Staff for Policy
Chief Information Officer (CIO)
Chief Financial Officer (CFO)
Chief Procurement Officer (CPO)
Privacy Officer
General Counsel

The IRB is the forum that provides senior management the proper visibility, oversight, and accountability for Level 1 investments. The primary function of the IRB is to review Level 1 investments for formal entry into the annual budget process and at Key Decision Points (KDP). The IRB conducts systematic reviews of investment preparations and approves key decisions. It also serves as a forum for discussing investment issues and resolving problems requiring senior management attention.

B. **Management Review Council (MRC).**

The MRC is the review authority for DHS Level 2 investments and supports portfolio management. The structure of the council follows:

Membership: CIO
CFO
CPO

The MRC reviews Level 2 investments for formal entry into the annual budget process using Enclosure (3), Exhibit 300 Light (non-IT). Note that for acquisitions already in progress, reviews shall occur prior to award. A one-page request for MRC review shall be submitted in these instances (see Enclosure (4) for sample). If after the MRC meets, no issues are noted within the seven-day period, activities may presume the authority to proceed with the acquisition or award as planned. If issues are identified as a result of this review, appropriate coordination and resolution will take place with the Under Secretary, the Commandant of the Coast Guard, or the Director of the Secret Service, or designee, responsible for the acquisition. The Deputy Secretary will decide any issue that cannot be resolved. For additional guidance on IT only investments, reference the IT Investment Review provided in Enclosure (5).

C. **Joint Requirements Council (JRC).**

The JRC is a senior requirements review board that conducts program reviews to oversee the requirements generation process, validate mission needs statement, review cross-functional needs and requirements, and make programmatic recommendations to the IRB on proposed new programs. Note that the Enterprise Architecture Board (**EAB**) **will provide this function for IT requirements**. The structure of the council follows:

Members: Chief Operating Officers (COO) of Directorates/Organizational Elements
Executive Secretary – Director, Program Analysis and Evaluation (PA&E)

Note: COO representation may not be delegated. Examples of COO include the Chief of Staff of the Coast Guard, Deputy Commissioner for Customs and Border Patrol, and Deputy Administrator, Transportation Security Agency.

The JRC reviews Level 1 investments annually and prior to KDPs and Level 2 investments at the time of submission to validate mission needs and review proposed programs for cross-functional applications, and/or to determine if existing capabilities can meet the need. The JRC makes a recommendation to the IRB or MRC as appropriate for each program.

D. **Enterprise Architecture Board (EAB).**

The EAB reviews and approves Level 3 IT investments. The EAB also reviews and makes recommendations to the IRB and the MRC regarding Level 1 and Level 2 IT

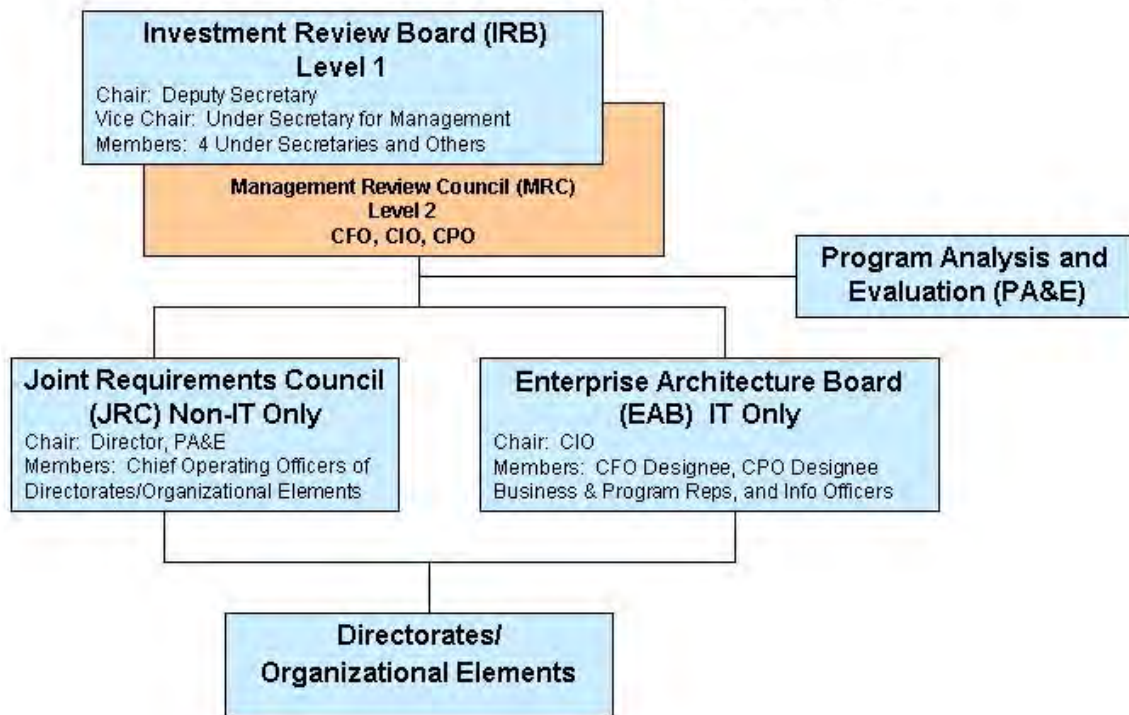
investments. On an annual and ongoing basis, the EAB approves business cases; participates in strategic planning and develops IT strategic guidance; and establishes standing and ad hoc committees as deemed appropriate. The structure of the board follows:

Chair: CIO
 Members: CFO Designee
 CPO Designee
 Business Unit and Program Representatives
 Information Officers, Directorates/Organizational Elements

E. Director, Program Analysis and Evaluation (PA&E).

The Director, PA&E will develop a recommended prioritized list of investments based on portfolio management criteria and scoring criteria similar to the example found in Enclosure (6). Decision support information will be provided to the IRB on Level 1 investments and to the MRC on Level 2 investments.

