

**COORDINATION OF
HOMELAND SECURITY
SCIENCE AND TECHNOLOGY**



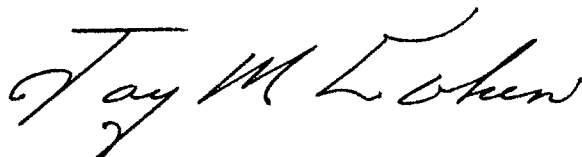
DECEMBER 2007
(REVISED JANUARY 2008)

Foreword

Securing the homeland and preparing for national emergencies is an exceedingly complex mission and requires a focused effort from our entire society if we are to be successful. One primary reason for the establishment of the Department of Homeland Security was to provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure our Nation. Science and technology is a key enabler for many aspects of homeland security and can benefit from similar coordination.

Section 302 of the *Homeland Security Act of 2002* assigns responsibility to the Department of Homeland Security for coordinating the Federal government's civilian research and development efforts for developing countermeasures to chemical, biological, and other emerging terrorist threats. This document, *Coordination of Homeland Security Science and Technology*, is a descriptive baseline for homeland security research and development measures across the Federal government and was developed with the cooperation of the Federal agencies identified herein.

This document lays out the roles and responsibilities of Federal agencies as well as initiatives already under way to counter threats to the homeland. It identifies strategic goals through 2015 and intermediate steps to achieve those goals, and is the first step in developing a more prescriptive plan that will guide the efforts of all participants in the Homeland Security Science and Technology enterprise. Following steps will be concurrent with the Quadrennial Homeland Security Review beginning in 2008 which will play an important role in helping align strategies and missions to adapt to a fast-changing world and an ever evolving enemy.



Jay M. Cohen
Under Secretary for Science and Technology
Department of Homeland Security

ERRATA 1

Revisions Made January 14, 2008

#	Reference	Revision
1.	Foreward	Misspelled. Should be "Foreword"
2.	Chapter 3 – Defense Against Chemical Threats	Numerous corrections necessary resulting in entire chapter being replaced.
3.	Page 99 of the report, the second sentence of the first bullet under the "Communications and Information Management" section.	Change the sentence to read: "SAFECOM, the communications program shared by the Office of Emergency Communications and the Office for Interoperability and Compatibility, is intended to address interoperable wireless communications across all Federal, State, local, and tribal agencies supporting the homeland security mission."
4.	Pg 126 Paragraph 3 under "Strategic Goals for 2015"	Remove "and incrementally increase the" and "to a total of 20 Centers and their consortium members. DHS also will institute a summer faculty study program at the Centers."
5.	Pg 127 Bullet 2 under Mid- and Long- Term Priorities	Change "20" to "10"

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
INTRODUCTION	7
CHAPTER 1: DEFENSE OF HUMANS AGAINST BIOLOGICAL THREAT AGENTS.....	9
INTRODUCTION	9
THREATS AND VULNERABILITIES	9
REQUIREMENTS	9
GAPS	11
STRATEGIC GOALS FOR 2015	12
AGENCIES' ROLES AND RESPONSIBILITIES	17
RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES	19
CHAPTER 2 – DEFENSE OF ANIMALS, PLANTS, AND FOOD AGAINST BIOLOGICAL THREAT AGENTS.....	26
INTRODUCTION	26
THREATS AND VULNERABILITIES	27
REQUIREMENTS	28
GAPS	30
STRATEGIC GOALS FOR 2015	31
AGENCIES' ROLES AND RESPONSIBILITIES	35
RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES	36
CHAPTER 3 – DEFENSE AGAINST CHEMICAL THREATS.....	42
INTRODUCTION	42
THREATS AND VULNERABILITIES	42
REQUIREMENTS	42
GAPS	44
STRATEGIC GOALS FOR 2015	46
AGENCIES' ROLES AND RESPONSIBILITIES	49
RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES	51
CHAPTER 4 – DEFENSE AGAINST EXPLOSIVES AND WEAPONS	57
INTRODUCTION	57
THREATS AND VULNERABILITIES	57
REQUIREMENTS	58
GAPS	58
STRATEGIC GOALS FOR 2015	59
AGENCIES' ROLES AND RESPONSIBILITIES	62
RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES	62
CHAPTER 5 – CRITICAL INFRASTRUCTURE PROTECTION AND CYBER SECURITY	67
INTRODUCTION	67
THREATS AND VULNERABILITIES	67
REQUIREMENTS	68
GAPS	69
STRATEGIC GOALS FOR 2015	69
AGENCIES' ROLES AND RESPONSIBILITIES	74
RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES	75
CHAPTER 6– EMERGENCY PREPAREDNESS AND RESPONSE	82

INTRODUCTION	82
THREATS AND VULNERABILITIES	83
REQUIREMENTS	84
GAPS	85
STRATEGIC GOALS FOR 2015	86
AGENCIES' ROLES AND RESPONSIBILITIES	91
RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES	92
CHAPTER 7 – BORDER AND TRANSPORTATION SECURITY	95
INTRODUCTION	95
THREATS AND VULNERABILITIES	95
REQUIREMENTS	96
GAPS	99
STRATEGIC GOALS FOR 2015	99
AGENCIES' ROLES AND RESPONSIBILITIES	103
RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES	103
CHAPTER 8 – THREAT AND VULNERABILITY ANALYSIS.....	107
INTRODUCTION	107
REQUIREMENTS	107
GAPS	108
STRATEGIC GOALS FOR 2015	108
AGENCIES' ROLES AND RESPONSIBILITIES	112
RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES	113
CHAPTER 9 – SOCIAL, BEHAVIORAL AND ECONOMIC SCIENCES.....	117
INTRODUCTION	117
REQUIREMENTS	117
GAPS	117
STRATEGIC GOALS FOR 2015	118
AGENCIES' ROLES AND RESPONSIBILITIES	120
RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES	121
CHAPTER 10 – FUTURE HOMELAND SECURITY SCIENCE AND TECHNOLOGY WORKFORCE	126
INTRODUCTION	126
THREATS AND VULNERABILITIES	126
GAPS	126
STRATEGIC GOALS FOR 2015	127
AGENCIES' ROLES AND RESPONSIBILITIES	128
RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES	128
APPENDIX	131
ACRONYM LIST	131

EXECUTIVE SUMMARY

“The United States derives much of its strength from its advantage in the realm of science and technology (S&T), and we must continue to use this advantage and encourage innovative research and development to assist in protecting and defending against the range of natural and man-made threats confronting the Homeland.”

-- The National Strategy for Homeland Security, October 2007

The United States has embarked on a systematic national effort to harness its scientific and technological resources to prepare for all-hazards and to achieve its strategic objectives for homeland security:

- Prevent and disrupt terrorist attacks;
- Protect the American people, our critical infrastructure, and key resources;
- Respond to and recover from incidents that do occur; and
- Continue to strengthen the foundation to ensure our long-term success.

Consistent with the Homeland Security Act of 2002 as modified by the Security and Accountability For Every (SAFE) Port Act of 2006 (P.L. 109-347), this document articulates the Department of Homeland Security’s strategic vision for science and technology in support of these objectives, as well as identifying key near- and mid-term priorities that will help achieve that vision. It builds on legislation, National Strategies, and Presidential Directives to show how the Federal government, in coordination with State, local, and tribal governments, as well as industry, academia, the national laboratories, and international partners is addressing the Nation’s homeland security goals.

This document addresses science and technology from the perspective of particular threats to the homeland, as well as broader homeland security-related challenges, including:

- Countering chemical, biological, and explosives threats, including those directed against agriculture, food, and water;
- Enhancing critical infrastructure protection;
- Enhancing national capabilities in all-hazards emergency preparedness, border and transportation security, and threat and vulnerability analysis;
- Fully utilizing the social, behavioral, and economic sciences to counter terrorism and promote resiliency to national emergencies; and
- Continuing to build the workforce of scientists and engineers necessary for future homeland security-related science and technology efforts.

The Federal government evaluates all-hazards threats to the homeland, vulnerabilities of our population and critical infrastructure¹, and gaps in our national capabilities to prevent, protect against, deter, mitigate, and respond to these threats. Although we have certainly made progress, fully realizing the potential of our

¹ The *National Plan for Research and Development in Support of Critical Infrastructure Protection* (Office of Science and Technology Policy and Department of Homeland Security, 2004) defines the nation’s critical infrastructure as consisting of 17 sectors and resources: Agriculture and Food; Water, Public Health and Healthcare; Emergency Services; Defense Industrial Base; Information Technology; Telecommunications; Energy; Transportation Systems; Banking and Finance; Chemical; Postal and Shipping; National Monuments and Icons; Dams; Government Facilities; Commercial Facilities; and Nuclear Reactors, Materials, and Waste.

Nation's scientific and technological advances will require numerous years of unwavering dedication. This document identifies both strategic goals for 2015 and key intermediate steps to achieving those goals, including adapting existing technology for homeland security applications, investing in basic research programs, and fostering education and workforce development. From the perspective of the particular threats and challenges described above, the Nation's goals and priorities include:

Defense against Chemical, Biological, and Explosives Threats

Terrorist use of chemical, biological, and explosive weapons against our population and critical infrastructure poses potentially catastrophic risk to the United States. Preparing for, preventing, and responding to these potential threats is one of the Nation's highest priorities. In support of these efforts, we will:

- Conduct basic and applied research on potential threat agents to inform prioritization of countermeasures research, development, testing, and evaluation (RDT&E);
- Develop end-to-end system architectures to defend against chemical, and biological threats; and
- Develop and deploy tools and approaches to identify potential chemical, biological, and explosive threats, mitigate their consequences, and respond rapidly in the event of an attack.

Critical Infrastructure Protection

Attacks on critical infrastructure could disrupt the direct functioning of key business and government activities, facilities, and systems, as well as have cascading effects throughout the Nation's economy and society. Developing and encouraging the adoption of technology and approaches to protect critical infrastructure, including cyber networks, are essential for the resilience of the Nation from terrorist attacks and natural disasters. In support of these efforts, we will:

- Develop architectures to create a national common operating picture of the Nation's critical infrastructure and key resources;
- Develop and apply advanced risk modeling, simulation, and analysis to determine how best to protect critical infrastructure sectors and key resources;
- Develop secure internet protocols including standard security methods, and information system insider threat detection models and mitigation technologies
- Improve capability to model the effects of cyber attacks and understand internet topography
- Develop technologies and standards for managing identities, rights and authorities used in an organization's networks

All-Hazards Emergency Preparedness

In any disaster, emergency responders are our Nation's front line of defense, saving lives and reducing property damage. Highly trained responders, equipped with the proper tools, planning, and resources, can dramatically reduce the devastating effects of emergencies, ranging from natural disasters to terrorist attacks. Developing and deploying enabling tools and technologies will strengthen our Nation's emergency preparedness and response capabilities. In support of these efforts, we will:

- Enhance modeling- and simulation-based training and exercises to plan for, mitigate the effects of, respond to, and recover from catastrophic events;
- Develop advanced protective equipment and tools to shield responders from the effects of chemical, biological, and radiological agents, as well as blast and incendiary effects; and

- Develop open architecture methods for nationwide command, control, interoperable communications, and intelligence.

Border and Transportation Security

Protecting the United State's borders and transportation networks is vital to our Nation's security. A top priority is to prevent the entry of terrorists and the instruments of terrorism into the United States, while simultaneously ensuring the efficient flow of lawful traffic and commerce. The development of new and enhanced technologies is a key to strengthening the Nation's border and transportation security infrastructure. In support of these efforts, we will:

- Develop integrated networks and improved screening, identification, and sensing tools to detect and prevent threats to the Nation's border and transportation system;
- Create systems and processes to provide integrated situational awareness and communications that will enhance apprehension, detection, seizure and removal capabilities; and
- Develop or adapt defensive technologies and methods to protect civilian ships, trains, and aircraft against terrorist threats.

Threat and Vulnerability Analysis and the Social, Behavioral and Economic Sciences

Fully understanding the threats our Nation faces, as well as identifying those individuals and groups who may perpetrate acts of harm against the United States are essential components of securing the homeland. By building this understanding, threat and vulnerability analysis (TVA) and the social, behavioral and economic (SBE) sciences can help the Nation better predict, prevent, prepare for, and respond to terrorist attacks. In support of these efforts, we will:

- Develop tools, technologies and methods to recognize threats and identify effective countermeasures;
- Enhance the understanding of the behaviors of both terrorists and their targets; and
- Provide guidance in remediation, restoration, and resiliency of those communities and areas affected by an attack or catastrophic event.

Building the Future Homeland Security Science and Technology Workforce

A multidisciplinary and dedicated workforce is necessary to accomplish the monumental tasks facing the Nation. Nurturing, recruiting, retaining, and encouraging ongoing professional development of the best and brightest personnel who possess the technical breadth necessary to anticipate and address present and future threats is the foundation that supports all efforts to defend the homeland. In support of these efforts, we will:

- Sustain university-based centers of excellence for homeland security;
- Support the education of scientists and engineers who are pursuing degrees relevant to homeland security; and
- Invest in targeted recruitment, training, and retention efforts to address shortages of expertise in mission-critical homeland security areas.

Future Coordination

This document establishes a baseline reflecting the roles and initiatives of the various homeland security contributors. A process for regular updates and reporting the nation's progress in meeting its goals will be developed in conjunction with the Quadrennial Homeland Security Review beginning in 2008. The components of the formal updating and reporting process will include:

- The strategic goals articulated must remain consistent with changes in legislation, national goals, and new strategies and directives. Threats need to be assessed, capabilities evaluated, and gaps identified on a regular basis. The Quadrennial Homeland Security Review (QHSR), reflecting these elements, will be a significant driver to this update. Thus, the update will be timed to coincide with the outcome of the first QHSR.
- Future updates will be timed to contribute to Federal agency decision making on their science and technology initiatives. It will be tied to the Federal budget cycle for the year in which it is published.
- Future updates include an annual update on the progress against performance measures established for each of the priorities outlined above and for the key research and development needs discussed in the Plan. These measures will be developed by the end of 2008 to provide guidance for the first QHSR, with the initial performance report coming with the 2009 QHSR. The results from the performance reviews will be used as guidance for the Nation's homeland security partners and be reported in future updates to the Plan.
- Future updates will leverage well-established homeland security reporting processes developed by the Office of Science and Technology Policy (OSTP) and the National Science and Technology Council (NSTC).

Together, the entire Nation is working to secure the homeland and to prepare for national emergencies. As in times past, we are bringing together scientific and technological capabilities from all levels of government, the private sector, academia, and the national laboratories to focus on a critical national mission. Advances in science and technology afford the unique opportunity to protect our population, economy, and way of life from terrorists and natural threats while at the same time maintaining our civil liberties and commerce. This document articulates our vision for RDT&E in support of homeland security and outlines the specific priorities, goals, and objectives that can help make this vision a reality.

INTRODUCTION

“By promoting the evolution of current technologies and fielding new, revolutionary capabilities, S&T will remain an essential and enduring enabler of our Strategy.”

– The National Strategy for Homeland Security, October 2007

The Federal government is making a significant effort to harness its technical superiority in science and technology to ensure a secure homeland. Science and technology is being utilized to support all missions in homeland security, from countermeasures to threats posed by weapons of mass destruction to promoting preparedness and resiliency to natural disasters.

Guided by the *Homeland Security Act of 2002*, the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002*, the *Agricultural Bioterrorism Protection Act of 2002*, the *Project BioShield Act of 2004*, the *National Strategy for Homeland Security*, and Homeland Security Presidential Directives (HSPDs), this document articulates strategic goals to bridge the gaps between our Nation’s existing resources and those needed to counter the risks we face, identifies Federal agencies that conduct homeland security research and development, and establishes a baseline of existing Federal homeland security research and development efforts.

This baseline will enable the Federal government and the Nation to identify specific goals and targets for homeland security research, development, testing, and evaluation (RDT&E) and further establish synchronized approaches to address them. It will be used to provide an overarching strategy for addressing the science and technology needs for homeland security that have been identified through extensive interagency coordination in response to statutory and policy guidance, as well as national plans and strategies for securing our Nation that include but are not limited to:

- *The National Strategy for Combating Terrorism;*
- *The National Strategy for Homeland Security;*
- *The Strategy for Homeland Defense and Civil Support;*
- *The National Response Plan;*
- *The National Infrastructure Protection Plan;*
- *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets;*
- *The National Plan for Research and Development in Support of Critical Infrastructure Protection;*
- *The Federal Plan for Cyber Security and Information Assurance Research and Development;*
- *The National Strategy to Combat Weapons of Mass Destruction;*
- *The National Strategy to Secure Cyberspace;*
- *The National Pandemic Response Plan;*
- *The Biological Defense Strategy;*
- *The National Biological Integrated Surveillance System;*
- *The National Agricultural Security Plan; and*
- *The National Improvised Explosive Device (IED) Strategy.*

HOMELAND SECURITY RESEARCH, DEVELOPMENT, TESTING, AND EVALUATION

Homeland security science and technology is a wide-ranging enterprise that touches on all aspects of securing our Nation. Research, development, testing, and evaluation (RDT&E) is being conducted across a broad range of scientific disciplines to counter specific threats of chemical, biological, and explosives threats, reduce vulnerability of critical infrastructure, and improve our capabilities to respond all-hazards emergencies. The Nation is also developing technology and tools to support specific operational missions, such as border and transportation security, and is addressing key supporting capabilities, such as bolstering

our ability to identify threats and vulnerabilities, establishing standards for procedures, technology, and tools, and providing for education and training.

Research, development, testing, and evaluation represent the four major phases of bringing new technologies, techniques, tools, and integrated systems from conceptual stages to real-world application. This is a long-term process and must be sustained at each stage. In the near term, rapid progress can be made by leveraging existing science and technology solutions across the Federal government. For the longer term, the Federal government is investing in the facilities, basic research programs, and science and technology education required ensuring that we will have the knowledge, resources, and workforce in place to facilitate future progress.