DHS Investment Review Structure



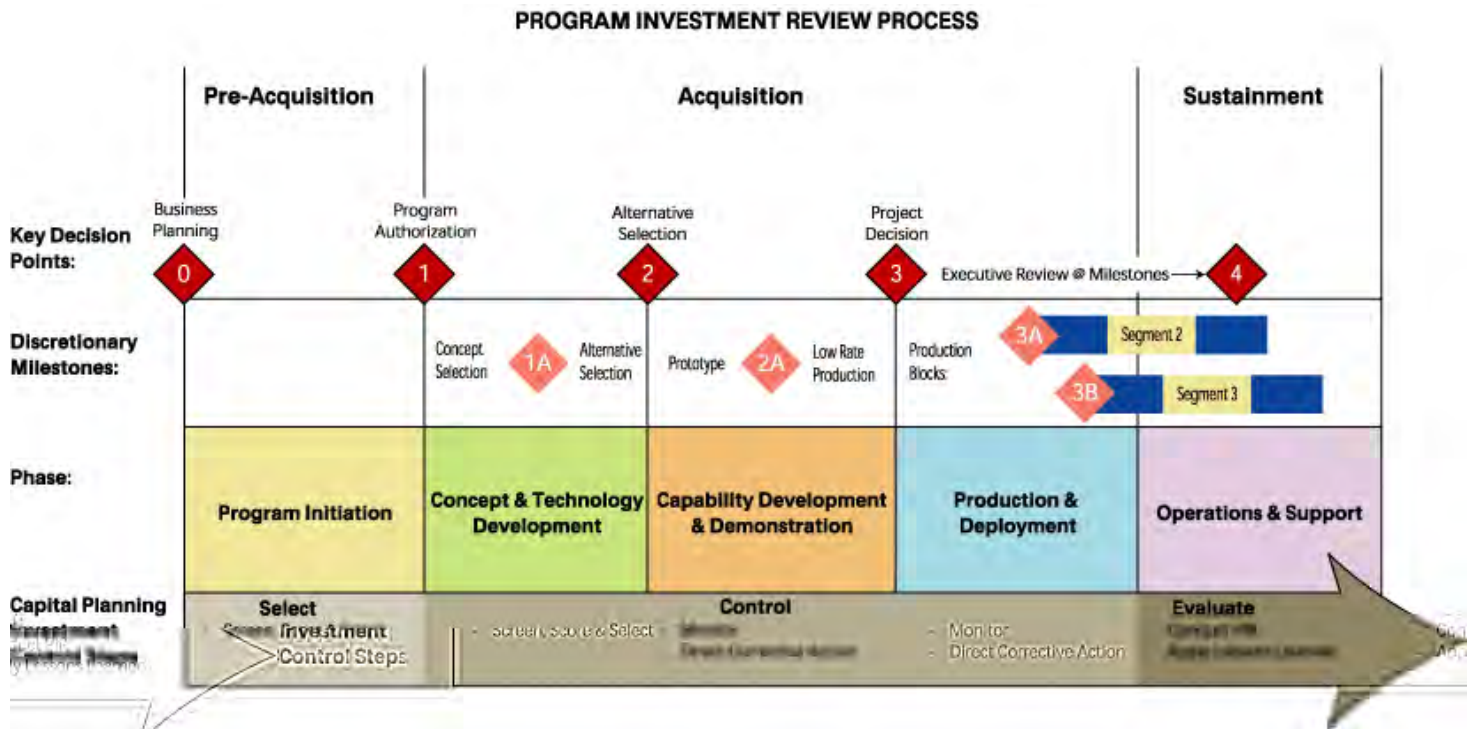
F. Acquisition Phases.

Major investment programs are treated in a systematic manner progressing from pre-acquisition to sustainment. The acquisition process is categorized into the following phases: 1) Program Initiation, 2) Concept and Technology Development, 3) Capability Development and Demonstration, 4) Production and Deployment, and 5) Operations

and Support.

Complex developmental investments require a highly disciplined structure and rigorous acquisition process while less complex investments (e.g., off-the-shelf procurements or service contracts) warrant combining phases and less complex risk management.

After validation by the JRC/EAB, the IRB reviews Level 1 investments at KDPs, which follow each acquisition phase, and are tailored to properly manage the inherent risk of a specific investment. At each KDP review, the program must: (1) review and update, as needed, documents prepared during the previous acquisition phases, (2) demonstrate achievement of activities appropriate to that phase, and (3) satisfy exit criteria approved by the IRB for that phase. IRB approval is mandatory at KDPs for programs to proceed to the next acquisition phase. **Exit Criteria are program specific accomplishments or performance parameters that must be satisfactorily demonstrated before a program can transition to the next acquisition phase, phase segment, or production block.** It should be noted that discretionary KDPs might be required at critical milestones within an acquisition phase when top management decision-making is deemed necessary.



Program Initiation Phase. Programs are responsible for conducting ongoing operational analysis. A capability gap is determined when current or future program/mission requirements exceed existing capability. Program requirements are developed to define the new capability required to satisfy a mission. The key to obtaining resources to proceed is to develop an effective Exhibit 300 Business Case that justifies the need and value of the new investment.

In preparation for KDP1 the Program Manager is responsible for preparing: (1) a Mission Need Statement, (2) the Exhibit 300 Business Case, and (3) proposed Exit Criteria for the Concept & Technology Development Phase. The Program Manager will submit an initial Exhibit 300 Business Case containing or based on items identified above. This information and associated presentations are used to screen, score, and select initiatives.

With approval at KDP1, the initiative is: (1) designated as a Level 1 acquisition, (2) directed to charter a major acquisition Integrated Product Team (IPT), (3) authorized to commence the Concept & Technology Development Phase, and (4) entered into the budget process. Typically the initiative will enter the Fiscal Year (FY)+2 budget to provide staff and funding to proceed.

Concept and Technology Development Phase (CTD). The CTD Phase focuses on setting operational requirements and exploring alternative solutions for meeting mission needs. Typically, competitive, parallel short-term concept studies by the Government and/or industry will be conducted during this phase. The objective of CTD is to define and evaluate the feasibility of alternatives and to provide a basis for assessing the relative merits (e.g., advantages and disadvantages, degree of risk, life cycle cost, cost-benefit, etc.) of alternatives. Alternative solutions are solicited from across industry to achieve the optimal solution, with emphasis placed on innovation and competition. Promising alternative solutions are defined in terms of cost, schedule, and performance objectives; identification of interoperability, supportability, and infrastructure requirements; opportunities for tradeoffs; an overall acquisition strategy; and a test and evaluation strategy (including Development Test and Evaluation (DT&E), and Operational Test and Evaluation (OT&E)).

In preparation for KDP 2 the Program Manager will review and update documents prepared during the previous phase and develop: (1) a Program Plan, (2) a Risk Management Plan, (3) an Acquisition Plan, (4) Operational Requirements, (5) an Alternatives Analysis, including identification of life cycle costs, (6) an Acquisition Program Baseline, and (7) proposed Exit Criteria for the Capability Development and Demonstration Phase. The Program Manager will submit an updated Exhibit 300 containing or based on items identified above. This information and associated presentations are used to monitor initiatives, direct corrective actions, and determine when the investment is ready to proceed to the next phase.

In some cases, a discretionary KDP (KDP 1A) may be required prior to KDP 2. This would typically occur for developmental programs with a range of conceptual solutions. The KDP 1A decision results in the selection of a concept. The format would be similar to KDP 2 less proposed Exit Criteria.

With approval at KDP 2, a preferred acquisition alternative is selected, funds are identified for this phase, and the investment is authorized to commence the Capability Development and Demonstration Phase.

Capability Development and Demonstration Phase (CDD). The CDD Phase is focused on demonstrating feasibility of the preferred alternative and refining the solution prior to a full production commitment. CDD phase activities include developing the first article for the completion of DT&E. OT&E is conducted on production representative units to confirm that the item meets mission needs and operational requirements. Any Low Rate Initial Production (LRIP) units required for OT&E are fabricated during this phase.

In preparation for KDP 3 the Program Manager will review and update documents prepared during previous phases and develop: (1) proposed Exit Criteria for the Production and Deployment Phase. The Program Manager will submit an updated Exhibit 300. This information and associated presentations are used to monitor initiatives, direct corrective actions, and determine when the investment is ready to proceed to the next phase.

A discretionary KDP (KDP 2A) may be required prior to KDP 3. This would typically occur for a LRIP decision for developmental or high integration programs, after Developmental Testing.

With approval at KDP 3, the investment is authorized to commence the Production and Deployment Phase and the future years program plan must be fully funded.

Production and Deployment Phase (P&D). The P&D Phase activities produce systems and equipment for deployment into operational use. The objective of the P&D Phase is to achieve the full operational capability that satisfies the mission need. Asset(s) are produced and deployed in lots or blocks, each of which is a programmatically and economically useful segment. The necessary logistics systems are in place to support the end-items. Each operating unit is readied for unrestricted operations and deployment.

In some cases, a discretionary KDP (KDP 3A) may be required for follow-on block production authorization to implement useful segments.

Operation and Support Phase. The Operation and Support Phase activities include using the asset to perform required missions. Post Implementation Reviews (PIRs) are conducted to assure the asset(s) are meeting performance and cost goals. The operating program continues operational analysis to measure asset performance against department goals.

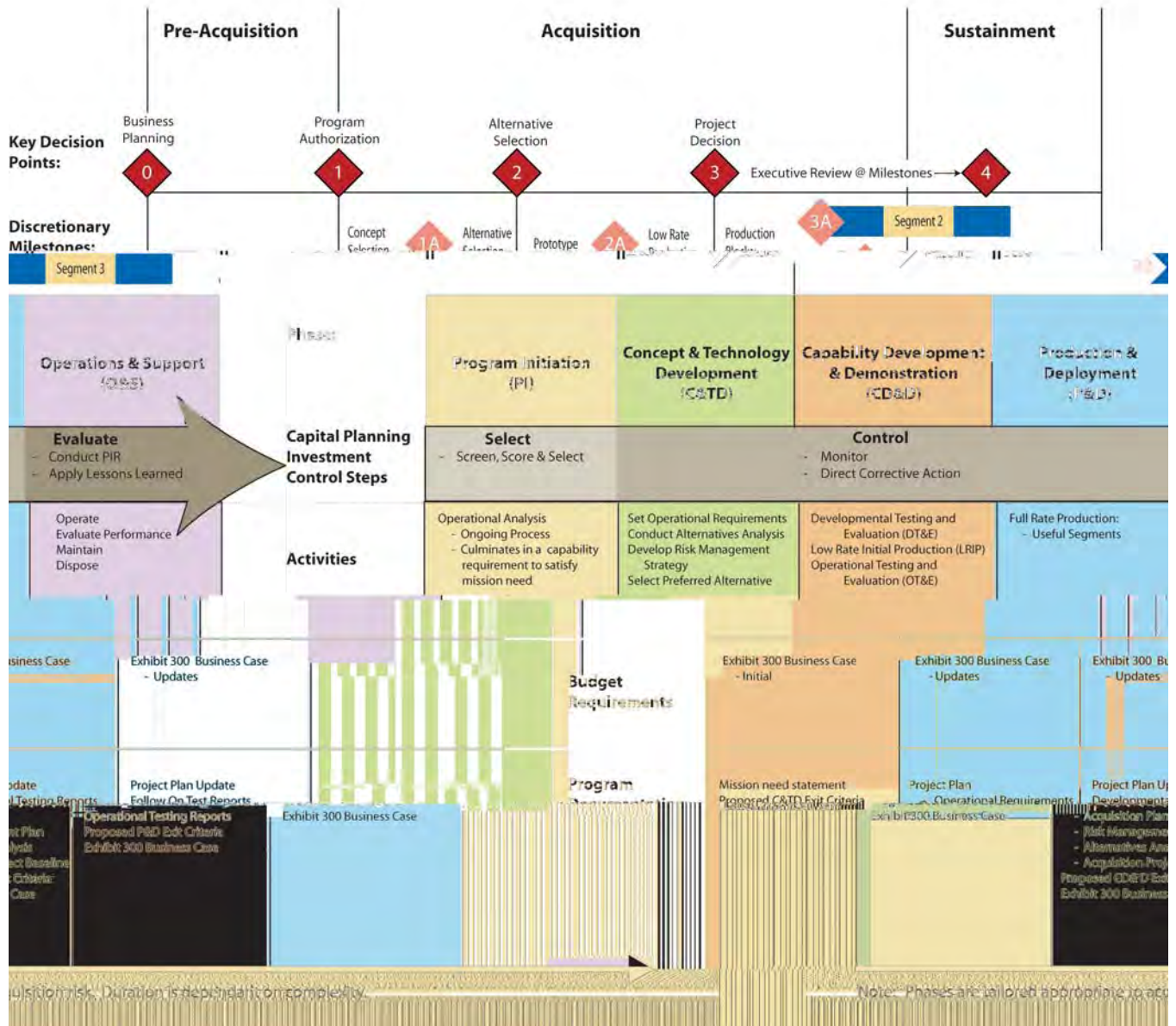
In some cases, KDP 4 is scheduled to conduct a Post Implementation Review (PIR). PIRs may be required annually to monitor effectiveness and continued value of an investment.

Exit Criteria

As described in the example, the Exit Criteria must be directly related to and supplement the objectives, required accomplishments and documents to be produced for the phase, phase segment or useful segment.

Sample Exit Criteria	
Discretionary KDPs	Required KDPs
Discretionary KDP 1A for entry into the Alternative Refinement Phase Segment	KDP 2 for entry into the Development and Prototyping Phase Segment/CDD Phase
<ul style="list-style-type: none"> • Establish IPT • Establish preliminary operational requirements • Completion of alternative analysis • Determine acquisition strategy 	<ul style="list-style-type: none"> • Finalize operational requirements • Demonstrate program affordability • Establish program baseline • Document feasibility and tradeoff analyses (if applicable)
Discretionary KDP 2A for entry into the LRIP Phase Segment	KDP 3 for entry into the Production and Deployment Phase and 1 st useful segment or production block (if applicable)
<ul style="list-style-type: none"> • Completion of Critical Design • Review 	<ul style="list-style-type: none"> • Successful completion of OT&E • Validate production quantity
Discretionary KDP(s) 3A, B, etc. to authorize production of the next useful segment or production block	
<ul style="list-style-type: none"> • Revalidate operational effectiveness and suitability • Revalidate production quantity • Demonstrate affordability of next production block 	

The IRP with associated activities, budget requirements, and required documentation is summarized in the table below.