CONTENT OVERVIEW

This document establishes the baseline for the efforts of the entire Federal government homeland security research and development community. Science and technology for homeland security includes a broad range of disciplines and priorities, so it is organized into chapters that focus on specific research initiatives in priority homeland security areas.

These include:

- Defense of Humans Against Biological Threat Agents
- Defense of Animals, Plants, and Food Against Biological Threat Agents
- Defense Against Chemical Threats
- Defense Against Explosives and Weapons
- Critical Infrastructure Protection
- Emergency Preparedness and Response
- Border and Transportation Security
- Threat and Vulnerability Analysis
- Social, Behavioral, and Economic Sciences
- Workforce Development

Chapters then look at the *threats and vulnerabilities* specific to each research area, the scientific and technological *requirements* for addressing these threats and vulnerabilities, and the *gaps* between existing resources and those requirements. Based on this analysis, the largest section of each chapter provides an overview of the near-, mid-, and long-term strategic goals determined necessary to bolster our Nation's defenses against terrorism and prepare for all-hazards emergencies. Together, these components lay out a path for RDT&E activities through 2015.

Achieving these national goals and priorities for homeland security science and technology will require continued cooperation among Federal departments and agencies. Recognizing the tremendous scope of homeland security science and technology, and building on the expertise and resources of traditional mission area lead agencies, each chapter then summarizes the roles and responsibilities of Federal departments and agencies in the coordinated national effort to secure the homeland.

Each chapter ends with a review of the recent accomplishments and ongoing work of Federal agencies and their private and public sector partners within these areas. This provides a baseline of the Nation's RDT&E programs that will help us to formulate better approaches to continue advancement in homeland security science and technology.

CHAPTER I: DEFENSE OF HUMANS AGAINST BIOLOGICAL THREAT AGENTS

INTRODUCTION

Potential acts of biowarfare and bioterrorism constitute major threats to our Nation's military and to its civilian population, agriculture, food supply, and infrastructure. Even small amounts of biological agents such as bacteria, viruses, or toxins can cause large numbers of casualties, costly economic ramifications, and major societal disruption. As articulated in the President's *Biodefense for the 21st Century*, the key to defending against such attacks is an integrated, multilayer defense built upon four essential pillars: Threat Awareness; Prevention and Protection; Surveillance and Detection; and Response and Recovery.

This chapter outlines specific research, development, testing, and evaluation (RDT&E) efforts within each of these pillars, as well as identifies applicable cross-cutting needs and basic research. This strategy does not detract from, but rather complements and relies upon, a parallel sustained research and development effort focused on naturally occurring infectious diseases that can provide critical discoveries, tools, and workforce training to support the national biodefense strategy. Most importantly, this national strategy recognizes that continued involvement, support, and guidance from the medical, scientific, public health, and engineering communities, public and private organizations, and our Nation's people and their representatives will be critical in the ultimate success in defending the U.S. from biological threat agents.

THREATS AND VULNERABILITIES

The anthrax attacks of 2001 demonstrated that our Nation faces the threat of, and is vulnerable to, biological attack. While the threat level remains difficult to assess, some conclusions can be drawn from our knowledge of past biological weapons programs and our understanding of biotechnological advances.

Several nations are known to have maintained robust biological weapons programs in the recent past. At the sub-state level, terrorist groups have expressed interest in using biological agents to attack the United States. Meanwhile, advances in biotechnology are gradually making basic biological agents capabilities available to experienced individuals or groups, a potentially serious problem for the long term. Further adding to the proliferation of biological threat capabilities is that modern biology research and biotechnology are global enterprises, so the expertise and knowledge needed to create modified or novel organisms are becoming ever more widespread.

Aspects of biological research have inherent dual use potential, so the same knowledge and research needed to develop countermeasures to naturally occurring infectious diseases and to biological agents of concern – such as an increased understanding of how pathogens cause disease – can also be used to make pathogens more deadly. In addition to traditional biological threats that arise from agents that may be found in nature, enhanced agents that have been modified to defeat current and emerging countermeasures, agents such as antibiotic-resistant bacteria, could be feasible in the near future. While basic research advances in immunology, physiology, and neurobiology promise humanity a wide range of medical benefits, they also provide knowledge necessary to develop still more advanced agents – such as novel toxins, live agents, and bioregulators – that are not found in nature and are specifically designed to attack or disrupt targeted biological systems and pathways.

REQUIREMENTS

To provide an effective defense against current and emerging biological threat agents, short- and long-term biodefense capability goals that encompass the full breadth of medical and non-medical countermeasures must be established and then implemented. This defense must address not only classical human biological threat agents but should also be flexible enough to evolve to meet changes in the threat brought on by rapid and widely accessible advances in biological science and technology.

To address these goals, which are based on the President's *Biodefense for the 21st Century*, the *Medical Countermeasures against Weapons of Mass Destruction*, and the work of interagency committees such as

the joint National Security Council (NSC) - Homeland Security Council (HSC) Biodefense Policy Coordinating Committee (PCC), the following are key research and development needs:

- ***Threat Awareness*** – Methods, scientific analyses, and information analysis tools are needed to support intelligence activities to identify and characterize potential biological threats; monitor for and understand the potential impacts of emerging infectious diseases; and to identify scientific trends that might enable development of next-generation biological agents. Threat scenarios, end-to-end systems studies, and risk assessments are required to guide countermeasure development and acquisition strategies and the development of integrated system defenses. These efforts require intelligence-informed science-based risk assessments: analyses of motivations, intents, triggers, and preferred modalities for attack; scientific characterization of threat agents; and analyses of existing defenses, vulnerabilities, countermeasure efficacies and attack consequences.
- ***Prevention and Protection*** – Science and technology support of multilateral nonproliferation initiatives are needed to limit the spread of agents, technology, and expertise to countries, groups, or individuals seeking to develop, produce, and use biological agents. These “prevention” activities must be complemented by “protection” activities such as assessing and reducing vulnerabilities in our critical infrastructures, particularly the medical, public health, food, water, energy, agricultural, and transportation sectors.
- ***Surveillance and Detection*** – Methods, architectures, and technologies for an integrated and comprehensive attack warning and characterization system are needed to enable rapid initiation and guidance of robust responses in order to minimize loss of life, economic losses, and societal disruption. Environmental monitoring systems, medical surveillance systems, incident characterization tools, such as meteorological and epidemiological modeling, a national network of analytical laboratories, and the technical expertise and tools to integrate these into a comprehensive picture are all required to meet this capability. Technical forensics analysis and interpretation methods and technologies are required to support apprehension of perpetrators and to contribute to deterrence.
- ***Response and Recovery*** – Concepts of operation, architectures, and technologies are needed to respond rapidly to a biological attack so as to reduce its consequences dramatically. Appropriate medical countermeasures that are available for use by all segments of the general population need to be developed, approved, and stockpiled. These include vaccines, post exposure prophylaxis, therapeutics, and medical diagnostics. Applied public health research is required to enable and strengthen public health response and recovery activities. This includes research to improve the effectiveness of SNS distribution and mass casualty treatment plans and approaches, isolation and quarantine activities, medical care surge capacity, and risk communication strategies that maximize effective behaviors and minimize panic. Systems approaches to decontamination, including their associated concepts of operations, protocols, standards, and tools, are needed to enable timely and cost-effective clean-up of potentially extensive outdoor areas as well as facilities and personnel. Decision support tools are required to inform policy decisions about biodefense options and to help guide incident response. Simulation tools and other training aids are needed to support the exercises and drills critical to developing an effective response capability.

In addition to these biodefense pillar-specific requirements, there are important cross-cutting requirements for homeland security research and development:

- ***Interagency Coordination*** – Federal government coordination is required for determining and developing biodefense science and technology requirements and standards, setting priorities, establishing management and budget plans that accommodate the entire product development cycle from discovery to acquisition, and for generating the necessary product development tools such as animal models. To support this Federal government coordination, threat scenarios, end-to-end systems studies, and risk assessments are required to inform countermeasure development and acquisition strategies and the development of

integrated system defenses. These efforts require science-based threat assessments, scientific characterization of threat agents, modeling to inform medical and public health consequence assessments, scientific assessments of existing defenses and medical countermeasure gaps, and analyses of motivations, intents, triggers, and preferred modalities for biological attack.

- **Basic Research** – Basic science information is the single most important commodity needed for the development of future countermeasures to biological agents. This includes a broad-based understanding of known biological agents, naturally occurring infectious diseases, immune responses, and host-pathogen interaction. A strong and sustained basic research effort, including an integrated national research agenda in the biological, medical, and physical sciences is required across all responsible entities within the Federal government in order to drive the medical, scientific, and, technological advances needed to meet our long-term biodefense needs. Such research will benefit both biodefense and general health and security.

GAPS

There are already significant activities across the Federal government in support of the above research and development needs, especially for defending against traditional agents. Based on the experience to date and the various assessments of these activities, the following additional high priority gaps were identified:

- **Need for a Concerted Effort to Address Enhanced and Advanced Threats:** A systematic approach to understand and defend against modified, evolved, or engineered biological agents is needed. To maximize early warning and characterization, this effort should include improved environmental detection systems that can detect enhanced and advanced agents, characterization technologies that can speed the identification of antibiotic-resistant and countermeasure susceptibility, and rapid sequencing devices that can characterize these agents. Recognizing the impracticality of predicting which of the broad range of possible future threats the Nation will actually have to contend with, the President’s *Medical Countermeasures against Weapons of Mass Destruction*, calls for flexible broad spectrum medical countermeasures that would address classes of agents rather than just an individual agent. Furthermore these broad spectrum countermeasures would be developed using platform technologies that allow one to very rapidly develop new countermeasures countermeasure should the need arise. This approach includes, but is not limited to, the “identification and use of early markers for exposure, greater understanding of host response to target therapeutics, and development of integrated technologies for rapid production of new countermeasures.” Many of the technologies developed through this effort would also have significant public health benefits through their application to naturally occurring infectious diseases.
- **Need for a More Robust Pipeline for Medical Countermeasure Development:** While the early implementation of Project BioShield has taken significant steps in bringing new countermeasures to bear on such high priority threats as anthrax, smallpox, botulinum toxin and radiological-nuclear effects, it has also revealed some of the challenges in rapidly developing new medical countermeasures. Better integration and communication of U.S. national requirements (civilian) that drive well-funded translational research and development of medical countermeasures is needed. While the U.S. government holds substantial research assets and funds high-quality, productive basic science research, the capabilities to produce large-scale, clinical-grade countermeasures reside within the private sector. A more clearly defined and integrated process to develop countermeasures from early research through advanced product development to acquisition, including approaches and incentives to increase Federal government and private sector partnering, is needed. These process improvements are now underway as a result of passage of the Pandemic and All Hazards Preparedness Act and the development of the Public Health Emergency Medical Countermeasure Enterprise Strategy and Implementation Plan for CBRN Threats. Their continued development,

sufficient funding, and implementation are critical to developing the additional medical countermeasures – including new classes of antibiotics, antivirals and rapid medical diagnostics – needed to address the full range of current and future Material Threats.

- ***Need for Improved Research and Development Methods:*** The HHS report *Innovation/Stagnation: Challenge and Opportunity on the Critical Path to New Medical Products* emphasizes the need for new product development tools, such as animal models (including non-human primates), vaccine platform technologies and safety evaluation methods, and biomarkers of infection and immunity.
- ***Need to Develop Timely and Affordable Decontamination Frameworks, Protocols, and Technologies for Large Outdoor Areas and Their Associated Facilities:*** Some biological attacks have the potential to contaminate large portions of a metropolitan area, displacing people and shutting down critical infrastructure. Current standards, protocols, and technologies are such that decontamination of a single building, such as the Brentwood Post Office, is a major undertaking. The Nation currently lacks and urgently needs protocols, systems, technologies, and standards for addressing such an event if it should occur tomorrow, in three years, or in five-to-ten years. These new protocols, systems, and technologies need to be less expensive, easy to deploy quickly and use, less damaging to materials, less toxic to response personnel, and tested for their intended applications prior to emergency use. The Nation also needs political and social science research to help set acceptable clean-up standards in response to a major event and to communicate those standards most effectively.
- ***Need to Address Critical Knowledge Gaps in the Environmental Microbiology Underlying Risk Assessments:*** Currently there are extremely limited data on infectivity, morbidity, and mortality as a function of dose for various biological agents, as determined through respiratory and oral routes of entry. This knowledge is critical for conducting threat assessments, modeling attack consequences, developing detection and protection systems, and driving decisions on the priority of the threat and requirements for medical countermeasures. Similarly, there is a lack of data on the fate of these agents in the environment, such as their viability as a function of time after release. Such data are critical to providing realistic estimates of short- and long-term exposure levels and to underpinning decontamination and recovery.
- ***Need to Address Critical Facility Infrastructure Requirements to Ensure Federal Research and Partnerships with Private Industry and Academia are Secured:*** DoD is committed to expanding and recapitalizing the U.S. Army Medical Research Institute for infectious diseases (USAMRIID) in order to ensure available laboratory space for varying levels of biological research. USAMRIID will be part of the National Interagency Biodefense Campus, currently under construction at Ft. Detrick, MD. This is an interagency effort comprising DoD, DHS, HHS, and USDA.

STRATEGIC GOALS FOR 2015

By 2015, the goal is to take advantage of advances in life sciences, biotechnology, physical, and information sciences to have robust biodefense architecture against known biological agents and the flexibility and responsiveness to address an evolving threat that makes use of the rapid, widely accessible advances in biotechnology. Key capabilities include:

- ***Threat Awareness*** – A fully integrated biological risk assessment infrastructure (combining technical and intelligence-based threat, vulnerability, and consequence assessment capabilities) will be in place. This will enable effective biodefense planning by providing a thorough understanding of current threats and effective anticipation of future threats. Underlying this will be critical data on agent properties that significantly affect the risk assessments, such as dose-response data for inhalation and ingestion of the top priority threat agents, a scientifically defensible way for extending these data to provide guidelines for chronic exposure levels and to guide decontamination guidelines, and agent-fate data

(e.g., viability vs. time) for a variety of indoor and outdoor environments, various food matrices and processing conditions, and in water distribution systems. A strategy for identifying and prioritizing future threats and an active technology watch across the intelligence, open-source, and commercial sectors for scientific trends and indicators related to future threats will be in place.

- **Prevention and Protection** – Tools and methodologies will be in place to aid in the identification, detection, and monitoring of biological agents, to help secure and control access to and transfer of “select” biological agents that could be used for bioterrorism applications and to identify and minimize the dissemination of critical bioweapons expertise and technology. Appropriate protection will be afforded to critical infrastructures through a mix of passive and active protective measures including improved physical security, personnel security, design and operation of facilities, and, where appropriate, biological detection systems.
- **Surveillance and Detection** – An integrated and comprehensive national biosurveillance system will be in place to enable early warning and characterization of attacks using conventional or enhanced biological agents to enable rapid initiation and guidance of robust responses. This system will combine the elements of near real-time monitoring of air, water, and critical infrastructures with medical surveillance and incident characterization tools. An integrated consortium of national analytical laboratories will provide both the capability (e.g., standards, protocols, training, and quality control) and capacity for both routine and surge characterization of environmental, clinical, and food samples. This will include the ability to characterize enhanced and advanced agents rapidly (e.g. sequence, morphology, infectivity, transmission efficiency, and persistence) and to perform rapid screening for drug susceptibility. New diagnostic capabilities will be available that enable pre-symptomatic detection of possible exposure to allow more and earlier targeted treatment of the at-risk population and provide additional assurance to those who are not at risk. Well-established biodetection standards, tests, and validation procedures will also be in place, and suitable detection equipment will be available at the Federal, State, local, and tribal levels. The National Bioforensics Analysis Center (NBFAC) and its associated laboratories will be fully operational, with a full complement of validated protocols and tools for the biological, physical, and chemical analysis of suspect samples and the associated reference libraries of comparison samples for rapid performance of technical forensics analysis on traditional, enhanced and advanced agents.
- **Response and Recovery** – Robust medical and decontamination response capabilities for attacks with traditional agents and a basic response capability for enhanced agents will be in place. A broad range of medical countermeasures (e.g., vaccines, diagnostics, and drugs) for the top threat agents will have been developed and stockpiled, including approaches to agents engineered to be antimicrobial resistant. Concepts of operations will be in place and will have been tested for the rapid characterization of modified or unknown threats and for determining the best available medical countermeasures for addressing them. A strong government-industry partnership, and its associated management and coordination structure, will be in place to move new medical countermeasures smoothly and rapidly from research to early and advanced development to acquisition. Incident characterization tools will combine information on environmental monitoring, plume and epidemiological modeling, medical surveillance, and early medical diagnostics to provide the best possible estimates of the exposed population and area. Approaches, protocols, standards, and technologies will be in place for the timely and cost-effective decontamination of large outdoor areas and their associated facilities and personnel.
- **Basic Research** – Basic research in the life sciences, disease generation (pathogenesis) and human response, medical countermeasures, diagnostics, detection systems, and information technology will all be essential to stay ahead of evolving future threats. A “Grand Challenge” that will be of special importance is: Developing broad-spectrum countermeasures that can address families of threats consisting of multiple agents rather than the current “one bug, one drug” approach. Possible approaches to broad-spectrum

countermeasures include anti-infective therapies, broad-spectrum antimicrobial and antiviral drugs, and immunomodulatory therapies

- **Applied Research** – Dramatically accelerating the bug-to-drug pipeline is another “Grand Challenge” that will be of special importance. Accelerate the time frame for the identification of candidate drug targets to the approval of medical countermeasures from the current 10- years to months. An accelerated pipeline requires real-time detection and diagnostic systems that are able to recognize and characterize biological threat agents rapidly and new platform technologies for rapid drug discovery, development, and production. Streamlined development and regulatory procedures that ensure medical countermeasure safety and efficacy and that resolve legal concerns are required, as are mechanisms such as public-private partnerships and consortium arrangements that allow the full and cooperative engagement of government and industry in the management and oversight of product discovery, development, licensure, and production activities.