Program Managers must understand the link between acquisition phase activities and the Exhibit 300 Business Case Evaluation Criteria/Elements. The figures in Enclosure (7) depict the acquisition phase activities that correspond to the evaluation criteria and Exhibit 300 elements.

G. **Portfolio Management,**

The Department must annually 'make the business case' for all Level 1 and 2 investments (IT and non-IT) through budget exhibits to OMB. Exhibits prepared for inclusion in the President's annual budget will go through a rigorous management process. This process begins with Program Managers submitting budget requests based on the Department's annual budget process.

PA&E will adjust and publish programming and planning guidance based on executive level direction, legislation, and triggering events. In turn, the programming and planning guidance will influence annual procedural guidance for submission of the Exhibit 300 Capital Asset Plan and Business Case. The Exhibit 300 will be used for all Level 1 IT and non-IT programs, and for all Level 2 IT programs. I-TIPS will be used to record information for new non-IT investments and all IT investments (see Enclosure (6)).

PA&E will review all submitted Exhibit 300's for structural integrity and compliance, and will distill cross-DHS issues for coordination and prioritization. PA&E will develop the overall DHS investment portfolio, monitoring and tracking the impacts that investment decisions have on individual programs and cross-DHS program capability interdependencies.

The IRB approves Level 1 investments (resolving associated cross-department issues), and approves and submits the DHS investment portfolio with required Exhibit 300 Business Cases to OMB. The MRC approves Level 2 investments and provides investment information to PA&E. Submission of the portfolio and accompanying exhibits are generally due to OMB in the early-September timeframe.

Appendix H: Uncovering Requirements

The following pages include slides on how to start the requirements gathering discussion. It includes useful questions that you may want to consider.

Slide 1

Uncovering Requirements

How to start the conversation...

Tom Cellucci, PhD., MBA
Chief Commercialization Officer
Science and Technology Directorate
thomas.cellucci@dhs.gov

January 2008



1

Slide 2

Discussion Guide

- Requirements versus Specifications
- An Example
- Methods for Uncovering Requirements
- Requirements Development
- Available Resources/Background Materials
- Open Discussion



2

Requirements versus Specifications

- **Requirements** describe an environment—the way it should be—after a product, system or service is integrated (describes the problem)
- **Specifications** are descriptions that are sufficient for building a product or system or providing service (describes the solution)



An Example

(M. Jackson)

- **GOAL: Construction of a *system* with specified characteristics**
 - *Example:* An elevator should enable persons in a building to get from one floor to another
- Components of the system:
 - **Environment:** Part of “real world” relevant for the problem
 - *Example:* Floors, persons, etc.
 - **Machine:** Controlling software and hardware



An Example (continued)

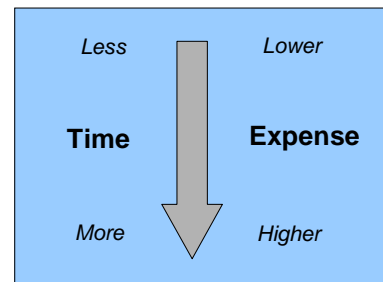
- Properties of the environment are fixed. We have to build the machine so that it realizes the desired properties of the system
- Machine can interact with the environment by:
 - Observing certain phenomena (*input*)
 - Causing certain phenomena (*output*)
- Known:
 - 1. Fixed characteristics of the environment (*domain knowledge*)
 - 2. Desired characteristics of the system (*requirements*)
- Clear: Machine must close the “gap” between 1 and 2
- Searched: **Specifications** for the machine

“How should the machine act so that the system fulfills the requirements?”



Methods for Uncovering Requirements

1. One-on-one interviews
2. Group discussions
3. Delphi focus groups
4. Observation

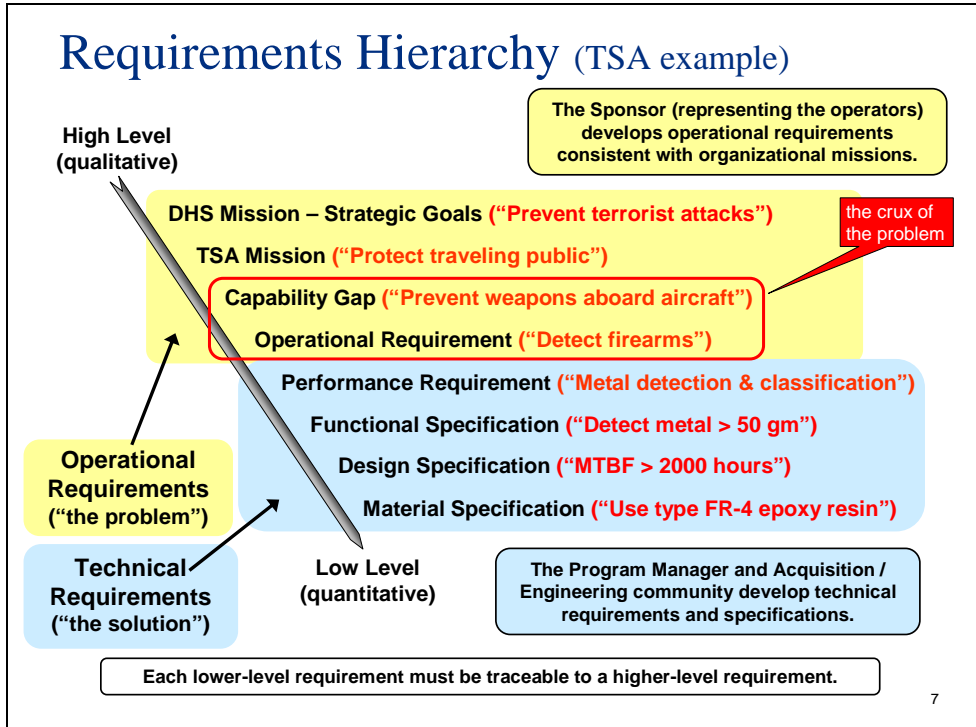


Note: Common Misconceptions:

- The customer is always right
- The potential customer knows what he/she needs/wants
- All customers are equal



Slide 7



Slide 8

Remember to define the problem (not the solution)

- Must be expressed as a needed capability, not a needed product or system
- Usually expressed in broad operational terms

8

How to start ...

- Capability gaps are derived from analysis of threats, vulnerabilities, and consequences
- Operational requirements are derived from talking to operators
 - Include functional requirements (“what the product must do”) as well as operational concepts (“how the product will be used”)

Make sure you're talking with someone who has the authority and knowledge to represent both the end users and those who make buying decisions.

9

Questions to ask a customer (1 of 3)

- **Users**
 - Who are the end users? And who are the “end customers” (those who make buying decisions), who may be neither the end users nor a DHS Agency.
- **Capability Gap**
 - What new capability do the end users need? Do they recognize the need? Can they articulate it? And what new capability do the “end customers” think the end users need?
- **Market Survey**
 - Does the new capability really require a new product or system? What's the existing COTS product which comes closest to meeting the need, and who produces it? And if no product exists, why not? (There may be a good reason why it doesn't exist, and that reason may be a good reason why DHS should not develop it.)
- **Logistics Requirements**
 - How will the product to be developed ultimately find its way to the field and have an impact on operations? Can it be deployed to captive users (e.g., Federal employees) or must it be adopted by independent users (e.g., first responders or shipping companies)? Who will develop the end product (prime contractor, private sector, S&T)? Who will manufacture it? Who will distribute it? How will the end users be trained, and by whom? In short, who will do the logistics planning and support?

This last cluster of questions is grouped because, taken together, these questions address one of the most critical questions that DHS must answer: “What's the channel to the end users?” If there's no feasible channel, then why develop the product?



10

Questions to ask a customer (2 of 3)

- **Functional Requirements**
 - What is the product or system supposed to do? How well does it have to do it? (e.g., for detection systems, what detection probabilities are required, and what false-alarm rates are tolerable?)
- **Operational Concept**
 - What are the most typical use scenarios? What are standard operating procedures? Where will the product or system be used and under what conditions (dirty? cold? hot?). How often? How long?
- **Affordability**
 - How cheap does the product have to be to be affordable? Who will be paying the bill? What's their willingness to pay? How do we know?

The last topic is critical, particularly for the private sector where price (not performance) is king. If the product will be unaffordable, there's no sense in developing it, whatever its capabilities. (And remember that the "end customer," for whom it must be affordable, may be neither the end user nor a DHS component.)



Questions to ask a customer (3 of 3)

- **Other Considerations**
 - Under what conditions will the products be shipped? Stored?
 - Any constraints on product size and weight? Any objectives for these parameters? Does the product have to be portable?
 - How rugged and reliable does the product have to be to be useful?
 - What other products or systems does the product have to interface with, be compatible with, or interoperate with?
 - Are there safety issues? Privacy issues?
- **User Contact**
 - How can we talk to and observe the intended end users in their operational environment?



Selected Questions (continued)

- What are the most typical use scenarios? What are standard operating procedures?
- Where will the products of the system be used?
- Under what conditions will the products be used? (Dirty? Cold? Hot?)
- How often? How long?
- Under what conditions will the products be shipped? Stored?
- How cheap does the product have to be to be affordable? Who will be paying the bill? What's their willingness to pay?
- Any constraints on product size and weight? Any objectives for these parameters? Does the product have to be portable?
- How rugged and reliable does the product have to be to be useful?
- What other products or systems does the product have to interface with, be compatible with, or interoperate with?
- How will the product be maintained in the field? By whom? How will the maintainers get spare parts? What support equipment is required? Do the maintainers need maintenance training? Are any new facilities required?
- Are there safety issues? Privacy issues?
- How can we talk to and observe the intended end users in their operational environment?



TEMPLATE

COMMERCAILIZATION OPERATIONAL REQUIREMENTS DOCUMENT

[Name of System or Product]

**to be developed by the
[Name of Acquisition Program]**

**[Name of Program Manager]
Program Manager, [Name of Acquisition Program]
[Name of PM's Organization]**

**[Name of Sponsor]
Sponsor, [Name of Acquisition Program]
[Name of Sponsor's Organization]**

**[Name of S&T Project Manager]
Project Manager, [Name of S&T Project]
[Name of S&T Division]
Science and Technology Directorate**

**Date
Version X.X**

Contents

1. General Description of Operational Capability	3
1.1. Capability Gap	3
1.2. Overall Mission Area Description.....	3
1.3. Description of the Proposed Product or System.....	3
1.4. Supporting Analysis.....	3
1.5. Mission the Proposed System Will Accomplish	3
1.6. Operational and Support Concept	3
1.6.1. Concept of Operations	3
1.6.2. Support Concept	3
2. Threat.....	3
3. Existing System Shortfalls.....	4
4. Capabilities Required	4
4.1. Operational Performance Parameters	4
4.2. Key Performance Parameters (KPPs)	4
4.3 System Performance.....	4
4.3.1 Mission Scenarios	4
4.3.2 System Performance Parameters	4
4.3.3 Interoperability.....	4
4.3.4 Human Interface Requirements	4
4.3.5 Logistics and Readiness	4
4.3.6 Other System Characteristics	4
5. System Support.....	5
5.1 Maintenance	5
5.2 Supply.....	5
5.3 Support Equipment	5
5.4 Training.....	5
5.5 Transportation and Facilities.....	5
6. Force Structure.....	5
7. Schedule	5
8. System Affordability.....	5
Signatures	6
Appendixes.....	6
Glossary	6

1. General Description of Operational Capability

In this section, summarize the capability gap which the product or system¹ is intended to address, describe the overall mission area, describe the proposed system solution, and provide a summary of any supporting analyses. Additionally, briefly describe the operational and support concepts.

1.1. Capability Gap

Describe the analysis and rationale for acquiring a new product or system, and identify the DHS Component which contains or represents the end users. Also name the Capstone IPT, if any, which identified the capability gap.

1.2. Overall Mission Area Description

Define and describe the overall mission area to which the capability gap pertains, including its users and its scope

1.3. Description of the Proposed Product or System

Describe the proposed product or system. Describe how the product or system will provide the capabilities and functional improvements needed to address the capability gap. Do not describe a specific technology or system solution. Instead, describe a conceptual solution for illustrative purposes.

1.4. Supporting Analysis

Describe the analysis that supports the proposed system. If a formal study was performed, identify the study and briefly provide a summary of results.

1.5. Mission the Proposed System Will Accomplish

Define the missions that the proposed system will be tasked to accomplish.

1.6. Operational and Support Concept

1.6.1. Concept of Operations

Briefly describe the concept of operations for the system. How will the system be used, and what is its organizational setting? It's appropriate to include a graphic which depicts the system and its operation. Also describe the system's interoperability requirements with other systems.

1.6.2. Support Concept

Briefly describe the support concept for the system. How will the system (hardware and software) be maintained? Who will maintain it? How, where, and by whom will spare parts be provisioned? How, where, and by whom will operators be trained?

2. Threat

If the system is intended as a countermeasure to a threat, summarize the threat to be countered and the projected threat environment.

¹ In this document, the terms "product" and "system" are synonymous. The word "system" is used to refer to either.

3. Existing System Shortfalls

Describe why existing systems cannot meet current or projected requirements. Describe what new capabilities are needed to address the gap between current capabilities and required capabilities.

4. Capabilities Required

4.1. Operational Performance Parameters

Identify operational performance parameters (capabilities and characteristics) required for the proposed system. Articulate the requirements in output-oriented and measurable terms. Use Threshold/Objective² format and provide criteria and rationale for each requirement.