Achieving these goals requires basic research to develop a comprehensive understanding of common pathogenic mechanisms, microbial evolution, the evolution of virulence and antimicrobial resistance, and host-pathogen co-evolution. Particularly when dealing with engineered threats, achieving these goals will also require developing comprehensive and predictive systems models of critical immunological, physiological, and neurological pathways and responses.

Beyond its benefits for biodefense, success in meeting the Grand Challenges will likely generate tremendous advances in our ability to reduce the global burden of naturally occurring emerging, re-emerging, and surging infectious diseases.

To achieve these capabilities by 2015, the following near-, mid-, and long-term priorities have been developed.

NEAR-TERM PRIORITIES

- **Threat Awareness** – Complete the second formal risk assessment required under the President’s *Biodefense for the 21st Century* – adding engineered threats, agricultural threats and economic consequences to the earlier baselines --and use these to establish an improved risk assessment methodology as well as to prioritize the threats of concern, key vulnerabilities, and data gaps critical in reducing the uncertainties in the assessments and guiding the national response. Perform the analyses and laboratory experiments needed to close those data gaps for the classical biological agents, including the effective infectious doses of the agent in media such as air, food, and water and the viability of those agents as a function of time after their release and after decontamination. Start to characterize and prioritize key attributes of enhanced threats (e.g., modified organisms, such as antibiotic-resistant agents) and advanced threats (engineered agents that are not found in nature). Develop and document the scientific concept of operations for identifying, characterizing, and responding to an enhanced, emerging and advanced threat and use this to identify key gaps and better guide the formulation and implementation of an engineered threat strategy.
- **Prevention and Protection** – Work with the National Science Advisory Board for Biosecurity better to define the guidelines and reporting of “dual-use” research (i.e., life sciences research that has intrinsic scientific value but that may also have significant bioterrorism implications). Continue to identify and control select agent use and transfer. Develop methodologies and technologies for monitoring international transportation nodes. Conduct research and development activities that build on earlier vulnerability studies and systems studies to protect and harden critical nodes in our national infrastructure. Pilot integrated facility protection systems (“shields”) drawing on the best elements of the DoD Immune Building, EPA Safe Buildings, and DHS Protective and Responsive Options for Airport Counter-Terrorism (PROACT) programs, as well as other programs with a similar focus.

- ***Surveillance and Detection*** – Develop a first-generation integrated biosurveillance system that provides decision makers with critical information regarding early detection and situational understanding of a possible biological attack. Develop the underlying capabilities for this system and develop a system for integrating human health data (e.g., from BioSense, the Veterans Health Administration, and the DoD TRICARE System), environmental data from air (e.g., from BioWatch, Guardian, and the United States Postal Service Biohazard Detection System), food, and water supply monitoring systems (e.g., from Water Sentinel), and intelligence data, while continuing to ensure privacy protections for individuals. Continue to expand the coverage, granularity, and timeliness of this system and its component elements and develop and validate tools for early event detection and for hazard assessments. Complete the development, test and piloting of the fully autonomous Generation 3 BioWatch detection technology. Pilot and deploy a first-generation contaminant warning system to provide early indication of intentional contamination in metropolitan water distribution systems. Continue to expand the coverage and timeliness of BioSense. Track and monitor emerging zoonotic diseases (i.e., those that infect both animals and humans). Develop integrated, interagency concepts of operations, notification protocols, and incident characterization procedures for early detection and characterization of a possible biological event. Establish a coordinated network of laboratories for analyzing environmental, clinical, food, and agricultural samples for biological agents and for providing the necessary surge capacity needed to respond to an attack. Initiate programs for developing rapid, pre- and early post-symptomatic medical diagnostic devices that allow rapid determination of exposure and development of biomedical countermeasures to second-generation threat agents. Continue to develop enhanced detection methods with improved timeliness, sensitivity, selectivity, and ability to determine treatment-relevant characteristics such as viability and antimicrobial sensitivity.

- ***Response and Recovery*** – Continue the near-term Project BioShield programs focus on improved medical countermeasures for anthrax, smallpox, botulinum toxin, and acute radiation syndrome (ARS). Utilize the new Public Health Emergency Medical Countermeasure Enterprise (PHEMCE) and the Biomedical Advanced Research and Development Authority (BARDA) to provide greater transparency into future countermeasure needs, better integration of the full development cycle for research through acquisition, and greater involvement and partnering with local, private, and academic partners. Provide funding for critically needed advanced development activities. Develop the ability for rapid screening of existing antimicrobials and antivirals for “off-license” applications. Define and initiate an applied Federal government RDT&E program to develop critical product development tools to support the product pipeline. Conduct early stages of R&D on the development of broad-spectrum countermeasures. Develop improved medical decontamination and protection protocols for incoming patients and the medical personnel who treat them. Establish an interim set of guidelines, protocols and tools for the restoration of large areas and enclosed facilities for the highest priority agents, considering user and stakeholder needs and incorporating an effective risk communication strategy. Develop a coordinated Federal government roadmap and milestones for the desired mid- and long-term (e.g., five or more years) capabilities in this area.
 - ***Basic Research*** – Continue research to characterize pathogenic mechanisms, innate and adaptive immune responses, and host-pathogen interactions. Identify candidate targets for environmental sensors, early biomarkers for medical diagnostics, and new mechanisms for broad-spectrum antimicrobials, antivirals and immuno-modulators

MID-TERM PRIORITIES

- ***Threat Awareness*** – Conduct formal risk assessments every two years, as required by the President’s *Biodefense for the 21st Century*. Use these assessments to guide and refine biodefense priorities. Conduct net assessments every four years to assess the fundamental assumptions underlying our biodefense strategies and to measure progress against this

strategy. Complete closing the major knowledge gaps on the traditional threat agents. Begin focusing attention on strategies for countering enhanced and engineered threats, including those that focus on basic biological building blocks such as virulence pathways and their regulators. Develop and monitor indicators of the development of enhanced and advanced agents and conduct a technology watch for unexpected breakthroughs that can have significant threat implications.

- ***Prevention and Protection*** – Continue the development of methodologies and technologies to identify and monitor potential bioweapons activity and to secure the acquisition, use, and transfer of select agents. Implement, as appropriate, passive and active protection systems as identified and developed through such programs as DoD’s Immune Building Program, EPA’s Safe Buildings Program, and the DHS PROACT Program. Continue research on cost-effective, non-intrusive protection methodologies to enable the extension of facility protection to a broader range of facilities and to minimize the potential of exposure to biological agents in case of an event.
- ***Surveillance and Detection*** – Continue to improve biosurveillance system capabilities. Extend BioSense to many local sources as well as national sources, incorporating emergency rooms, laboratories, and other sources throughout the Nation. Greatly expand the capability of urban bioaerosol monitoring systems, by deploying the Generation 3 BioWatch system. The reduced operational cost of this fully automated system will enable monitoring a much larger fraction of the Nation’s population for a broader range of agents with readouts several times per day. Enhance and expand food surveillance and water monitoring systems. Continue to improve the abilities of the National Biosurveillance Integration System (NBIS) and its associated analysis group to integrate these and other sources to provide near real-time situational awareness. Improve environmental and medical detection capabilities for enhanced agents through identifying and using signatures for threat agents that are tied to virulence factors, antimicrobial resistance genes, and markers of genetic engineering. Begin development of environmental and clinical detection systems for detecting and rapidly characterizing advanced agents. Develop “detect-to-warn” systems with very low false alarm rates that can detect biological agents in less than five minutes and that can facilitate taking protective actions to avoid exposure in critical facilities and at special events. Bring the NBFAC to full operational capacity and achieve International Organization for Standardization (ISO) accreditation for all its associated laboratories so that the data it generates can withstand scrutiny in the international community and can be used by appropriate agencies for attribution purposes. Assemble a comprehensive biological threat agent reference strain collection and develop analysis plans, protocols, tools and high-throughput analysis systems for forensic analyses of all top-priority threats.
- ***Response and Recovery*** – In accordance with the PHEMCE Implementation Plan, pursue Project BioShield acquisitions against those threats for which there are Material Threat Determinations and for which subsequent medical modeling has shown the need for additional medical countermeasures. Through DoD and HHS, bring several next generation broad spectrum countermeasures and their enabling platform technologies to the early and advanced development stages. Using animal models, identify pathogen- and host-derived biomarkers of infection as potential early indicators of exposure, and use these biomarkers to develop prototypes of pre- and early post-symptomatic diagnostic devices. Develop, demonstrate, approve, and certify guidelines, protocols, and supporting technologies that enable timely and affordable restoration of large outdoor urban areas, the facilities therein, and other critical infrastructures, such as the water distribution and transportation systems from the high-priority classical threat agents. Develop and approve an interim strategy for addressing decontamination of enhanced agents.
- ***Basic Research*** – Continue implementation of the strategies for broad-spectrum countermeasures and for greatly accelerating the bug-to-drug timeline. Continue basic research programs in infectious disease, developing initial systems models of immune

response and host-pathogen interactions. Continue research on advanced techniques for detecting and characterizing totally new agents and on novel preventives and therapeutics.

LONG-TERM PRIORITIES

- ***Threat Awareness*** – Achieve a fully integrated Federal government biological threat assessment infrastructure that will combine technical and intelligence-based threats with vulnerability and risk assessment capabilities. Provide a thorough intelligence-informed, science-based understanding of current threats and effective anticipation of future threats. Continue implementation of the strategy for defending against enhanced and engineered threats.
- ***Prevention and Protection*** – Develop and incorporate affordable and sustainable passive and active protection measures for critical infrastructures. Where appropriate, these protection systems will exploit advances in immune and safe building design and real-time biodetection to initiate protective measures and will be part of an integrated all-hazards facility protection system.
- ***Surveillance and Detection*** – Achieve widespread international, national, and local coverage and integration of the biosurveillance system to enable early warning and characterization of biological attacks. Fully develop and deploy the environmental, pre-symptomatic, and clinical diagnostic tools needed for rapid detection, identification, and characterization of traditional, enhanced and advanced biological agents. Have well-established biodetection standards, protocols, and validation procedures available for use throughout the government and private sector. Bring to full operational status the integrated network of environmental, clinical, food, and agricultural analytical laboratories with sufficient surge capacity to provide necessary response and characterization during a major event.
- ***Response and Recovery*** – In accordance with the President’s *Medical Countermeasures against Weapons of Mass Destruction’s* (HSPD-18) pursue advanced development and, where appropriate, acquisitions of broad spectrum antibiotics and antivirals, including post exposure countermeasures against filoviruses. To the extent possible develop medical countermeasures that are simpler to administer, thereby reducing the burden of mass casualty treatment. Establish an initial capability for rapid drug development going from initial ‘detection’ of a modified or new threat to production of sizeable quantities of medical countermeasures in a period of months. Fully develop, deploy, and integrate inexpensive and rapid pre- and early post-symptomatic medical diagnostic devices able to identify both conventional and novel biological agents. Develop, as needed, next-generation databases, tools, protocols and systems to support timely and affordable decontamination of large outdoor exposed areas and their included personnel and facilities.
- ***Basic Research*** – Continue basic research programs in infectious disease, developing second-generation systems models of immune response and host-pathogen interactions. Test the initial and interim approaches to broad spectrum countermeasures and use results to inform next stages of their development as well as to feed into the advance development and acquisition process.

AGENCIES’ ROLES AND RESPONSIBILITIES

The roles and responsibilities of the various Federal Departments and agencies are clearly defined in the President’s *Biodefense for the 21st Century*. DHS is responsible for overall coordination of domestic Federal operations to prepare for, respond to, and recover from attacks with biological agents. The Department of State is responsible for international terrorist incidents that take place outside the U.S. territories. The Department of Health and Human Services is responsible for coordination of public health response to a biological event and development of medical countermeasures to support preparedness and response and recovery.

Within the four essential pillars of biodefense the various Federal departments and agencies have the primary responsibilities listed below:

AGENCIES' ROLES AND RESPONSIBILITIES

Department of Defense (DoD)

- Conducts research, development, and acquisition for medical and non-medical countermeasures focused on requirements of the military population.

The Department of Health and Human Services (HHS)

- Leads (in coordination with other Departments and agencies) the anticipation of future biological threats to humans; the research, development, acquisition, stockpiling, and distribution of medical countermeasures for chemical, biological, radiological, or nuclear threat agents; strengthening and coordinating the Nation's public health preparedness and response and mass casualty response. Also under the National Response Plan, HHS has the lead responsibility, in coordination with other Departments and agencies, for the public health response to any biological event.

Department of Homeland Security (DHS)

- Leads (in coordination with other Departments and agencies) threat, vulnerability, and risk assessments; critical infrastructure protection; coordination of attack warning; research, development, testing, and evaluation of non-medical countermeasures; technical forensics analysis in support of attribution; development of the *National Response Plan* to provide for seamless coordinated Federal, State, local, tribal, and international response; and coordination of risk communications. DHS has the primary responsibility to coordinate domestic Federal operations to prepare for, respond to, and recover from attacks with biological agents.

Department of State (DOS)

- Coordinates Federal operations to prepare for, respond to, and recover from international attacks with biological agents that take place outside the U.S. territories.

Environmental Protection Agency (EPA)

- Develops science and technology to support development of specific standards, protocols, and capabilities to address the risk of contamination following a biological attack, as well as strategies, guidelines, and plans for decontamination of persons, equipment, and facilities. Conducts testing and evaluation of decontamination and detection technologies. Additionally, the EPA, in coordination with its Federal partners, is the lead agency for protection of the water infrastructure sector and is the lead agency that shares responsibility with the U.S. Coast Guard for coordination of the National Incident Command Center under the *National Response Plan*.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Since the anthrax letter attacks in the fall of 2001, the Federal government has greatly expanded its biodefense capabilities and science and technology activities. The following are examples of accomplishments, capabilities, and ongoing activities of the Federal government. While these accomplishments are listed under the lead Federal agency, many, if not all, involve strong interagency collaborations and partnerships. Biodefense is inherently a multi-agency undertaking and such multi-agency partnering and collaborations are central tenets of the President's directive concerning *Biodefense for the 21st Century*.

Department of Defense (DoD)

- Expanded the Electronic Surveillance System for the Early Notification of Community-Based Epidemics (ESSENCE), DoD, and Global Emerging Infections System (GEIS) human health surveillance systems which may provide early signals of deliberate and natural disease outbreaks.
- Began the deployment of the Guardian system at military bases in the U.S. to enable early detection of biological attacks and initiation of life-saving prophylaxes.
- Developing next-generation chemical and biological detection systems.
- Conducting research and development on individual and collective protection, including strategies and technologies for protecting key facilities.
- Researching decontamination systems to neutralize or remove contamination from fixed sites.
- Transitioned lead candidates for medical countermeasures from its science and technology base to the Department of Health and Human Services (HHS) for advanced development, including a next-generation anthrax vaccine (recombinant protective antigen, rPA) and botulinum antitoxin.
- Continues to pursue vaccines for botulism, plague, and Ebola virus, as well as therapeutics for plague, anthrax, botulism, smallpox, and viral hemorrhagic fevers.
- Developing broad spectrum medical countermeasures and novel, rapid approaches to drug development to counter future threats

Department of Health and Human Services (HHS)

- Registered over 330 entities for possession, use, and transfer of select agents and toxins to help control access to and use of those biological agents that have the potential to pose a severe threat to public health and safety.
- Collaborated with the Department of Agriculture (USDA) in promulgating the final select agent rule including a common set of biosafety and biosecurity compliance requirements and is putting in place a joint select agent information system.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

HHS, continued

- Expanded to all 50 states the Laboratory Response Network which connects public health labs of many kinds that can help in an emergency.
- Enhanced its laboratory-based capabilities to develop rapid tests, to detect and identify biological agents in a wide range of environmental specimens, and to investigate and identify unknown pathogens.
- Established performance measures for public health preparedness to set priorities and measure progress of the public health system's ability to respond to threats and emergencies.
- Funded two Microbial Sequencing Centers, ten Regional Centers of Excellence for Biodefense and Emerging Infectious Diseases, and eight Cooperative Centers for Translational Research on Human Immunology and Biodefense that will build a strong infrastructure and workforce for biodefense research and development.
- Finalized the "animal rule" which provides for using animals to test the efficacy of medical countermeasures when human tests would be unethical or unfeasible.
- Provided funding to States, localities, and hospitals to improve their capacity to detect, diagnose, prevent, and respond to attacks with biological agents.
- Expanded the Strategic National Stockpile (SNS) to include millions of doses of medical countermeasures and associated medical equipment in "12-hour Push Packages" that can be delivered anywhere in the U.S. within 12 hours.
- Acquired and stored in the SNS enough smallpox vaccine for every American.
- Implemented Project BioShield, which involves the coordinated activity of the Department of Homeland Security (DHS) and HHS to create a guaranteed market to stimulate the development and acquisition of new medical countermeasures and to accelerate their development.
- Using its Project BioShield authority to pursue acquisition of the next-generation medical countermeasures for anthrax, a safer smallpox vaccine, a botulinum antitoxin, and radiological and nuclear countermeasures for the SNS.
- Conducting research on new therapeutics for anthrax, plague, botulism, smallpox, viral hemorrhagic fevers and on broad spectrum medical countermeasures.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

HHS, continued

- Prepared and published guidance on and implements the Emergency Use Authorization (EUA) established under the *Project BioShield Act of 2004* to authorize the emergency use of unapproved medical products, or of unapproved uses for approved products, where these are the best available products in an emergency.
- Created the Public Health Emergency Medical Countermeasure Enterprise (PHEMCE) to better integrate all aspects of medical countermeasure development from R&D through advanced development, to licensure, acquisition, deployment and use.
- Developed and published the HHS medical countermeasure strategy and an implementation plans, conduct annual stakeholder workshops, and ongoing dialogue with stakeholders, released a draft Strategic Bioplan for the Biomedical Advance Research and Development Authority (BARDA) established a web portal to better communicate medical countermeasure needs and plans, to increase transparency, and to build more effective partnering with local government, public, private and academic sectors.
- Developing and deploying BioSense, a human health electronic surveillance system to provide early detection of deliberate and natural disease outbreaks and a situational awareness safety net that currently has over 400 users in 49 states and 34 metropolitan reporting areas and has processed over 850 million records.
- With the Association of State and Territorial Health Officers and the National Association of City and County Health Officers, has defined the technical architecture (the Public Health Information Network, PHIN) for public health information systems for early event detection and situational awareness, outbreak management, countermeasure and response administration, connecting laboratory systems, and partner communication and alerting. To support this, HHS has developed 10 software systems and services that are available for Federal, State, and local participants.
- Supporting Federal government decontamination efforts by conducting environmental microbiology research in areas such as detection, identification, pathogenicity, transmissibility, and persistence of microbial pathogens.
- Provides national technical support for response and preparedness for environmental monitoring and sampling strategies, laboratory analysis, diagnosis, surveillance, and treatment.
- Maintains a field workforce of 440 public health advisors and medical and epidemiology officers to assist State and local public health agencies and supports terrorism training and preparedness through the Public Health Readiness Certificate Program.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

HHS, continued

- Established the National Science Advisory Board for Biosecurity (NSABB) to provide advice to Federal departments and agencies on ways to minimize the possibility that knowledge and technologies emanating from vitally important biological research will be misused to threaten public health or national security.
- Co-founded and actively participates in the Global Security Health Action Group (GSHAG), composed of the health ministers of seven leading nations convened for the purpose of coordinating international efforts in biodefense and public health preparedness.
- Collaborating with the Department of State in promoting model biosecurity legislation based on the Select Agent rule.
- Maintains the U.S. Public Health Service Commissioned Corps, composed of trained clinicians and public health experts that can augment staffing in vaccination clinics and prophylaxis sites, evaluate occupational and environmental health risks, perform epidemiological tracking, and assist in other emergency public health services for affected communities.