4.2. Key Performance Parameters (KPPs)

The KPPs are those attributes or characteristics of a system which are considered critical or essential. Failure to meet a KPP threshold value could be the basis to reject a system solution.

4.3 System Performance.

4.3.1 Mission Scenarios

Describe mission scenarios in terms of mission profiles, employment tactics, and environmental conditions.

4.3.2 System Performance Parameters

Identify system performance parameters. Identify KPPs by placing an asterisk in front of the parameter description.

4.3.3 Interoperability

Identify all requirements for the system to provide data, information, materiel, and services to and accept the same from other systems, and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

4.3.4 Human Interface Requirements

Discuss broad cognitive, physical, and sensory requirements for the operators, maintainers, or support personnel that contribute to, or constrain, total system performance. Provide broad staffing constraints for operators, maintainers, and support personnel.

4.3.5 Logistics and Readiness

Describe the requirements for the system to be supportable and available for operations. Provide performance parameters for availability, reliability, system maintainability, and software maintainability.

4.3.6 Other System Characteristics

Characteristics that tend to be design, cost, and risk drivers.

² The threshold value for a requirement is the minimum acceptable performance. The objective value is the desired performance.

5. System Support

Establish support objectives for initial and full operational capability. Discuss interfacing systems, transportation and facilities, and standardization and interoperability. Describe the support approach including configuration management, repair, scheduled maintenance, support operations, software support, and user support (such as training and help desk).

5.1 Maintenance

Identify the types of maintenance to be performed and who will perform the maintenance. Describe methods for upgrades and technology insertions. Also address post-development software support requirements.

5.2 Supply

Describe the approach to supplying field operators and maintenance technicians with necessary tools, spares, diagnostic equipment, and manuals.

5.3 Support Equipment

Define the standard support equipment to be used by the system. Discuss any need for special test equipment or software development environment

5.4 Training

Describe how the training will ensure that users are certified as capable of operating and using the proposed system.

5.5 Transportation and Facilities

Describe how the system will be transported to the field, identifying any lift constraints. Identify facilities needed for staging and training.

6. Force Structure

Estimate the number of systems or subsystems needed, including spares and training units. Identify organizations and units that will employ the systems being developed and procured, estimating the number of users in each organization or unit.

7. Schedule

To the degree that schedule is a requirement, define target dates for system availability. If a distinction is made between Initial Capability and Full Operational Capability, clarify the difference between the two in terms of system capability and/or numbers of fielded systems.

8. System Affordability

Identify a threshold/objective target price to the user at full-rate production. If price is a KPP, include it in the section on KPPs above.

Signatures

Sponsor's Acquisition Program Manager [print and sign] Date

Sponsor's Representative [print and sign] Date

S&T Project Manager [print and sign] Date

S&T Division Head [print and sign] Date

Appendixes

Glossary

SECURE Program: Concept of Operations



Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
Department of Homeland Security
Science and Technology Directorate
Email: Thomas.Cellucci@dhs.gov



**Homeland
Security**

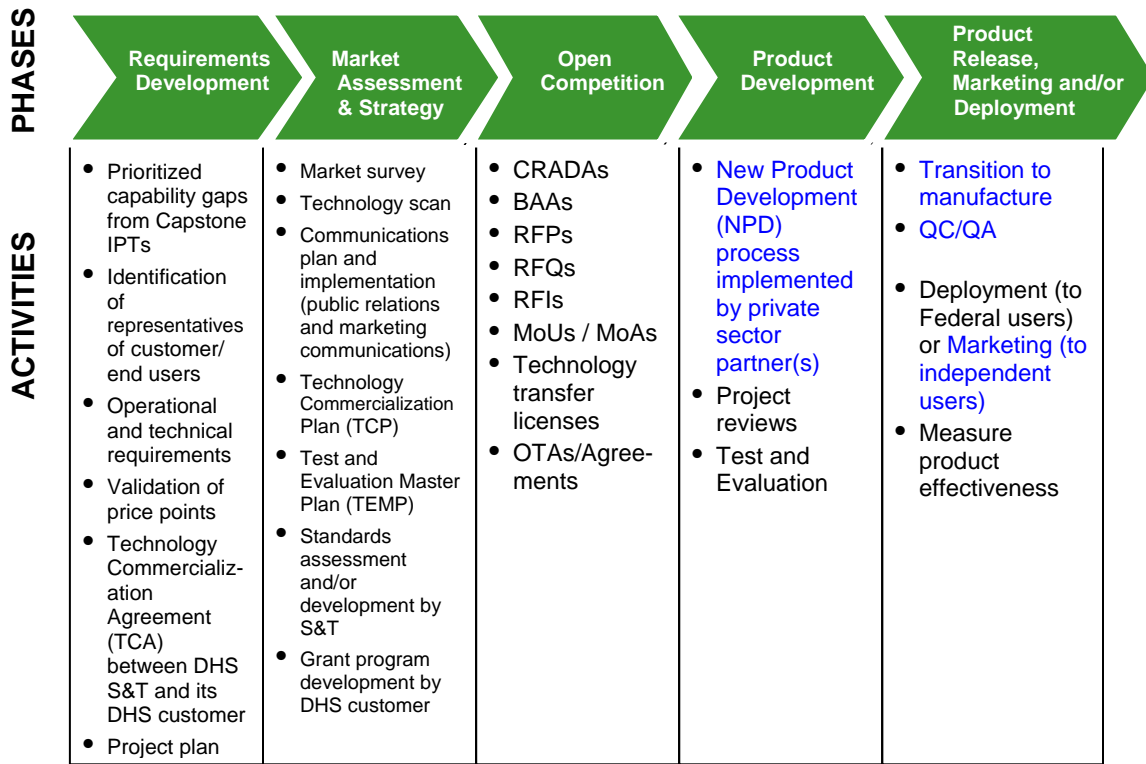
SECURE Program: System Efficacy through Commercialization, Utilization, Relevance and Evaluation

Scope:

We have developed a comprehensive program to enable DHS-S&T to efficiently and cost-effectively leverage the resources, skills, experience and productivity of the Private Sector to develop technologies and products in alignment with specific requirements obtained from DHS Components, the First Responder Community and other End-Users involved in Homeland Security applications.

Overall Process:

Below is a graphical representation of the overall outreach process we have implemented to stimulate and engage the Private Sector to use its resources to rapidly develop technology, products and services that can yield significant benefits for DHS-S&T with a speed-of-execution not typically observed in the Public Sector.



Legend: Black text = Typical Government activities
Blue text = Typical Private-Sector activities

Outreach to the Private Sector



Program Process:

In order to provide DHS Operating Components, the First Responder Community and other End-Users with products that meet their specific requirements, DHS-S&T will provide a vehicle by which Private Sector entities can offer products and/or conduct product development geared specifically toward meeting those needs. Private Sector entities currently possessing a technology/product/system rated at a Technology Readiness Level TRL-5 (i.e. applied or advanced R&D) or above that potentially closes a defined DHS capability gap by addressing detailed operational requirements supplied by DHS-S&T will have the opportunity to continue development of their technology/product/system to TRL-9 (i.e. fully field deployable product) at the expense of the Private Sector entity with the assurance that DHS-S&T will verify their independent third-party test(s) of a given technology/product/system.

Only when TRL-9 is achieved, will Private Sector entities be assured that their testing and evaluation (T&E) of the fully deployable technology/product/system (performed by an independent third-party) is verified by a DHS-S&T assessment of a given third party, independent T&E. DHS-S&T will publish its assessment on the DHS' public website as validation of the success (or failure) to meet the Private Sector entity's own established specifications. This approach enables DHS-S&T to review several highly developed technologies/products/systems in an open and fair manner while successful Private Sector entities will share in the imprimatur of DHS-S&T. DHS Operating Components, the First Responder Community and other End-Users are enabled to make informed purchasing decisions for necessary technologies/products/systems to enhance their capabilities through meeting their detailed requirements. In addition, these solutions are excellent candidates for liability protection under the provisions of the DHS SAFETY Act.



Application:

In the spirit of open and free competition, and in order to capitalize on the free-market system, DHS-S&T intends to publish this program and all ancillary requirements documents/information on the DHS-S&T website. These materials will be accessible by all businesses. Given this information, Private Sector entities may file an application to develop or enhance their technology/product/system in cooperation with DHS-S&T that will improve upon currently fielded DHS technologies. We envision a simple application for this program that can be completed via the internet. The contents of the application will include basic, non-proprietary business information, contact information, alignment to widely available DHS-S&T capability gaps and ancillary requirements documents we choose to offer such as ORDs (Operational Requirement Documents), etc.



Selection:

In order to be fully considered by DHS-S&T for cooperative development:

- The company entity must demonstrate they possess technology at TRL-5 (i.e. applied or advanced R&D) or above and possess the resources to invest in the commercialization of its technology to TRL-9 (i.e. fully field deployable product)
- The company entity must propose a technology/product development effort that has clear and substantial alignment with published DHS-S&T capability gaps and other announced requirements

A DHS selection committee will be established to review applications and monitor the mutually-agreed-upon roles and responsibilities of the partnership. The selection committee will consider these and other DHS proprietary metrics for selection consideration.



Agreement:

The Private Sector entity and DHS-S&T will execute a simple, straightforward and binding agreement whereby the Private Sector entity details milestones with dates and agrees to bear full and total financial responsibility to develop its technology/product/system to a TRL-9 state (if not already at that level). DHS-S&T will publish on the DHS-S&T website the factual findings of such assessment. DHS-S&T has the right to cancel an agreement if the Private Sector entity does not fulfill/achieve any of its milestones by the mutually-agreed-upon dates.



Publication of Results:

It is apparent that the Private Sector highly values DHS-S&T's potential assessment of a given product's independent third-party test and evaluation. DHS-S&T will openly publish these T&E results on the DHS public web portal for review by the DHS Operating Components, First Responder communities and other end users.

SECURE Program: System Efficacy through Commercialization,
Utilization, Relevance and Evaluation

DHS-S&T SECURE Program Application



1. Company Name: _____
2. Address: _____
3. Contact (Title & Contact Information): _____
4. Website: _____
5. Brief Description of Firm: _____

Product/Technology Offered for Productization by Applicant:

Current Technology Readiness Level: _____ **Estimated time to TRL-9:** _____
SAFETY Act QATT Designation Y/N: _____ **D&B D-U-N-S Number:** _____

Product Name: _____

Description of Product, Technology or Technical Capability: _____

Alignment with Homeland Security Operational Requirements Document: _____

Please describe your new product development process(es): _____

Please describe your experience in commercializing products: _____

DHS Use Only: Review: _____ Rating Index: _____

Questions:
Please contact (202) 254-6749 or
SandT_Commercialization@dhs.gov

FutureTECH: Concept of Operations



Thomas A. Cellucci, Ph.D., MBA
Chief Commercialization Officer
U.S. Department of Homeland Security
Science and Technology Directorate
Email: Thomas.Cellucci@dhs.gov

FutureTECH Program

Scope:

We have developed a new program to enable DHS S&T to efficiently and cost-effectively leverage the resources, skills, experience and productivity of the private sector and other non-DHS entities to develop technologies/capabilities in alignment with research/innovation focus areas obtained from DHS S&T. These technologies/capabilities can ultimately be used by DHS, the first responder community, critical infrastructure/key resources (CI/KR) owners/operators and other DHS stakeholders. In essence, FutureTECH provides a "window of visibility" or "preview" of research/innovation focus areas that DHS and its stakeholders believe are essential in future products and services where detailed operational requirements documents (ORDs) can not be fully developed at this time. The program also provides insight into areas where Independent Research and Development (IRAD) monies could be spent by firms possessing funding to address DHS research/innovation focus areas.

Analogous to the popular SECURE Program, FutureTECH is another innovative private-public partnership and outreach program that outlines focus areas for which current technology only exists at earlier stages on the technology readiness scale (TRL 1-6). Technologies developed in alignment to stated focus areas could lead to cost-effective and efficient product development (TRL 7-9) when detailed requirements contained in ORDs are available. Like the SECURE Program, DHS will provide information to the public in an open and free way. The private sector and other non-DHS entities may use their own resources (including IRAD) to develop technologies/capabilities that will be of potential benefit to the DHS mission. Like the SECURE Program, DHS may enter into a simple CRADA (Cooperative Research and Development Agreement) with an organization that shows it has the ability to deliver technology aligned with the research/innovation focus area sought after by DHS.

To state it simply, the SECURE Program focuses on product/service development to create products and services to protect our nation in the shorter term, while FutureTECH will focus on critical research/innovation focus areas at lower TRLs for eventual deployment. Like all of the Commercialization Office's programs, all parties "win" in the FutureTECH Program--the private sector and others by receiving valuable insight into future research/innovation focus areas needed by DHS and its stakeholders. DHS "wins" because it will leverage the valuable skills, experience and resources of the private sector and other non-DHS entities to expedite efficient and cost-effective technology development; the non-DHS entities "win" because they receive valuable information useful for their own strategic plans; and most importantly, all American taxpayers "win" because this innovative partnership yields valuable technologies/capabilities aligned with research/innovation focus areas developed in a more cost-effective and efficient way saving taxpayer money.

Overall Process:

Figure 1 is a graphical representation of the overall outreach process the Commercialization Office continues to implement to stimulate and engage the private sector and other non-DHS entities to use their resources to rapidly develop technology

aligned with research/innovation focus areas that can yield significant benefits for DHS S&T with a speed-of-execution not typically observed in the public sector.