Department of Homeland Security (DHS)

- Created the National Biodefense Analysis and Countermeasures Center (NBACC) to provide scientific support for intelligence on and assessment of the current and evolving threat and to provide bioforensic analysis of evidence in support of attribution and interdiction activities.
- Conducts biennial, formal, risk assessments of a broad range of biological agents and threat scenarios as part of the President's *Biodefense for the 21st Century*. The output of the risk assessments are used to inform national priorities and investments in biodefense.
- Issues Material Threat Determinations for the most significant threats and conducts Population Threat Assessments to estimate exposed populations in support of Project BioShield.
- Deployed, in collaboration with HHS and the Environmental Protection Agency (EPA), the first-generation BioWatch environmental detection system in major cities throughout the United States to enable pre-symptomatic detection of aerosol releases of biological agents and the initiation of life saving prophylaxes and is currently significantly enhancing this capability in the top threat cities.
- Developing next-generation, fully automated, affordable detection systems capable of continuous operations for urban monitoring, as well as for selected agricultural and food applications.
- Leads an interagency effort to develop a coordinated National Biomonitoring Architecture.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DHS, continued

- Leads an interagency effort to develop a comprehensive early attack warning system that integrates and analyzes information from environmental detection and human and animal health surveillance systems in the context of threat information to provide the capability for rapid recognition and characterization of both deliberate and natural biological outbreaks.
- Developed, in partnership with other Federal and local authorities, protocols and tools for rapidly restoring transportation hubs after a biological attack and, in partnership with DoD and others is developing protocols and tools for restoring wide urban areas following an attack.
- Established an interim capability for the National Bioforensic Analysis Center (NBFAC) and is conducting operational casework in support of Department of Justice (DOJ) investigations into biocrimes and bioterrorism.
- Led the Federal government-wide effort that developed the National Response Plan and the National Incident Management System for responding to and recovering from terrorist attacks and natural disasters.
- Working with the EPA to develop a systems framework for decontaminating facilities and outdoor areas.
- Conducts systems studies and modeling of the consequences of biological attacks in order to help guide biodefense strategic planning and the countermeasure research, development, and acquisition strategies to implement those plans.

Department of Justice (DOJ)

- Processed over 7,100 risk assessment applications for registered entities under the Select Agent Program.
- Established the Weapons of Mass Destruction Directorate.
- Partnered with DHS, HHS, and EPA to develop sampling, detection and response protocols that protect the public health while also protecting the evidentiary material needed to prosecute biocrimes and acts of bioterrorism
- Worked with DHS to establish the NBFAC component of NBACC based on DoD technology.

Department of Veterans Affairs (VA)

- The U.S. Department of Veteran Affairs manages the largest integrated health care system in the United States. This system uses electronic medical records that endow the VA, and with appropriate agreements other Federal agencies, extraordinary capability for biomedical surveillance.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Environmental Protection Agency (EPA)

- Conducts systems studies and modeling of the consequences of several potential types of biological attacks in order to help guide decontamination and remediation research, development, and acquisition programs and strategies.
- Performed a CARVER + Shock analysis to understand the nature of the biological threat to drinking water distribution systems. These results inform research activities.
- Developed and disseminated guidance for water utilities, called the Response Protocol Toolbox that is intended to allow water utilities to prepare for and respond to potential terrorist attacks.
- Developing a first-generation contaminant warning system, Water Sentinel, that would deploy an integrated monitoring and surveillance system to provide warning of intentional biological contamination of drinking water.
- In collaboration with DHS, is developing a national program that would expedite the recovery of water utilities from a biological attack through mutual aid agreements and other means of assistance.
- Manages, in collaboration with DHS, the ongoing field sampling activities for the BioWatch program, and assists with the development of consequence management guidance and planning templates.
- Staffing a new National Decontamination Team to provide scientific and engineering expertise in decontaminating buildings, building contents, and critical infrastructure contaminated by biological agents and other weapons of mass destruction (WMD).
- Developed reference guides and tools for decontamination options, including more than 20 Quick Reference Guides for high priority agents and a National Decontamination Portfolio which will provide a comprehensive, integrated electronic source of the best available information on WMD decontamination.
- Developed an online Environmental Laboratory Compendium listing the capabilities and estimated capacities of 280 governmental and commercial laboratories that might be called upon to respond to a terrorist attack.
- Enhanced its microbiology laboratory's capabilities and capacities to support decontamination research and response.
- Has participated extensively in the cleanup of facilities contaminated with *Bacillus anthracis* spores since October 2001, tested the efficacy of selected decontamination chemicals, and approved 28 crisis exemptions permitting the use of unregistered antimicrobial products for the cleanup of these sites.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

EPA, continued

- Conducts research and development for the protection of buildings, including the evaluation of commercial detection systems, air cleaners, air filters, and shelter-in-place protocols for use in protecting building occupants and response personnel.
- Developed procedures for handling and processing emergency water samples suspected of contamination with known or unknown biological material.
- EPA is evaluating effectiveness of building protection options, developing corresponding cost/effectiveness models and is working with NIST to develop effective guidance for building owners, operators, and designers.

National Science Foundation (NSF)

- Conducts, jointly with HHS, research and development programs in ecology and infectious diseases, microbial genome sequencing, and microbial interactions and processes that build the knowledge base for understanding potential biothreats and suggest approaches to avoid and counteract such threats. Supports efforts to generate information about the natural occurrence of potential pathogens in water, soil, and air. Is conducting research on novel sensors to detect biological agents.

Federal Government, cooperatively

- Maintains, along with the U.S. Coast Guard, an emergency operations center and a cadre of “On Scene Coordinators” who respond to environmental contamination events and coordinate the Federal response and clean up effort.
- Established the Integrated Consortium of Laboratory Networks to leverage the laboratory capabilities of the Federal departments and agencies better.

CHAPTER 2 – DEFENSE OF ANIMALS, PLANTS, AND FOOD AGAINST BIOLOGICAL THREAT AGENTS

INTRODUCTION

The country's agriculture and food production systems are vital to the economic, social, psychological, and political well-being of the U.S. and the world. Food production, processing, and distribution account for one-in-eight U.S. jobs and constitute approximately 10 percent of the gross national product. Agricultural exports contribute positively to the balance of trade. The remarkable success of the U.S. in agriculture and food production provides the Nation with subsistence independence, a significant strategic advantage over most countries of the world. At the same time, compared to other sectors of the U.S. economy, overseas markets are proportionally more important to U.S. agriculture, and reliance on these markets is increasing at a rapid rate.

Nations have always valued the provision of a safe, abundant and wholesome food supply. Governments and industry have focused food protection efforts to protect against accidental or naturally occurring contamination, spoilage due to improper processing and handling, or economic fraud. In the wake of September 11 and recent anthrax incidents, our nation's bioterrorism response capability has become an eminent priority for policymakers, researchers, public health officials, academia and the private sector. As terrorist attacks continue to escalate internationally, there is widespread concern about an attack on the food supply. In 1984, in Oregon, a religious cult contaminated salad bars with Salmonella, resulting in more than 750 reported illnesses. In 2002, in China, 38 people died and hundreds were sickened from consuming food intentionally contaminated with rat poison. In 2003, New Zealanders were warned of a potential intentional food contamination following the World Cup race. Israeli oranges contaminated with mercury negatively impacted international trade; the threat of Chilean grapes spiked with cyanide had a deleterious effect on economic markets. These terrorist events, to date, have been localized, but have served as a warning to shift our attention to protection of the food supply from the risk of intentional contamination.

Adequately protecting the food supply requires a multifaceted coordinated and global approach. Concerned governments, companies, and academic institutions are instituting or increasing counterterrorism programs to protect the entire food chain from production to the consumer. Numerous research and development programs have been initiated to develop and deploy technologies that will deter and detect an attack on the food supply. Research and development are needed to develop countermeasure that will minimize the likelihood and reduce the scope of an attack. Research and development and coordinated efforts are also needed for a complete and rapid recovery from a food borne attack.

Any deliberate or natural disruptions of the Nation's agriculture or food production systems could have enormous economic, public, and mental health impacts, and would present a serious threat not only to the Nation's economy and society, but also to the national strategic posture.

Protecting the agriculture and food infrastructures are clearly national priorities. Homeland security science and technology for agricultural and food biodefense focuses, supports, and enables an integrated, multi-layered defense. Requirements are derived from the Presidential Directives on *Defense of United States Agriculture and Food* and *Biodefense for the 21st Century*, which specify four essential pillars for biodefense: Threat Awareness, Prevention and Protection, Surveillance and Detection, and Response and Recovery. The strategy is also informed by reports from a number of Federal government working groups and non-governmental organizations that have identified requirements, research and development gaps, and priorities for the Nation's agricultural and food biosecurity and have clarified the roles and responsibilities of the respective Federal agencies.

THREATS AND VULNERABILITIES

The agriculture and food systems of the U.S. are extensive, open, international, interconnected, diverse, and complex structures that are largely owned and operated by the private sector. According to a 1999 report by the congressionally created Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction, most of the nations identified as sponsors of terrorism either have or are seeking weapons of mass destruction. According to the commission, more than a dozen states have offensive chemical and/or biological weapons programs. Of the biocrimes and bioterrorism events within the last century, attacks on the food supply have predominated other possible methods of delivery.

The potential impact from a planned attack can be imagined by considering previous examples of accidental exposure to food borne poisoning. In 1994, roughly 224,000 people in 41 states were sickened accidentally by Salmonella enteritidis infection linked to a contaminated ice-cream premix. A naturally occurring outbreak of Hepatitis A from clams sickened nearly 300,000 people in China in 1991. A deliberate concerted attack on the food supply has the potential to be a public health and economic disaster. As a consequence, defense of the food supply from intentional contamination has now become a worldwide concern for the 21st century. In the U.S. alone, efforts in the U.S. Department of Agriculture, Department of Homeland Security, Health and Human Services, Department of Energy, Department of State, and Department of Defense have allocated and increased resources to defend the nation's food supply from intentional attack. The G-8 Meeting of Scientific Experts and the Asia-Pacific Economic Cooperation (APEC) Nations have both convened scientific meetings to address food defense.

The epidemiology of food borne diseases has undergone profound changes in the recent years. Factors influencing this change are the global distribution of food supplies to meet increasing consumer demands for greater variety and freshness of foods, and centralization of food production. The current centralization of food production, processing, and distribution now allow food security failures to cause high numbers of casualties over a large geographic areas that could result in a public health emergency with tremendous economic consequences and loss of confidence in national security.

The food industry is critically important to the social, economic, and political stability of the United States, in addition to its obvious significance to public health. One in eight people works in an occupation that is directly supported by food production. Agriculture's share of produce sold over seas is more than double that of other U.S. industries, which makes the sector a major component in the U.S. balance of trade. The crisis in Belgium, in which dioxin contaminated products involved a world-wide recall, demonstrates not only the extensive costs to individual countries,(a complete change in political structure in that country) but also the extent of disruption of global trade that can be caused by this type of incident.

There are dozens of economically important species of domestic animals and plants, and these have hundreds of known pathogens. Of these, there are many host-pathogen combinations with properties that terrorists may chose to exploit. The potential also exists for the development of agents that have been altered to escape detection, or those that are resistant to current conventional treatments. The density and breadth of the agriculture and food sectors (including the transportation systems that interconnect them), the communicability of threat agents, and trade concerns all limit control options and increase the potential for rapid disease spread across the country.

In addition to disease outbreaks that originate within the U.S., the speed and global reach of the travel and cargo movements, especially in the international agricultural and food trade, makes the U.S. vulnerable to disease outbreaks and contaminated foods, whether deliberate or natural, that originate outside the Nation. Whatever their origin, an outbreak of selected plant or animal diseases in this country would severely compromise domestic retail markets, as well as the ability to export U.S. agricultural or food products. This would cause significant harm to a U.S. agricultural sector whose economic well-being depends on access to export markets.

All of these factors combine to provide numerous potential targets and opportunities for terrorist attacks and a challenging threat and vulnerability environment. Without adequate surge capabilities, our capacity to diagnose and treat disease outbreaks (animals or plants), or to identify contamination in the food supply and manage its consequences, would quickly become saturated, and the quality of any response would be degraded rapidly.

REQUIREMENTS

To defend successfully against attacks on the Nation's agricultural and food systems, priorities need to be established and investments need to be made in a number of key areas. Federal agencies have received extensive guidance in this regard, most recently in the President's *Defense of United States Agriculture and Food and Biodefense for the 21st Century*. Major elements of these directives include:

- ***Threat Awareness*** – Methods, architectures, technologies, and knowledge are required to support enhanced intelligence operations and analysis capabilities for the agriculture and food sectors, including threat, vulnerability, and risk assessments (including secondary and other higher-order effects); intelligence collection focused on actual agriculture and food chain vulnerabilities; improved guidance to industry and law enforcement on appropriate (accurate, concise, and timely) incident reporting; exercises across all levels of government and industry; and information sharing among government agencies, the private sector, and international partners.
- ***Prevention and Protection*** – Science and technology support for vulnerability assessments is required to identify and prioritize requirements of the *National Infrastructure Protection Plan* concerning agriculture and food to reduce the overall vulnerability of the agriculture and food systems (see Chapter 6: “Critical Infrastructure Protection”). A tremendous amount of research will be required to support vulnerability assessments mandated by HSPD-9. Although there is substantial information regarding survival of threat agents such as *Listeria*, *E. coli* O157:H7 and *Salmonella* that are common foodborne pathogens in food; very little is known about the behavior /survival of atypical threat agents such as *Bacillus anthracis* or ricin in food matrices. In addition, there are currently few validated methods available for the detection and quantitation of those atypical threat agents that are not routinely found in food. Little is known about the effects of typical processing, handling and storage effects on threat pathogens, toxins and chemicals in complex food matrices. Mitigation technologies and strategies are required to protect critical production, as well as increasingly centralized processing nodes, from the introduction of diseases, pests, or toxins. Methods, architectures, and technologies are required for the cost-effective and timely screening and inspection of both the domestic food supply and agriculture and food items entering the United States.
- ***Surveillance and Detection*** – National and international surveillance and reporting systems, environmental and facilities monitoring systems, and laboratory diagnostic systems are required to provide early detection, awareness, forensics, and attribution capabilities for naturally occurring and intentionally introduced animal and plant diseases, pests, or poisonous agents. Local, regional and national tracking systems for animals (domestic, companion animals, and wildlife), plants, and food are also required, as are national laboratory networks for animal, wildlife, and plant health and food that enable rapid and reliable detection (including pre-symptomatic) and confirmation of infection or contamination.
- ***Response and Recovery*** – Methods, architectures, and technologies are required that enable robust and cost-effective response capabilities. Science and technology support for a coordinated response plan for agriculture and food which is integrated into the *National Response Plan* is required, including the development of decision support tools and concepts of operations for scenarios at local-to-continental scales. Veterinary countermeasures to animal and zoonotic diseases that are pre-positioned in a rapidly

deployable National Veterinary Stockpile are required, including vaccines, antiviral, antimicrobial, and other therapeutic products for the most damaging animal diseases affecting human health and the economy. Countermeasures for plant disease and pest control are required for a National Plant Disease Recovery System, including pesticide control measures and the development of resistant crop varieties for foreign crop pathogens. Science-based methods and technologies for rapid, affordable, safe, and environmentally sound disposal of contaminated agriculture and food products or infected plants and animals and for decontamination and restoration of associated infrastructure are also required. Effective and affordable equipment for the rapid and stringent implementation of enhanced biosecurity measures at farms, shipping, and processing facilities must be developed and stockpiled.