Outreach to the Private Sector

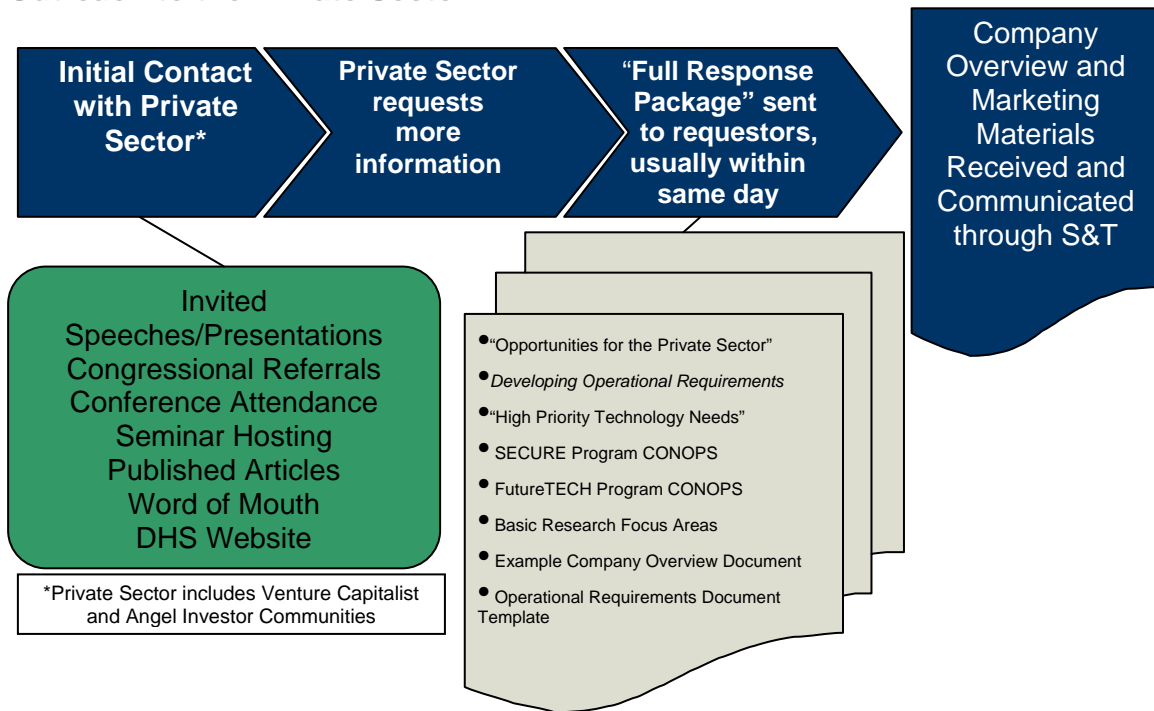
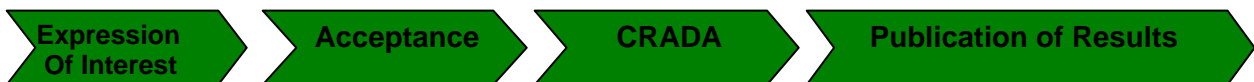


Figure 1: Overview of S&T Directorate Private Sector Outreach Process



Program Process:

DHS S&T will provide this FutureTECH vehicle by which the private sector and other non-DHS entities can identify or develop technology aligned with research/innovation focus areas ranging from TRL-1 through TRL-6 (not fully developed TRL-9 products and/or services) based on DHS S&T's insight and knowledge mainly through its Research and Innovation portfolios/areas.

This approach enables DHS S&T to collaborate on the development of technology aligned with several research/innovation focus areas in an open and free way. The private sector and other non-DHS entities receive information on what new technologies will be required over-the-horizon to protect our nation, removing much of the "guess work" normally associated with predicting future needs.

As with the popular SECURE Program, DHS will review third party, recognized test and evaluation data to ensure that all milestones/objectives of an executed CRADA agreement are met and DHS will place a given research/innovation focus area solution developed by an entity on the FutureTECH website demonstrating that the

research/innovation focus area has met DHS's broadly defined requirements (in contrast to the SECURE Program where products or services must demonstrate compliance to detailed operational requirements contained in an ORD).



Expression of Interest:

In the adherence to fairness of opportunity, and in order to capitalize on the free-market system, DHS S&T intends to publish this program and all ancillary requirements documents/information on the DHS website. These materials will be accessible by ALL. Given this information, the private sector and other non-DHS entities may contact DHS S&T if they are interested in developing or enhancing their technology within a research/innovation focus area in cooperation with DHS S&T. Potential research/innovation focus areas for this program (along with a simple CRADA agreement used in the SECURE Program) are provided on our website. The private sector organization or non-DHS entity must provide DHS S&T with basic, non-proprietary business information, contact information and demonstrate their potential alignment to widely available DHS S&T research/innovation requirements that are more detailed than what are commonly referred to as technology need statements, yet not as detailed as a well-defined ORD.



Acceptance:

In order to be fully considered by DHS S&T for cooperative research/innovation focus area technology development:

- An entity must demonstrate they either possess technology at TRL-1 or higher (i.e. basic research) or possess the ability to develop a technology aligned with the research/innovation focus area to TRL-6 for later technology insertion into a potential acquisition or commercialization program.
- The private sector and other non-DHS entities must propose a research/innovation focus area technology development effort that has clear and substantial alignment with any published DHS S&T requirements delineated above.

A DHS committee will be established to review the private sector and/or non-DHS entities' potential alignment to DHS research/innovation focus areas, and monitor the mutually-agreed-upon roles and responsibilities of partnership participants. The committee will consider these and other DHS proprietary metrics for determining which opportunities to pursue.



CRADA:

The private sector and/or non-DHS entity and DHS S&T could execute a simple, straightforward and binding CRADA whereby the non-DHS entity details milestones with dates and, in most cases, agrees to bear full and total financial responsibility to develop its technology aligned within the research/innovation focus area to a TRL-6 state. Under the Stevenson-Wydler Act (which is the statutory authority enabling DHS to enter into CRADAs), agencies may not contribute funds under a CRADA; however, they may contribute know-how, expertise, materials and equipment. It is important to mention that the execution of a CRADA agreement is at the sole discretion of the corresponding DHS S&T program manager. Additionally, a CRADA with DHS S&T will not necessarily lead to any follow-on contract actions or solicitations by DHS or other government agencies. Any solicitations for funding agreements related to technology areas collaborated upon in a CRADA would be subject to full and open competition. DHS S&T will publish on the DHS S&T website the factual finding(s) of any final assessment. DHS S&T has the right to cancel an agreement if the non-DHS entity does not fulfill/achieve its milestones or performance objectives by the mutually-agreed-upon dates.



Publication of Results:

It is apparent that the private sector and other non-DHS entities highly value DHS S&T's potential assessment of a given technology's recognized third-party test and evaluation (T&E) data. DHS-S&T will openly publish summary findings and an acknowledgement of an entity's attainment of performance objectives on the DHS public web portal for review by the DHS operating components, first responder communities, CI/KR owners/operators and other potential users.