- ***Cross-Cutting RDT&E*** – There are important cross-cutting requirements for agricultural and food biodefense research and development, including the critical need for better coordination and synchronization of Federal, State, local, tribal, and private efforts.
 - Robust models are required to determine and optimize strategies for agriculture and food biodefense, to prioritize biodefense investments across the range of economically important food products and animal and plant species, and to enable government and industry to develop appropriate changes to these infrastructures to defend against disease, adulteration, and contamination. These models include general and disease-specific epidemiologic models of disease spread within target animal and crop populations. In addition, models of the social and economic impacts of disease outbreaks, and full end-to-end systems studies are needed. Modeling of growth, survival, and inactivation of high consequence pathogens in complex food matrices and survival of bioterror toxins and high consequence chemicals in food matrices must be developed to support risk management decisions.
 - Basic understanding of the biology, pathogenesis, host-pathogen interactions, and epidemiology of disease spread for specific animal and plant diseases are required to enable development of new diagnostics, countermeasures, and forensics capabilities and to support the development of epidemiologic models. Research on the social, psychological, and economic impacts of disease outbreaks and intentional attacks on food supply will contribute to our ability to build fully inclusive models and is also required for the development of effective risk communication and response and recovery strategies. All of these activities will support threat and risk assessments and end-to-end systems studies, as well as the development of decision support tools and exercises.
 - Modern, state-of-the-art biocontainment facilities are required for basic research studies and for advanced research, development, testing, and evaluation of countermeasures to high-consequence foreign animal, zoonotic, and crop diseases. Such facilities, which include re-capitalized Biosafety Level 3-Agriculture (BSL-3Ag) laboratories and new large-animal BSL-4Ag laboratories, are also required for providing rapid diagnostic and support capabilities in the event of an animal health emergency.
 - Finally, both higher education programs and outreach and professional development in the agriculture and food sectors are required. This includes education and training of the next generation of research scientists and information sharing and analysis with the private sector. Leveraging over 100 years of cooperative state research and extension service, outreach programs for producers, private practitioners, and animal and plant care workers and disaster teams (including veterinarians and plant pathologists) that enhance education and awareness about foreign animal and plant diseases are also

required so that they know what to look for and who to contact in the event of a suspected disease outbreak, as well as providing education and training on best practices in the commercial and government sectors when animal disease incidents occur. Programs that foster interaction and collaboration with other nations and their scientists are also required, including those relating to the sharing of scientific information, collaborative research, and working internationally to strengthen U.S. scientific capabilities.

GAPS

Interagency working groups have provided a number of analyses of gaps and priorities for agricultural and food research and development. Common themes recur in these studies, and their highlights are provided below:

- ***Need for Enhanced Intelligence and Threat Information*** – Comprehensive intelligence, threat, vulnerability, and risk assessments are lacking for a large number of economically important agricultural species (animals and plants), food products, disease vectors, and their respective pathogens. This includes the need for focused and persistent vulnerability- and risk-based intelligence collection for the domestic and international agriculture and food systems.
- ***Need for Enhanced Protection of Critical Agricultural and Food Production and Processing Nodes*** – Vulnerability assessments that identify critical nodes and define requirements for efficient and cost-effective protection and prevention architectures, or “food shields,” have been performed for only a subset of the major agriculture (animal, crop) and food systems. Food shields, including methods for deactivating pathogens during food processing that lacks a traditional “kill step”, are not yet in place for most systems that have been assessed.
- ***Need for Improved Surveillance and Detection Technologies and Systems*** – National coordination of infectious disease surveillance and reporting is important for enabling rapid and integrated responses to domestic disease outbreaks. In the case of animal or plant disease outbreaks abroad, international surveillance needs to be improved to meet U.S. security needs.
 - Research to support development of validated robust methods to detect threat agents in food is needed to support the Food Emergency Response Network of laboratories. A reliable stream of reagents and assays is necessary to support food testing in the case of an attack on the food supply system and to allow for release of safe food in the aftermath of an attack.
 - Field-deployable detection systems capable of reliably recognizing a large number of diseases of concern and distinguishing them from low-consequence diseases with similar clinical presentations are lacking, while validated diagnostics for animal and plant health and food are not yet placed throughout the national laboratory networks in a manner that provides adequate surge capacity and the capability for rapid deployment.
 - Tracking systems for animals, plants, and food products throughout the domestic and international food supply systems, including cost-effective capabilities for rapid detection, identification, and tracking of contaminants in a wide variety of food matrices throughout the production system, are not yet in place.
 - End-to-end assessments and systems studies that evaluate the feasibility, requirements, and cost of these surveillance, detection, and tracking systems are in progress, but the recommendations of these studies (including requirements, architectures, and trade-offs) are not yet available.

- Bioforensics and attribution capabilities for animal, plant, and food pathogens, including rapid diagnostics, a comprehensive international strain archive and genome sequence database, and dedicated forensics laboratories and personnel, have not been developed.
- ***Need for Improved Response and Recovery Architectures, Systems, and Technologies*** – There is insufficient surge capacity to cope with animal, plant, and food emergencies, including laboratory and field personnel, laboratories, validated assays and rapid diagnostics, mobile and field-deployable diagnostic capability, and vaccine stockpiles. Current response strategies for highly contagious infectious animal diseases like foot-and-mouth disease (FMD) which rely on stop-movement, quarantine, depopulation, carcass destruction, and limited application of available vaccines, are inadequate to meet the logistical challenges of multilocus outbreaks and to manage the psychological, social, and economic, and trade consequences of disease outbreaks. Safe and economical vaccines with minimal need for re-application and high-throughput modes of vaccine delivery are not readily available for a wide range of important animal pathogens such as some FMD strains, classical swine fever, and Rift Valley fever. Current vaccines are not optimal for differentiating infected animals from vaccinated but uninfected animals. There are also inadequate options for antiviral and antibacterial therapeutics to enable recovery from an animal disease outbreak. Capabilities to recover, assess as safe, and restore large tracts of cropland that are treated with pesticides or “plowed under” during an outbreak are not yet available. Methods and technologies for economical large-scale disposal of contaminated biomass (animals, crops, and food) that minimize environmental, health, and social impacts and for verifiable decontamination and restoration of the agriculture and food infrastructures are inadequate. Personal protective equipment to protect agricultural and food workers against pathogen, toxin, and zoonotic risks is cumbersome and increases the heat-stress burden on the wearer.
- ***Cross-Cutting RDT&E*** – Basic understanding of the biology, pathogenesis, host-pathogen interaction, and epidemiology of animal and plant diseases is currently insufficient for meeting agricultural and biodefense needs. The knowledge gained will contribute to meeting the urgent need to enhance our ability to model infectious disease spread and its impact on animal and plant populations, both generally and for specific diseases. Modern research facilities capable of conducting this advanced research work, conducting countermeasures development, testing, and evaluation, and performing operational diagnostic testing are scarce in the United States. Existing BSL-3Ag biocontainment facilities for animals, plants, and food are in need of repair or replacement, and there are no BSL-4Ag level facilities for studying high-consequence foreign zoonotic diseases of large animals in the United States. For zoonoses, better linkage among the animal, wildlife, and public health communities is needed. In general, better linkages are needed between the animal and wildlife health communities. There is also a critical unmet need for better understanding and modeling of the social, psychological, and economic impacts of disease outbreaks and for developing science-based public and risk communication strategies. Additional education, training, and workforce development is required to enhance the number and capabilities of private practitioners, producers, animal and plant care workers and disaster teams (including veterinarians and plant pathologists), supporting response personnel (e.g., law enforcement, transportation, water, sanitation, and public health), and researchers in order to enhance protection of the agriculture and food systems.

STRATEGIC GOALS FOR 2015

- ***Threat Awareness*** – A fully integrated and government-wide agriculture and food threat assessment infrastructure combining technical and intelligence-based threat, vulnerability, and risk assessment capabilities will be in place, enabling effective biodefense planning by providing a thorough understanding of current and emerging threats and effective anticipation of future threats.

- ***Prevention and Protection*** – “Food shields” will be deployed nationally at all critical food production and transportation nodes to protect the food supply through preventing the introduction of threat agents and detecting, inactivating, and decontaminating threat agents that have been introduced.
- ***Surveillance and Detection*** – A comprehensive national biosurveillance system for public, animal, wildlife, and plant health, as well as food and water which is integrated with the NBIS will be established and will also integrate information from international sources (see also Chapter 1: “Defense of Humans Against Biological Threat Agents”).
- ***Response and Recovery*** – A comprehensive national response and recovery system and countermeasures for deliberate or natural outbreaks of animal and plant diseases or contamination of the food supply will be established.
- ***Cross-Cutting RDT&E*** – A robust infrastructure and knowledge base for animal and plant diseases will be in place to support end-to-end system studies, trained professionals, the development of epidemiologic and economic models of animal and plant diseases and food contamination, and better linkage between animal and public health.

To achieve these capabilities by 2015, the following near-, mid-, and long-term priorities have been developed.

NEAR-TERM PRIORITIES

- ***Threat Awareness*** – Identify gaps in current knowledge and determine critical agent characterization data for highest priority threat agents in the agriculture and food sectors, including effective infectious doses of the agent through various routes including air, food, water, and direct contact and agent viability as a function of time after release and after decontamination. Use these and other data to support formal threat assessments, to construct threat scenarios, and to conduct risk assessments and end-to-end systems studies that enable prioritization of biodefense research and development activities and the development of integrated system defenses. Enhance interactions and collaboration among Federal agencies, the private sector, internationally, and the intelligence community.
- ***Prevention and Protection*** – Conduct vulnerability assessments and systems studies to define and prioritize requirements and to define system architectures and concepts of operations for “food shields” at critical agriculture and food production and transportation nodes. Initiate the design, research, and development of detection technologies, sensors, and physical security methods for these “food shields,” and develop science-based decontamination technologies and procedures. Conduct vulnerability assessments and prioritize prevention and protection requirements for additional animal, crop, and food production and processing systems. Continue to develop methods for effective pasteurization that will destroy pathogens and toxins.
- ***Surveillance and Detection*** – Complete end-to-end systems studies to develop requirements for enhancing the detection, surveillance, diagnostics, and forensics capacities and capabilities of the national animal, plant, and food laboratory networks, as well as those of international systems, as appropriate. Deploy validated diagnostics for FMD, including diagnostics that discriminate vaccinated versus infected animals, and continue to develop diagnostic tests for major plant disease threat agents. Establish an initial strain archive and forensics characterization capability. Develop test protocols and evaluate current field detection devices for agricultural suitability, optimize current assays, and establish standards. Design and initiate implementation of national animal, plant, and food tracking systems. Establish information feeds from the detection, surveillance, diagnostics, and tracking systems to the NBIS, and improve data integration from domestic and international sources. Develop validated methods for detection of the major threat agents in the high risk food matrices in support of the Food Emergency Response Network laboratories, develop a

guaranteed reagent stream that can sustain surge capacity in the event of an attack on the food supply, and have triage protocols in place to confirm the etiologic agent in a foodborne attack.

- **Response and Recovery** – Enhance surge capacity for response to animal, plant, and food emergencies, including the routine and surge capacities of the respective national laboratory networks. Develop and deploy heightened biosecurity equipment and protocols, decision support and crisis planning tools and concepts of operations for scenarios at multiple scales of consequence, including epidemiological and economic models, and conduct interagency exercises across all levels of government and industry. Enhance research and development programs for marker vaccines, new vaccine platforms, rapid vaccine delivery systems, and novel therapeutics that can induce rapid protection against FMD and reduce its rate of spread. Develop methods to track immune responses to FMD vaccination and infection in cattle and swine. Begin protocol validation and testing of current vaccines for rapid protection against FMD and classical swine fever. Enhance pesticide control measures for vectors of high priority animal and plant diseases. Establish pesticide control measures and dedicated breeding programs for disease-resistant varieties for priority pathogens of major crops in the National Plant Disease Recovery System. Identify critical research and development gaps, develop requirements, and initiate rapid prototyping research and development projects for disposal, worker protection, decontamination, and restoration of the animal, crop, and food production systems following large-scale disease outbreaks or food contamination. Conduct feasibility studies of methods for salvaging protein instead of destruction and disposal.
- **Cross-Cutting RDT&E** – Continue basic research on the biology, pathogenesis, host-pathogen interaction, and epidemiology of animal and plant diseases. Develop granular, spatial (geo-referenced) animal disease epidemiological models that are predictive as opposed to retrospective, and initiate development of economic and social models of disease impacts. Develop the programmatic and facility requirements for the National Bio and Agrodefense Facility (NBAF). Develop a national strategy for other critical biocontainment facilities for agriculture and food (including necessary BSL-3Ag facilities for diseases of domestic animals and poultry, foreign plant diseases, and food). Expand programs for education, training, and workforce development to enhance protection of the agriculture and food systems using advanced training technologies to reach a large national audience efficiently.

MID-TERM PRIORITIES

- **Threat Awareness** – Characterize and prioritize key attributes of and conduct risk assessments for additional top priority agriculture and food sector threats, including emerging and second-generation threats (e.g., modified organisms and antibiotic-resistant organisms). Develop an understanding of the potential for, and develop and monitor indicators of, the development of second- and third- generation agents (e.g., engineered agents that are not found in nature). Conduct and use formal threat and risk assessments together with systems studies to guide further and refine biodefense priorities.
- **Prevention and Protection** – Deploy a national architecture of “food shields,” including detection technologies and inactivation systems for pathogens and toxins, at an initial set of critical central food processing nodes. Define and prioritize requirements and define system architectures for “food shields” at additional critical food production nodes, and design and develop the associated detection technologies, sensors, physical security, and decontamination technologies and procedures. Develop additional protective food processing procedures.
- **Surveillance and Detection** – Expand laboratory diagnostics and forensics capabilities for additional high-priority threat agents, including deploying high-throughput diagnostic systems for animal and plant diseases and detection methods for pathogens and toxins

effective in food matrices with improved reliability and lower cost. Expand and strengthen international surveillance, reporting, and response mechanisms. Establish an in-depth forensic strain analysis and associated database and bring it on-line for use. Develop high-throughput facility-based monitoring systems and sampling procedures for critical central food processing nodes, as well as next-generation, high-throughput field detection systems. Develop a strategy for the rapid identification of both emerging pathogens and “unknown” samples. Bring NBIS to full operational capability, with major information feeds from sector-specific agencies, industry, and the national laboratory networks, including domestic surveillance and tracking systems for animals, plants, and food products.

- **Response and Recovery** – Establish robust surge capacity that is able to cope with large scale scenarios for high-priority threat agents.
 - Identify intervention points and develop methods to concentrate efforts on selected critical points for disruption of disease spread for high-priority diseases.
 - Deploy and regularly exercise decision support tools, crisis action plans, and interagency distance learning systems to educate and train personnel for top scenarios at multiple scales of consequence.
 - Integrate geographic information systems (GIS), web-based, and hand-held technologies into emergency response plans at both Federal and State levels. Integrate these efforts with international trading partners.
 - Complete development, testing, and evaluation of vaccines, therapeutics, and efficient delivery systems for rapid protection against FMD in multiple species and deposit them in the NVS at levels sufficient to contain major outbreaks quickly. Test new genetically engineered attenuated FMD virus vaccine platforms and antiviral products that induce early protection against FMD infection and transmission and that do not interfere with rapid diagnostics. Establish prioritized requirements and develop defense strategies for other top foreign animal disease threats.
 - Bring the National Plant Disease Recovery System to full operational capability, with pesticide control measures and disease-resistant varieties of major crops for priority pathogens.
 - Develop capabilities for disposal, worker protection, decontamination, and restoration of the animal, crop, and food production systems following large-scale disease outbreaks or food contamination, including both portable and regionally based disposal or recycling methods.
- **Cross-Cutting RDT&E** – Continue basic research on the biology, pathogenesis, host-pathogen interaction, vector ecology and control, and epidemiology of animal and plant diseases. Identify mechanisms of immune system-mediated protection against FMD and mechanisms to induce specific immune responses to vaccination. Create models of the dynamics of establishment and spread of each disease within potential vectors and hosts present in the United States. Develop or gain access to data needed to transition from conceptual epidemiologic models to refined, specific models that are comprehensive for each disease and that are coupled to models of economic and social impact. Refine the spatial granularity requirements for use in all phases of modeling as well as for emergency response operations. Complete the engineering design and undertake construction of the NBAF, and begin implementation of the strategic plan for the Nation’s other critical biocontainment facilities for agriculture and food. Establish commodity-specific research groups that advise on the development of mitigation, response, and recovery strategies tailored to the production practices and biology of each commodity.

LONG-TERM PRIORITIES

- ***Threat Awareness*** – Characterize and prioritize key attributes of and conduct risk assessments for advanced and emerging agriculture and food sector threats. Conduct and use formal threat and risk assessments, together with systems studies, to guide and refine biodefense priorities for third-generation threats.
- ***Prevention and Protection*** – Deploy “food shields” nationally at all critical food production nodes.
- ***Surveillance and Detection*** – Expand capability for in-depth forensic strain analysis to multiple locations and establish multi-user, web-based knowledge discovery capabilities. Validate high-throughput detection and monitoring systems and deploy them to central food processing nodes and field locations. Develop and deploy detection and diagnostic technologies and systems capable of rapidly identifying both emerging pathogens and unknown samples. Continue to expand and strengthen international surveillance, reporting, and response mechanisms.
- ***Response and Recovery*** – Develop, test, evaluate, and deploy next-generation vaccines and therapeutics for FMD that are safe, inexpensive, and effective in one-to-three days with manufacturing, pre-deployment, and mobilization that is sufficient to handle large-scale outbreaks. Develop, test, evaluate, and deploy diagnostics and countermeasures for other top foreign animal and zoonotic disease threats. Develop ability for rapid immune status assessment and have immune status information available for diagnostic applications and policy decisions. Develop and deploy next-generation emergency responder tools that have improved fidelity, lower cost, and more efficient user interfaces. Establish a comprehensive capability, including deployment of new technologies that enables large-scale disposal, decontamination, and restoration of the Nation’s infrastructures for agriculture and food following large-scale disease outbreaks or contamination.
- ***Cross-cutting RDT&E*** – Continue basic research on the biology, pathogenesis, host-pathogen interaction, and epidemiology of animal and plant diseases. Deploy fully refined, specific, and comprehensive epidemiologic and economic disease models for use by decision makers. Complete construction of and occupy the new NBAF facility, and continue implementation of the strategic plan for the Nation’s other critical biocontainment facilities for agriculture and food.

AGENCIES’ ROLES AND RESPONSIBILITIES

The departments and agencies of the Federal government have been working in their sector-specific areas and as part of Federal government working groups to prepare the U.S. for a potential terrorist attack. The roles and responsibilities of the Federal departments for the Nation’s biodefense (including agriculture and food) have been outlined in the President’s directives concerning *Critical Infrastructure Identification, Prioritization, and Protection*; *Defense of United States Agriculture and Food*; and *Biodefense for the 21st Century*.

As established in these directives, DHS is responsible for coordinating the overall national efforts to enhance the protection of the critical infrastructure and key resources of the U.S., including plant and animal agriculture and food. DHS is also responsible for coordinating the development of an interagency *National Response Plan* (NRP) and National Incident Management System (NIMS), as well as for coordination of Federal resources utilized in response to or recovery from terrorist attacks, major disasters, or other emergencies. The Department of State (DOS) is the designated lead agency for the coordination of international activities related to the prevention, preparation, response, and recovery from a domestic incident.

Sector-specific agencies are also designated to address the unique characteristics and operating models for each sector. The USDA is responsible for agriculture and certain foods (meat, poultry, and egg products); HHS is responsible for public health, healthcare, and foods other than meat, poultry, and egg products; and the Environmental Protection Agency (EPA) is responsible for drinking water and water treatment systems. The Department of Justice (DOJ), while not designated as a sector-specific agency, has the responsibility for reducing terrorist threats and investigating and prosecuting actual or attempted terrorist attacks.

In keeping with these responsibilities, DHS will coordinate with USDA, HHS, DOJ, EPA, and other Federal agencies to ensure that the combined Federal, State, local, and tribal response capabilities are adequate to respond both quickly and effectively to a terrorist attack, major disease outbreak, or other disaster affecting the national agriculture or food infrastructures. Interagency planning and the establishment of interagency agreements necessary for the division of resources and responsibilities are in progress to implement these Presidential Directives.

The Technical Support Working Group (TSWG) has and continues to play a unique integrative role as an interagency rapid prototyping program for combating terrorism technologies (members include DHS, USDA, HHS, DOJ, DOS, Department of Transportation, EPA, and the Intelligence Community). TSWG focuses on projects that rapidly put tools in the hands of users, including those for the protection of food and agriculture. The TSWG Chemical, Biological, Radiological and Nuclear Countermeasures (CBRNC) Subgroup works to identify, validate, and prioritize interagency combating terrorism requirements and deliver technology solutions for detection, protection, decontamination, mitigation, containment, and disposal.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

The Federal government has taken substantial action to expand its capabilities to defend the Nation against attacks on its agriculture. Examples of accomplishments, capabilities, and ongoing activities of the Federal government can be found below.

Department of Agriculture (USDA)

- Established and is expanding laboratory networks for both animal and plant health to detect and report pathogens rapidly and improve response, the National Animal Health Laboratory Network and the National Plant Diagnostic Network.
- Implemented the Emergency Management and Response System which utilizes veterinary practitioner and producer reporting to detect foreign animal diseases.
- Established Area Emergency Coordinators to work closely with State animal health and emergency management officials to improve State and Federal coordination.
- Established the National Veterinary Stockpile (NVS) Steering Committee to help ensure that the decisions regarding composition, inventory, storage, deployment, use, and staffing of the NVS are made based on current threats, the best science, predictive modeling, and the best expert advice available.
- Established the National Surveillance Unit to coordinate and integrate surveillance activities and lead the planning and design of surveillance strategies.
- Established relationships with international trade partners that lead to classified information exchanges, food defense workshops, and drafted a series of food defense principles which were endorsed by the APEC leadership.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

USDA, continued

- Worked with State agencies and stakeholders to develop the National Animal Identification System and began its implementation.
- Conducted and continued research on pathogens and toxins in foods that USDA required for its vulnerability assessments (CARVER + Shock).
- Undertook vulnerability assessments of processed food, livestock and crop production systems which are now guiding the design of countermeasures to protect key nodes in the food chain. The measures include monitoring, detection and surveillance systems, physical security as well as practices applied by industry during processing and transportation.
- Continuing to coordinate closely with the Department of Defense (DoD) and Department of State to ensure the security and integrity of food destined for U.S. military forces overseas and for personnel assigned to embassies, consulates, and other U.S. government facilities.
- Redirected research programs to focus on priority pathogens that pose the greatest threat to the U.S. agriculture to support diagnostic surveillance programs, the discovery of countermeasures, the National Veterinary Stockpile, etc.

Department of Health and Human Services (HHS)

- Completed a vulnerability assessment of the food production systems under its regulatory purview utilizing Operational Risk Management (ORM). Relevant results were communicated to State officials, as well as to sectors of the industry and relevant trade organizations. The Food and Drug Administration (FDA) also sponsored efforts to conduct an in-depth review of ORM and provide a critique on its application to food security and to identify preventive controls, process technologies, and other means to reduce or eliminate the potential threat to FDA-regulated foods.
- Released documents related to food security based on the results of the ORM vulnerability assessment. Each document identifies the types of preventive measures that companies can take to minimize the risk that food or cosmetics under their control will be subject to tampering or to criminal or terrorist actions.
- Refined the initial ORM threat assessments by using the Department of Defense CARVER + Shock Assessment tool for those commodities identified as being of higher concern through the ORM assessment process.
- Training selected industry segments on the use of the CARVER + Shock assessment tool.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

HHS, continued

- Directing its current food defense research agenda toward foods believed to be most vulnerable or attractive to terrorists ("high priority foods") and toward agents that pose the greatest threats to the public.
- Established procedures for administrative detention, including expedited procedures for perishable foods, as required by the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002*.
- Established a final regulation requiring the establishment and maintenance of records by persons who manufacture, process, pack, transport, distribute, receive, hold, or import food in the United States, as required by the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002*.
- Published an interim final regulation requiring submission of prior notice of food (including feed for animals) that is imported or offered for import into the United States.

Department of Homeland Security (DHS)

- Assumed responsibility for operation of the Plum Island Animal Disease Center (PIADC) on June 1, 2003, as required by the *Homeland Security Act of 2002*. Formed a Board of Directors with USDA partners to coordinate research and diagnostic programs on foreign animal diseases at PIADC.
- Established an Agricultural Biosecurity program which includes accelerating the development of countermeasures for foreign animal diseases, disease assessment capabilities, and development and demonstration of diagnostic tests.
- Established two multi-institutional Homeland Security Centers of Excellence: the National Center for Foreign Animal and Zoonotic Disease Defense, led by Texas A&M University and collaborators; and the National Center for Food Protection and Defense, led by the University of Minnesota and collaborators. Each Center is working closely with partners in academia, industry, and government to address potential threats through the development of capabilities for prevention, detection, response, recovery, risk communication, and education.
- Established the National Bioforensic Analysis Center (NBFAC) of the National Biosecurity Analysis and Countermeasures Center (NBACC) that includes a strain repository for selected pathogens and a new forensics capability for foreign animal diseases at PIADC, in order to enhance the capability for forensics and attribution.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DHS, continued

- Leveraging a range of expertise across other Federal agencies, academia, and the private sector to protect animal agriculture as part of the Homeland Security Biodefense Complex; this includes PIADC, the Centers of Excellence, NBACC, the national laboratories, and the Biodefense Knowledge Center.
- Conducted a systems design for, and began implementation of, the National Biosurveillance Integration System (NBIS). This system will integrate information from multiple agencies, as well as domestic and international sources, on the “state of health” of the Nation’s human and agricultural (animals, plants) populations, including environmental monitoring of air, food (domestic and imported, including animal feed), and water, as well as threat and intelligence data.
- Has established the Food and Agriculture Government Coordinating Council, and Sector Coordinating Council, to broaden industry participation, improve information sharing, provide a forum to share best practices, and coordinate public-private agriculture and food defense efforts.
- Established the Agriculture and Food Portal on the Homeland Security Information Network (HSIN) to improve information sharing and collaboration and provide a forum for industry to share sensitive information and best practices.

Environmental Protection Agency (EPA)

- Developed a strategy and research plans to test methods of disposal of large numbers of animal carcasses that might arise from a large-scale agricultural contamination event.

Technical Support Working Group (TSWG)

- Developed and transferred for commercialization a suite of personal protective clothing for use by veterinarians and farm technicians working with animals that are potentially infected with a zoonotic disease.
- Prepared and distributed a database of 78 animal and 22 plant pathogens for use by non-specialists, including an expert assessment of the potential for each pathogen to be used as a terrorist weapon as well as indicators of their use.
- Conducted with HHS a physical security assessment of fresh milk production and distribution in the U.S. and a demonstration of a low-cost technology to improve the security of milk tankers moving between farms and dairies; the report was distributed by HHS to all State and territorial public health and agriculture commissioners.
- Conducted with DoD a physical security assessment of food shipments to military facilities in the European and Central Command theaters of operation and identified specific recommendations for cost-effective enhancement to security.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

TSWG, continued

- Developed distance learning courses for food service managers to improve the security of food warehousing, preparation, and service for military and institutional food service facilities.
- Developing at Kansas State University an extensive “lessons learned” database from agricultural bioterrorism exercises and natural outbreak responses.
- Initiated a competitive solicitation to develop an affordable transportable high capacity incineration and gasification system for the destruction of contaminated animal carcasses and plant material.

National Science Foundation (NSF)

- Conducts research and development programs in ecology and infectious diseases (jointly with HHS), microbial genome sequencing (jointly with USDA), and microbial interactions and processes that build the knowledge base for understanding potential biothreats and suggest approaches to avoid counteract such threats. Supports efforts to generate information about the natural occurrence of potential pathogens in water, soil, and air. A new partnership with USDA will expand microbial observatories to habitats involved in agriculture, aquaculture, and forestry. Is conducting research on novel sensors to detect biological agents.

Federal Government, cooperatively

- HHS and USDA established the Food Emergency Response Network (FERN), a network of government laboratories for the detection of biological, chemical, and radiological agents in food.
- DHS and USDA have developed a joint research and diagnostic strategy for foreign animal disease at PIADC, initially focused on foot-and-mouth disease (FMD), which includes enhanced assays and diagnostics, vaccines and therapeutics, and a new bioforensics capability; USDA efforts are focused on basic research and diagnostics and those of DHS are focused on applied research and advanced development, including expediting the transition of promising vaccine and therapeutics to the private sector.
- HHS and USDA are maintaining the Electronic Laboratory Exchange Network (eLEXNET) to compare, share, and coordinate findings from the laboratory analysis of food samples that are monitored for “traditional” hazards.
- An interagency working group is working with the intelligence community to monitor threats to the Nation’s food supply and to share information across agencies; products or information developed by this group are reviewed and coordinated by DHS and are released to the food sector through established DHS and interagency protocols for clearance and consensus.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Federal Government, continued

- DHS initiated an interagency study for the conceptual design of the National Bio and Agrodefense Facility (NBAF), which will refine the programmatic drivers, requirements and tradeoffs for this next-generation facility, including requirements to meet the current and anticipated needs of the PIADC mission; additional capacity required for foreign animal and zoonotic diseases (as specified in the President's *Defense of United States Agriculture and Food*); and the capability to conduct comparative medicine studies of the same diseases in animals and humans.
- An international initiative on biodefense has been started among the "Group of Eight" (G-8) countries. This includes the creation of a G-8 bioterrorism experts group (co-chaired by the Department of State and DHS), with a major focus on protection of the food supply from deliberate contamination.
- HHS and USDA published final rules for the possession, use, and transfer of select agents and toxins.
- USDA, HHS, DHS, and the Department of Justice have begun a new collaboration with States and private industry to protect the nation's food supply from terrorist threats. The Strategic Partnership Program Agroterrorism (SPPA) Initiative will involve Federal, State, and private industry partners to conduct assessments on food commodities in order to determine security issues from farm-to-table and consider ways to protect our food supply better.
- HHS and USDA developed a web-based course entitled "An Introduction to Food Security Awareness" to increase awareness of the threat of intentional contamination of the U.S. food supply; enable recognition of preventive measures an establishment can take to ensure food security; identify Federal government efforts to ensure the security of the U.S. food supply; and enable recognition of how to encourage food establishments to increase their level of food security.

CHAPTER 3 – DEFENSE AGAINST CHEMICAL THREATS

INTRODUCTION

Protection of our civilian population, emergency responders, military forces, and critical infrastructure from the threats posed by the deliberate use of chemical weapons is a national priority. Until recently, the chemical threat spectrum was limited to the threats posed by chemical warfare agents (CWAs) in a military context and the threats posed by the accidental or inadvertent release of toxic materials in the homeland domain. Now, the chemical threat spectrum has expanded to include CWAs, toxic industrial chemicals (TICs), and non-traditional agents (NTAs). Similar to the complexity of the threat materials themselves is an array of delivery means ranging from traditional battlefield weapons systems to surreptitious scenarios perpetrated on civilians or components of our critical infrastructure. A fully coordinated and cooperative effort is needed to achieve the desired state of readiness and preparedness across the civilian and military complex.

THREATS AND VULNERABILITIES

The chemical threat spectrum has expanded over the past ten years to include three broad classes of toxic materials. Historically, CWAs, including vesicants (e.g., mustard) and the nerve agents, have received the greatest attention due to their use in wartime and the development of effective delivery methods. Terrorist groups have also used them in the past, including the 1995 Aum Shinrikyo sect release of sarin in the Tokyo subway. There continues to be a concern that modern terrorists may have significant interest in classical chemical agents.

The 1984 accidental release of methyl isocyanate in Bhopal, India, demonstrates the threats posed by toxic industrial chemicals (TICs) to the general public. A legitimate concern exists that terrorists may be interested in the release of large amounts of chemicals from industrial sites and during transportation. Further, terrorists may seek more accessible TICs to launch threats against the public until they achieve the capability to develop and deploy CWAs. Recent insurgent use of improvised explosives incorporating chlorine in the Iraq theater reflect the emergence of such tactics.

The final broad class of materials of concern in the chemical threat domain is non-traditional agents. Non-traditional agents comprise an array of materials that have received past interest by foreign entities for potential weaponization as well as materials that do not fall into the previous categories but may present substantial challenges if employed by terrorists. Non-traditional agents are characterized by an array of physical and chemical features that present unique challenges to the development of countermeasures. The level of defensive research and development interest assigned to any given subset of such agents is driven both by intelligence estimates and the challenges they present to defensive countermeasures.

In the past, national security programs focused on a narrow set of chemical threats. The investment has led to military-fielded standoff detectors, personnel protective equipment, and medical countermeasures for a limited set of threats and portion of the population. As the list of threats continues to broaden over time, it is possible that non-traditional agents and emerging threats will circumvent the current detector systems and countermeasures.

Effective medical countermeasures for TICs and many other toxic chemicals are few, due to lack of demand for these countermeasures in the past and the difficult generic problem of protecting tissues after exposure. Hence, most chemical injuries are treated with supportive care.

REQUIREMENTS

Preparedness against current and future chemical threats requires capabilities in four key areas: Threat Awareness and Characterization, Prevention, Attack Warning, and Response and Restoration.

- ***Threat Awareness and Characterization*** – Threat awareness provides a picture of potential threats and their evolution in time and across boundaries toward potential targets. Threat awareness includes definition and description of chemical threat materials that appear to be of interest to adversary groups as well as an assessment of the specific threats these materials pose, how these threats might be presented against targets, and the vulnerabilities these threats exploit. By maintaining vigilant awareness of potential threats, the Nation is able to identify vulnerabilities and act to close them or establish deterrent activities.

- ***Prevention*** – Preventing an attack before it materializes requires the defeat of adversary assets for production, storage, theft/diversion, and delivery of threat materials and the interdiction or disruption of the flow of precursors and finished threat materials. International conventions related to classical chemical warfare agents and precursor materials are intended to reduce the potential for state-sponsored attacks using these materials. However, these international treaties and agreements are neither designed nor able to prevent non-state actors from obtaining or using chemicals for an attack. No conventions are currently in place for TICs and NTAs, though DHS is developing a chemical security regimen to protect the chemical infrastructure and enable surveillance of toxic industrial chemicals across that infrastructure. There are international programs to aid in the prevention of terrorism, but these are not specific to chemical weapons. Prevention also requires detection, surveillance, interdiction, and rendering safe of chemical threats. Tools that enable responders to recognize, identify, and manage chemical threats are essential.

- ***Attack Warning*** – Protection of a target population or infrastructure is improved by the capability to provide warning and notification of a chemical attack. Ideally, an attack warning system should incorporate a sensor system to detect the presence of toxic materials in the environment quickly and reliably enough to allow a response that minimizes the damage caused by those chemicals. Use of detection tools to warn and enable protection is appropriate for facilities, such as buildings and transportation terminals, as well as some outdoor environments where significant numbers of people may be at risk in a toxic chemical release. Some water systems may be vulnerable to attack using chemical materials. Water systems are difficult to protect by physical security alone, and therefore chemical warning systems are needed to protect vulnerable points in the water system.

- ***Response and Recovery*** – The ability to conduct rescue, clean-up, and restoration activities following an attack is a critical requirement for homeland security preparedness. Among the major technology components of a successful response and recovery program are personal protection, medical countermeasures, decontamination tools and procedures, and detection and analysis tools to support immediate response and longer-term remediation activities. Personal protective equipment should include all-hazards protection suitable for long duration and extended reuse that does not impede the operations of the user. Injuries resulting from exposure to toxic chemicals generally evolve quickly and can be immediately life-threatening. A complete medical response would include rapid, effective countermeasures for all priority threats and the knowledge base and guidance that support their use. Decontamination should be effective against the full threat spectrum, environmentally friendly, non-toxic, and non-corrosive to materials. Decontamination procedures should promote rapid and safe restoration of contaminated facilities with a minimum of economic consequences. Ideally decontaminants should operate with a variety of delivery devices. Chemical monitors are of high value to responders in the course of rescue and immediate remediation activities. These capabilities should be engaged through a comprehensive incident management architecture that includes hazard prediction modeling and chemical, biological, and explosives decision support tools. Finally, effective forensic analytical tools will enable attribution of responsibility for an event, as well as identify steps needed to prevent a recurrence.

GAPS

In the past, the national security community has focused on a narrow set of chemical threats. The Federal investment has led to military-fielded detectors, personal protective equipment, medical countermeasures, and decontamination systems for a limited set of threats. As the list of threats increases, greater attention must be devoted to ensure countermeasure technologies keep pace in an expanded target environment that includes the civilian populace and our economic and industrial complex. Significant improvements are required in multiple technology areas to improve our defenses against chemical threats.

Gaps outlined in this document have been identified by an interagency assessment of national research and development programs under the auspices of the Counterproliferation Technology Coordinating Committee (CTCC), and are summarized below.

- ***Surveillance and Detection Technologies*** – An effective deterrent surveillance system for chemical threats would include container monitors. Container monitors must be able to assess quickly the contents of containers against a reasonable expectation of the contents based on operational context of examination. Two classes of detector systems enable detection surrounding a release of toxic chemicals: spatial domain monitors and portable detectors. In both cases, the requirement of a complete capability is to detect, discriminate, and identify all acutely toxic chemical materials in environments containing variable concentrations of background chemicals. Low-cost spatial domain and personal portable monitors with low false-positive response rates capable of detecting broad classes of toxic chemicals must be developed.
- ***Personal Protection*** – There is an urgent need for respiratory and skin (suits, gloves, boots) protection suitable for long-duration wear while doing strenuous work in a range of environments such as those encountered by emergency responders. The systems need to protect against radiological, chemical, and biological threats with the goal of all-hazards protection with reduced heat stress burden on the wearer compared to current equipment. In applications where respiratory protection is provided by masks with filters and in filter protection systems for facilities, improved performance of filters is required across not only classical chemical agents, but also against TICs and NTAs, as well as CWAs in TIC backgrounds. Ideally the protective equipment should be able to be effectively decontaminated for reuse.
- ***Medical Countermeasures*** – A number of prophylaxes and treatments, as well as a limited set of diagnostic tools, exist for the classical chemical warfare agents and are currently approved for use in a subset of the population (healthy adults). Medical diagnosis and treatment capabilities must be extended to a wider variety of chemical threats and must accommodate a wider population including children, pregnant women, and the elderly. Additionally, the treatment of complex injuries, such as chemically contaminated wound care, requires attention. Uncertainty remains about the effects of exposure to sublethal levels of many toxicants. An improved understanding is needed to plan treatments for injured personnel. Plans for the development and potential deployment of medical countermeasures, to include rapid on-scene screening capability to identify those who have been exposed and require treatment, must give consideration to the rapid onset of injury due to chemical exposures.
- ***Decontamination and Restoration*** – Effective decontaminants against the broad spectrum of chemical threats are needed for a variety of operational situations, including challenging locations like building ventilation systems and drinking water distribution system pipes. Ideally, the decontaminants should be non-toxic, non-corrosive, and environmentally benign. Proper waste disposal practices are a critical piece of the

decontamination process. Sampling and detection techniques are required to characterize rapidly the extent of contamination and to monitor progress of the decontamination process. Addressing the target level of decontamination will require the understanding of low-level exposure effects as well as establishment of standards based on these data. Additionally, the capability requires the development of planning and training tools to assist responders and decontamination crews in implementing these new technologies.

- ***Water Systems Security*** – Drinking water systems are spread over many square miles, contain thousands of miles of pipe, have easy public access, and are difficult to protect by physical security alone. Contamination warning systems consisting of multiple components, such as real-time sensors connected to computer systems, public health surveillance systems, data analysis tools, sampling techniques, and a laboratory network for water samples, are needed to provide the most effective long-term protection against contamination, whether intentional or accidental, and the best hope for providing rapid emergency response.
- ***Threat Agent Characterization and Analysis*** – In order to maintain an adequate level of awareness of current and evolving chemical threats, several well-defined activities must be undertaken. Characteristics of current and evolving potential threat agents need to be accumulated and given broader availability to the homeland security domain. Accumulation of such data will enable the performance of risk assessments, identification of vulnerabilities, and guidance of effective countermeasures development. Data needs include physical and chemical properties of important toxicants, as well as their fate in indoor, outdoor, and water environments. Analytical methodologies and process must be developed and sustained to support response activities and forensic quality investigations of chemical attacks. The development of medical countermeasures as well as other countermeasures will benefit from refined understanding of long-term, low-level toxic exposure effects and as well as short-term higher-level advisory levels for the full chemical threat spectrum. Finally, a laboratory response network with capacity capable of analyzing an appropriate number of environmental samples for toxic chemical materials does not exist.
- ***Facilities and Infrastructure*** – There are limited facilities for CWA medical research, development, testing, and evaluation (RDT&E). Surety requirements limit access to neat agents to two sites and only one has approved Good Laboratory Practices capability; dilute agent access is limited as well. This will impact expansion of the research programs and ability to provide collaborative research space to academic researchers engaged in basic science endeavors. As research expands to a broader set of chemicals, proper facilities for exposure of animals under controlled conditions may limit the advancement of research. A new generation of researchers must also become engaged in this arena as the effort to identify novel countermeasures expands. For low dose exposures that may or may not exhibit identifiable symptoms, there is significant laboratory analysis capability and capacity for clinical samples. At this time, HHS has the capability to perform quantitative analysis of human clinical samples for 150 chemicals; for a large incident, current environmental health laboratory resources would be redirected to chemical terrorism analysis response. Expansion of these methodologies to additional agents of concern is needed as additional threats are identified. HHS has disseminated sample collection and analysis protocols to state public health laboratories and continues to train staff and evaluate proficiency on a regular basis. An interagency environmental Chemical Laboratory Response Network (eCLRN) workgroup, which DHS chairs, has been formed and meets regularly to address environmental sampling and analytical chemical warfare agent needs. Assessments to identify the improvements in surge capacity and infrastructure needed to provide the required capability are completed. One issue to be resolved is the development of a mechanism that integrates environmental detection with public health. In addition to validated assay protocols and standards, an information management architecture is needed that connects the environmental laboratories with public health

laboratories. While DHS has committed to an enduring investment to improve and maintain chemical forensics analysis infrastructure, current facilities for proper, forensically acceptable receipt and long term storage of chemically contaminated evidence are inadequate.

STRATEGIC GOALS FOR 2015

To defend our Nation fully against the current and future chemical threats, the goal for 2015 is to create robust chemical countermeasures, including state of the art all-hazard personal protective equipment and early warning detection capabilities. Next-generation, real-time chemical monitors for all current and future chemical hazards will be developed and incorporated in high traffic transit systems, high security risk events, and national landmarks. Medical countermeasures will be produced and forward-deployed, as operationally appropriate, in a manner consistent with the April 2007 HHS Public Health Emergency Medical Countermeasure Enterprise Implementation Plan. Decontamination systems for all chemical hazards will be developed that are more environmentally benign, less toxic and less corrosive, and that can be dispersed through a variety of delivery devices. Complete restoration methodologies will be established, including processes for establishing target “clean” levels as well as the sampling and analytical technologies required to support them. Supporting operational capabilities will include fully functioning, interagency-coordinated, chemical analysis, characterization, and assessment.

NEAR-TERM PRIORITIES

- ***Threat Characterization*** – Conduct analyses of risk to the domestic population due to the full range of chemical threats, to include risk-based prioritization of chemical threats to guide countermeasure investments. Complete the development of data describing the impacts of exposure to low levels of highly toxic chemical hazards and the environmental fate of such materials, increasing the level of attention to NTAs.
- ***Sampling and Analysis Methods*** – Develop and validate methods for the sampling and analysis of all types of surfaces and materials and other environmental matrices contaminated with chemical threat agents, including drinking water distribution system components. Sampling procedures will be integrated with appropriate analytical procedures.
- ***Environmental Laboratory Response Network*** – Establish an Environmental Laboratory Response capability capable of addressing the full spectrum of chemical hazards. The network will be based on membership criteria consistent with the Integrated Consortium of Laboratory Networks and will be supported by robust analytical protocols for analysis of environmental samples.
- ***Mobile Laboratory*** – Demonstrate a mobile high-throughput analytical laboratory to permit on-site analysis of large numbers of samples on a daily basis to support identification of chemically contaminated areas as well as follow-on remediation efforts.
- ***Next Generation Firefighter Protective Gear*** – Complete certification of new protective gear for firefighters that integrates chemically protective layers into the protective matrix. Redesigned interfaces and closures should have dramatically reduced leakage while maintaining a rapid-donning capability and without compromising existing protection from flame, hot gases, and water. Certification should be to The National Fire Protection Association Standard 1971 on Protective Ensembles for Structural Fire Fighting and Proximity Fire Fighting, approved in June 2007, which includes a chemical, biological, and radiological protection option.

- ***Improved Personal Protective Equipment*** – Explore the development and transition for commercialization improved personal protection equipment that is more durable, can be worn longer, and is less burdensome for responder applications in CWA, TIC, and NTA environments.
- ***Infrastructure for Testing NTA Countermeasures*** – Construct a chamber for testing and evaluation of non-medical countermeasures to non-traditional chemical agents.
- ***Decontamination Methods***– Evaluate existing fielded decontamination methods and procedures. For contaminants of concern, apply promising decontamination methods and technologies that are currently unproven. Capability will address all classical chemical warfare agents, non-traditional agents, and persistent toxic industrial chemicals.
- ***Standards*** – Work with standards-setting organizations in industry and government to establish performance-based standards for detection, protection, and decontamination systems to focus development and procurement actions at all levels. Develop risk management approach to define personal protection and decontamination standards that inform cleanup of contaminated areas.
- ***Forensics*** – Develop a chemical forensics infrastructure supported by enduring investment, to include adequate space for proper receipt, analysis and storage of contaminated evidence. Develop methodologies to conduct conventional forensics on chemically contaminated evidence.

MID-TERM PRIORITIES

- ***Threat Characterization*** – Complete characterization of all current and near-term anticipated threats.
- ***Environmental Laboratory Response Network*** – Complete review and approval of comprehensive set of labs for membership. The network will be accredited through an interagency-agreed process and will be supported by robust analytical protocols for analysis of environmental samples.
- ***Mobile Laboratory*** – Deploy for use by appropriate agencies. Develop prototype to analyze non-traditional agents.
- ***Improved Detection Tools*** – Transition for commercialization and field a set of improved detection tools. Develop and commercialize network-capable detectors for use in building protection systems and by responders. These tools will address a broader set of agents at lower false response rate than currently available chemical detectors. Demonstrate a detector to monitor for surface contamination by low-volatility agents.
- ***Rapid Non-Intrusive Container Monitor*** – Demonstrate a rapid non-intrusive container monitor to enable effective portal monitoring of suspicious cargo, passenger baggage, and packages.
- ***Medical Countermeasures*** – Identify available medical countermeasures that can be broadly used in various subsets of the population, including products already developed for military use. Identify pharmaceutical products that may have additional direct applicability in the specific treatment of chemical injuries.
- ***Decontamination*** – Demonstrate an effective decontamination system that is environmentally benign, non-toxic and non-corrosive, and that can be dispersed through a

variety of delivery devices. Capability will address all classical chemical warfare agents, NTAs, and persistent toxic industrial chemicals. Develop and demonstrate procedures for decontamination of humans.

- **Water Contaminant Detector** – Develop a contaminant detection system for water security to detect an array of specific chemical and other contaminants as well as abnormal water quality parameters that may be indicative of intentional or accidental contamination of the water system.
- **Standards** – Evolve standards in a timely manner in response to new threats, to enable the use of new technologies, and to incorporate lessons learned from operational experience.

LONG-TERM PRIORITIES

- **Chemical Contaminant Detection System for Water** – Demonstrate and transition for commercialization the contaminant detection system for water security.
- **Improved Detection Tools** - Demonstrate a warning sensor for low-volatility agents.
- **Rapid Non-Intrusive Container Monitor** – Transition for commercialization and procurement the rapid non-intrusive container monitor to enable effective portal monitoring of suspicious cargo, passenger baggage, and packages.
- **Decontamination** – Transition the developed decontamination methods to commercial Government approved decontaminants. Capability will address all classical chemical warfare agents, NTAs, and persistent toxic industrial chemicals.
- **Mode of Toxic Response Detector** – Develop toxic chemical detection devices that discriminate by mode of toxic response. Instead of detecting known toxic chemicals, these devices will detect hazardous chemicals using sensing mechanisms that replicate physiological responses and thus detect all hazardous chemicals without prior characterization.
- **Future-Generation Medical Countermeasures** – Develop medical countermeasures for chemical toxicants as prioritized by risk assessments and material threat determinations.
- **Personal Protective Equipment** – Transition for commercialization broad-spectrum expedient protective devices for the general public. Enhanced technologies will enable cost-effective, broad-spectrum protection with reduced burden on the wearer.

AGENCIES' ROLES AND RESPONSIBILITIES

Department of Defense (DoD)

- Develops military standards for chemical and biological defense technologies. As such, DoD develops a broad range of both medical and non-medical defense capabilities to counter the effects of chemical warfare agent use against our forces abroad and in the homeland. DoD maintains a robust laboratory infrastructure for conducting chemical defense research, development, test, and evaluation activities. DoD laboratories play an important role in developing and testing new capabilities in chemical detection technology, computer modeling and simulation of agent release and dispersion, individual protection (medical and non-medical), collective protection, and decontamination. The DoD laboratory infrastructure is leveraged to support other DoD homeland defense activities, as well as the chemical defense efforts of other government agencies. DoD activities that contribute to the protection of the homeland against chemical terrorism include Guardian Installation Protection Program (IPP) and the National Guard WMD Civil Support Teams. In addition, development of technologies and procedures to identify and defeat targets outside the Nation are largely the responsibility of DoD and allied components.

Department of Health and Human Services (HHS)

- Holds responsibility for civilian human health-related research and development activities relating to medical countermeasures to emerging terrorist threats. Basic research on mechanisms leading to injury caused by chemical agents, and on elucidating processes that support recovery creates a critical knowledge base for medical countermeasure development. The Department is responsible for regulatory oversight and licensure of medical countermeasures, as well as providing technical support role in validating animal models and assays. HHS has a key role in the determination of requirements and acquisition of medical countermeasures through Project BioShield, and its other roles include human clinical diagnostic capabilities, educating health providers, addressing operational issues in responding to adverse health incidents, and leading the development of the Strategic National Stockpile. HHS has the responsibility for approval of human decontamination approaches.

AGENCIES' ROLES AND RESPONSIBILITIES, CONTINUED

***Department of
Homeland Security
(DHS)***

- Addresses all non-medical countermeasures including systems analyses, chemical detection and characterization, response and recovery, forensics, and domestic operational demonstration programs. The Department is responsible for coordinating Federal activities in preparation for and response to terrorist attacks. In addition, DHS has the lead in conducting the homeland threat assessment for chemical agents and works with HHS to inform development and acquisition priorities for medical countermeasures for the civilian community through the conduct of Material Threat Assessments. The Department is responsible for establishing a chemical security regimen to protect the chemical infrastructure and enable surveillance of toxic industrial chemicals.

***Department of
Justice (DOJ)***

- Serves as the lead agency for criminal investigations of terrorist acts or terrorist threats and intelligence collection activities within the United States. DOJ is responsible for the collection, forensic analysis, and attribution of forensic evidence for interdiction purposes and investigations following events.

***Environmental
Protection Agency
(EPA)***

- EPA shares responsibility with DHS for the detection, decontamination, and disposal of chemical agents and residues used in terrorist attacks on civilian infrastructure and places. Under the National Response Plan, EPA is the lead for Emergency Support Function 10- Oil and Hazardous Materials (including chemical, biological and radiological) response. It is also lead Federal agency for protecting water systems from terrorist attack. Other major components of EPA program are development of guidance and risk assessment methodologies to expedite restoration. EPA systematically studies near and commercially available decontamination, water treatment, and detection technologies in its Technology Testing and Evaluation Program.

***Technical Support
Working Group
(TSWG)***

- Supports an interagency rapid prototyping program for combating terrorism. It focuses on projects that put tools in the hands of users. The TSWG Chemical, Biological, Radiological, and Nuclear Countermeasures (CBRNC) Subgroup works to identify, validate, and prioritize interagency chemical, biological, radiological, and nuclear combating terrorism requirements and deliver technology solutions for detection, protection, consequence management, and information resources.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Department of Defense (DoD)

- Established a comprehensive installation protection program that will equip selected DoD installations with enhanced chemical and biological detection and consequence management capability over the next five years.

- Designed, integrated, and built state-of-the-art modular laboratory trailers.

- Established, equipped, trained, and certified National Guard Bureau Weapons of Mass Destruction-Civil Support (WMD-CST) teams.

- Developed two enzymes, now commercially available, that decontaminate certain nerve agents and pesticides.

- Obtained Food and Drug Administration (FDA) approval to use pyridostigmine bromide as a pre-treatment for the nerve agent Soman, which is the first countermeasure to receive FDA approval under the “animal efficacy rule.”

- Demonstrated efficacy of vaporous hydrogen peroxide for chemical agent decontamination at the chamber scale and performed an initial full-scale building demonstration.

- Is planning the next round of chemical agent decontamination efficacy chamber testing and another full-scale building demonstration with vaporous hydrogen peroxide using further improvements to hardware and application methods.

- Developed a nerve agent pretreatment candidate based on use of a bioscavenger.

- Established a collaborative research facility that performs chemical agent exposures for researchers from DoD, academia, industry, and other non-DoD organizations.

- Is performing research on cyanide therapy and diagnostics, improved nerve agent treatments, mustard therapy, and neuroprotectants, and a treatment effective for all nerve agents transitioned into accelerated advanced development.

- Is investigating FDA approval for expanded indications for an anticonvulsant that crosses the blood-brain barrier to be used against nerve agents.

- Constructed a new state-of-the-art surety facility dedicated to work exclusively with chemical warfare agents.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DoD, continued

- Maintains a laboratory alliance with Department of Health and Human Services (HHS) labs for confirmatory analysis of CWA exposures.
- Have major, ongoing programs to assess the physical and chemical interactions and fate of chemical warfare agents with militarily significant environmental surfaces and the toxicological impact of long-term, low-level exposure to our forces.
- Established and maintained the Chemical and Biological Forensics Analytical Center that is available for use by other agencies.

Department of Health and Human Services (HHS)

- Implemented the Strategic National Stockpile CHEMPACK program for forward deployment of antidotes to chemical nerve agents.
- Published the “Animal Efficacy Rule” to allow for approval of countermeasures when efficacy cannot be ethically or feasibly demonstrated in humans.
- Expanded neurological research programs, including investigating nerve agent effects in the brain, genetic factors for increased susceptibility to nerve agents, and a combinatorial neuroprotective drug therapy.
- Established a chemical Laboratory Response Network to enable the analysis of a broad range of toxic chemical materials, including chemical warfare agents or their metabolites, in clinical samples.
- Conducts pharmacokinetic studies on metabolism of CWAs and other chemicals of primary concern.
- Developed a Strategy and Implementation Plan for Public Health Emergency Medical Countermeasure programs, which address chemical threats to national security.

Department of Homeland Security (DHS)

- Developed and transitioned to local government ownership prototype networked subway chemical agent detection systems in three cities.
- Developed and commercialized a broad spectrum decontaminant with efficacy in foam-based applications.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DHS, continued

- Initiated development of a mobile high-throughput analytical laboratory.
- Initiated development of networked detector systems for building protection and responder applications.
- Developed a rapidly deployable chemical detection system.
- Initiated development of concepts for an expanded chemical Laboratory Response Network to enable analysis of environmental CWA contamination.
- Established the DHS Chemical Security Analysis Center to serve as repository of chemical hazard data and conduct risk analyses of chemical threats
- Initiated a demonstration program aimed at developing concepts for effective remediation of a high-traffic transit facility, to include contamination assessment/mapping, decontamination, and sampling approaches.
- Initiated development of capability to monitor for contamination due to low-volatility chemical agents.
- Completed development of an All Hazards Sample Receipt Facility for preliminary analysis of unknown samples.
- Completed the first Chemical Terrorism Risk Assessment to enable ranking of hazardous chemicals across a broad array of scenarios

Department of Justice (DOJ)

- Created the Chemical and Biological Sciences Unit within the Federal Bureau of Investigation (FBI) Laboratory for forensic analysis of chemicals and other hazardous materials in incidents involving chemical or biological materials, incorporating a hub-and-spoke network of partner laboratories to perform specialized analysis of evidence.
- Created and maintained the Hazardous Materials Response Unit within the FBI Laboratory to conduct scientific and technical threat assessments and to provide on-site technical support, monitoring, detection, and evidence collection capability and safety oversight at crime scenes involving the use, or suspected use, of chemical, biological, radiological, or nuclear (CBRN) materials.
- Provided standby response capability for scientific and technical threat assessments and collection of hazardous CBRN evidence in support of National Security and other Special Events.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DOJ, continued

- Created the Scientific Working Group for Forensic Analysis of Chemical Terrorism.
- Established WMD coordinators in all FBI field offices.
- Established, equipped, trained, and maintained Hazardous Materials Response Teams in FBI field offices to respond to events involving hazardous CBRN materials.
- Established and maintained a national outreach program with the chemical industry.
- Provides scientific representatives to other US Government agencies pertaining to incident response and scientific analysis of CBRN materials.

Environmental Protection Agency (EPA)

- Establishing an all-hazard, all media Environmental Laboratory Response Network (eLRN), including method development and validation.
- Evaluated and selected Federal and State fixed laboratory candidates to conduct environmental CWA analyses as part of a DHS-led interagency evaluation panel.
- Collaborated with DHS to refine design of and establish performance criteria for a mobile high-throughput analytical laboratory.
- Initiated EPA's chemical surety program with DoD to access chemical surety standards (both neat and ultra-dilute) for research and development and calibration of instrumentation and quality assurance purposes, respectively.
- Staffing a new National Decontamination Team to provide scientific and engineering expertise for decontaminating buildings, building contents, and critical infrastructure contaminated by WMDs
- Developing Decontamination Portfolio for chemical, biological and radiological agents to include information on Containment, Health and Safety, Decontamination Methods, Dispersion, and Risk and Toxicology.
- Added 30 chemical compounds and data to the airborne chemical detection platform, ASPECT, with increased spectral identification of compounds and upgraded video capability for improved georectification .

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

EPA, continued

- Developed emergency response tools for water utilities, including preparedness guidance and response protocols for managing chemical contaminants.

- Coordinating the development of a contaminant warning system for drinking water, consisting of real-time detectors, sampling procedures, and data analysis tools.

- Evaluating the performance of technologies related to contamination detection systems, point-of-use (POU) drinking water treatment, decontamination and wastewater treatment

- Performed research on solid, liquid, foam, gel, vapor and gas decontamination agents for use in the aftermath of a WMD incident using CWAs.

- Systematically evaluating technologies for the decontamination of indoor and outdoor materials contaminated with CWAs and TICs

- Developing risk-based, short-term exposure advisory levels (e.g., Acute Exposure Guideline Levels (AEGLs)) for chemical contaminants of concern including CWAs and TICs

- Developed methods for site-specific, risk-based indoor cleanup goals for chemical contaminants of concern including CWAs and TICs.

-

- Evaluated the persistence of CWAs and TICs on building materials at controlled indoor conditions.

- Developed an online Decision Support Tool to aid in the decision-making process for waste disposal activities resulting from restoration of critical infrastructure after a chem./bio/radiological attack.

Technical Support Working Group (TSWG)

- Evaluated, modified, qualified, and supported large-scale government agency procurements of three emergency escape respirator products. Developing improved supplied oxygen and low-profile escape respirators.

- Developed and transitioned for commercialization new chemical protection suits to include the first suit to meet National Fire Protection Association (NFPA) Standard 1994 for Class 2 chemical protection.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

TSWG, continued

- Developed, tested to HHS's National Institute for Occupational Safety and Health (NIOSH) CBRN Standards, and transitioned for commercialization a rehydration system for use with civilian respirator systems.
- Developed and commercialized a kit for training security and response personnel in the recognition of chemical and biological threat agents and to evaluate effectiveness of personnel decontamination training exercises.
- Developed and published science- and consensus-based best practices and guidelines for the decontamination of large numbers of civilian personnel after an attack with CWAs or TICs.
- Installed the first distributed chemical sensor based on fiber optics with reactive coatings for wide-area and facility monitoring for selected CWAs and TICs.
- Completed laboratory and user-acceptance testing of fire fighter protective ensembles with improved integrated protection against CWAs and TICs meeting the requirements of the Chemical, Biological and Radiological Option of NFPA Standard 1971 on Protective Ensembles for Structural Fire Fighting and Proximity Fire Fighting.
- Initiated development of capabilities to improve the design, safety, and effective utilization of response personnel to include bomb technicians in protective clothing and for broad-spectrum chemical and biological decontamination.
- Initiated testing to determine dermal toxicities of selected industrial chemicals to support development of risk based permeability protocols and standards for personal protective equipment.

Federal Government, cooperatively

- Is coordinating Federal investments and planning toward the full spectrum of medical countermeasures via the recently established Public Health Emergency Medical Countermeasures Enterprise, under the leadership of the HHS Assistant Secretary for Preparedness and Response. Chemical countermeasures are being addressed through two new working groups.
- Established the interagency Integrated Consortium of Laboratory Networks, under leadership of DHS Science and Technology Directorate, to identify and fill gaps in the Nation's laboratory response capability, and to promote overall coordination of laboratory response assets against all hazards.

CHAPTER 4 – DEFENSE AGAINST EXPLOSIVES AND WEAPONS

INTRODUCTION

An examination of the catastrophic and destructive terrorist attacks throughout history shows that conventional explosives and weapons predominate as terrorists' weapons of choice. Given the low expense, ready availability of materials, and relatively high chance for successful execution, terrorists will continue to make use of conventional attacks. This chapter addresses the mission to develop technical capabilities and procedures for efficient detection, interdiction, and mitigation of the consequences of terrorist use of explosives and weapons in attacks against the population and critical infrastructure in the United States. The threat from explosives is the primary focus for this chapter.

The strategic objectives for defense against explosives and weapons are:

- Reduce the risk of a successful attack on critical infrastructure, including all forms of transportation;
- Reduce the risk to the population from explosive devices;
- Detect and interdict the illicit movement and use of explosives and explosive devices within or inbound to the United States; and
- Safely, efficiently, and effectively manage suspect and actual IEDs of all types when discovered.

Tactics include enhancing awareness, prevention, detection, protection, and response to attacks. Awareness can be considered to include background screening, intelligence gathering and dissemination, risk analysis, training, and policy and procedural changes in tactics. Prevention is heavily focused on the detection of small and large explosive threats, whether carried on the person, in baggage or backpacks, vehicle-borne, or placed on-board modes of transportation as cargo. Protection is primarily the employment of materials and procedures to lessen or mitigate the effect of an attack.

This chapter focuses on technology solutions, including canines, in the form of products, procedures and best practices. Although the entire system-of-systems is addressed, this chapter primarily focuses on prevention, protection, and response.

THREATS AND VULNERABILITIES

Explosive attacks can be carried out by multiple means, such as suicide bombing or leaving behind explosive devices in baggage or cargo or in populated areas. Bombs can also be vehicle-borne, using either cars or trucks. Threats are typically categorized by the following: suicide bombers, leave-behind bombs, or vehicle bombs. These attacks can be carried out against civil aviation, mass transit systems, public buildings and gatherings, national symbols, ports, intermodal cargo, transportation, and other critical infrastructure.

Key vulnerabilities include insufficient security measures to protect the Nation's population, infrastructure, transportation systems, and vast territorial borders. In addition, there is insufficient physical security for preventing explosives, or improvised explosives and their component materials from falling into terrorist or criminal hands. The domestic focus of countermeasures to explosives attacks has been directed primarily at the threat to civil aviation. Following attacks in Oklahoma City, the U.S. has increased focus on vehicle bombs. The government must now shift its focus to deal with the threat presented to other modes of transportation and fixed targets. Current U.S. communications infrastructure and widespread use of radio-frequency devices offers a prime mechanism for terrorists to exploit. The government must now shift gears to deal with threats beyond those the U.S. has experienced in the past.

Depending on the target, the quantity and type of explosive needed can vary significantly. Explosives range from military- and commercial-grade to homemade devices concocted from recipes that can be found on the Internet. The IED can either be sensitive if the carrier will detonate the device or robust if the device

is to be shipped or left behind. Also, the explosives device may enter the vulnerable area assembled or in a distributed fashion, for the “bomb-maker” to assemble after passing through screening.

There are emerging threats in the explosives area which require an examination of the total breadth of explosives that can be used to damage the Nation’s infrastructure, including hundreds of possible improvised, or no-longer produced, commercial or military explosives. With very few exceptions however, a common pattern of these potential threats can be seen. All contain either as a mixture or in one molecule both an oxidizer and a fuel. The presence of high levels of nitrogen, oxygen or chlorine is often a strong indication of a threat. It does not matter if terrorists obtain ammonium nitrate to mix with fuel, commercial or military explosives, or if they undertake a complex and potentially dangerous chemical syntheses, the product which is ultimately capable of doing great harm will contain high levels of oxygen, nitrogen, or chlorine. As technologies are fielded to address today’s threats, additional methods must be developed to identify these broad categories of oxidizers.

REQUIREMENTS

U.S. government agencies have different roles in providing security for the homeland. In some cases it is the government’s responsibility to detect and mitigate threats. In other cases, the government provides leadership, regulation, guidance, and intelligence to State and local authorities to enhance security.

A strong and effective national defensive capability against the illegal use of explosives and weapons requires the development of technologies that detect, prevent, and protect against the use of these threats. The following capabilities are the necessary foundational components for this national defensive capability:

- Ability to detect, interdict, respond, and mitigate the consequences from leave-behind bombs or suicide bombers approaching high profile targets and densely populated areas;
- Ability to detect, interdict, respond, and mitigate the consequences from vehicle bombs to protect high profile targets;
- Ability to detect, interdict, respond, and mitigate the consequences of explosives and weapons on aviation (domestic and foreign inbound) passengers and carry-on baggage;
- Systems able to detect and interdict explosives in cargo;
- Technologies for detection and safe disabling of IEDs in urban and national transportation systems; and
- Detection of explosives and explosive-related material through the use of a comprehensive, specialized search system-of-systems, including trained personnel, canine units, integrated technology, and follow-on forensic analysis.

GAPS

There are limited or insufficient abilities to detect and interdict suicide bombers and explosives and weapons on people and in vehicles. Techniques and technologies for the detection of truck bombs have been developed and are being used in a limited fashion, but they are too costly and slow to address our broad national threat. Canines are deployed at some airports and Federal building parking facilities, but many locations remain unprotected. While it is possible to harden structures, there is a lack of cost-effective methods to perform this task for the government and private sector.

In addition, there are few effective means to detect, track, or neutralize certain classes of explosives and improvised explosive devices. Another key gap is in the area of comprehensive forensics, which includes attribution capabilities for explosive devices. Although there are some technologies to harden structures, there is a lack of cost-effective methods to perform those tasks for the government and private sector.

In the field of explosives detection, many of the current capabilities were developed for aviation security, in particular to screen checked baggage. These fielded explosives detection systems work well. However, they are large, expensive to procure, expensive to integrate, have considerable nuisance alarm rates, and the regular occurrence of false alarms requires considerable time and resources for resolution. Canines trained in explosives detection are widely used, but their breeding, selection, and training remains more of an art than a science. For targets other than government facilities and aviation transportation, currently deployed capabilities include canines for detection.

There is limited emphasis on screening passengers for explosives, and few resources in the civilian sector are directed to address explosive attacks outside the aviation arena. Even within civil aviation, screening of passengers, their carry-on items, and air cargo has room for improvement. Moreover, the current terrorist threat may include explosives not considered in past threat analyses and therefore not included in existing detection criteria. Most importantly, targets other than commercial aircraft have been attacked and will continue to be threatened. These targets include rail and other modes of transportation, public buildings and other fixed facilities, and gatherings of people.

Surveillance using closed-circuit television (CCTV) and human observation provides some level of prevention by the detection of suspicious behavior and an opportunity to respond quickly. Physical security around infrastructure targets of interest provides a degree of access control. Additionally, an awareness campaign, especially for the transportation sector, is underway in the form of public announcements and posters to provide guidance to passengers if suspicious baggage or behavior is detected, but in all of these areas more can and needs to be done.

Increasing sophistication of improvised explosive devices on people, packages, and vehicles poses new challenges to civilian bomb squad responders and military explosive ordnance disposal personnel. There are currently few tools available for recognition, threat assessment, intelligence dissemination, diagnosis, personnel protection, remote manipulation, disablement and disruption, and forensic analyses. Many solutions have been developed to mitigate blast effects against buildings and personnel. However, they are not yet applicable to all structures, threats, and operational scenarios, and the implementation of solutions that are available is not widespread. In particular there are a limited number of solutions for general transportation and infrastructure scenarios. These solutions include explosives containment units that have been deployed to deal with suspicious baggage and surveillance cameras to store images in case of breach of security in various transportation infrastructures. Additionally, force presence at checkpoints and public service announcements increase deterrence and awareness at vulnerable and critical facilities. There is also a requirement, using actionable intelligence, to conduct specialized search operations at potential bomb-making locations to find explosive materials, detonation devices, and tools that can lead to the arrest or capture of IED makers.

STRATEGIC GOALS FOR 2015

The goal for 2015 is reliable protection from attacks from suicide bombers, vehicle bombs, and leave-behind bombs within an affordable system to detect, prevent and mitigate threats without impeding the flow of commerce and other traffic. Defense against explosives and weapons includes the prevention of, protection against, and response to domestic attacks against civilians, national assets, and critical infrastructure. Attacks against civilians will be considered at places of mass congregation, such as shopping malls, amusement parks, and transportation terminals. A large emphasis has been placed on the prevention of an explosives attack against the transportation infrastructure and passengers, but this must be expanded.

Other scenarios that will be addressed include bombing of national symbols and Federal buildings or attacks on ships in rivers, harbors, restricted waters or intracoastal waterways that can have significant impact on port operations and economic impact via the flow of goods throughout the country. Near-term steps will focus on pilot testing commercially available systems and initiating the development of many capabilities that are currently unavailable. Many systems that contribute to a national protection capability

will be pilot tested in the FY 2007 – 2010 time frame in more primitive forms, with the aim of deploying fully mature, cost-effective systems by 2015.

NEAR-TERM PRIORITIES

This program will produce and pilot instrumentation, configurations, methods, and training that will enable the deployment of systems. The program will effectively counter threats posed by conventional and improvised explosives to the Nation's transportation system, civil aviation system, buildings, critical infrastructure, and general public.

Technical capability, efficiency, and operational utility are critical factors in the applicability of solutions. The development and deployment of solutions to satisfy these requirements will be evolutionary; it is anticipated that interim solutions will be available in the near term for many of these requirements; those solutions will be upgraded or transitioned after their lifecycle to become more capable, robust, and cost-effective. For example, portable versions of technologies will be necessary to prevent and mitigate incidents at temporary high profile locations.

- ***Civil Aviation Security*** – Develop and pilot new instrumentation and methods at airport checkpoints to detect explosives carried on the person or in carry-on items. Complete development of new explosives detection systems for checked baggage; develop configurations and concepts of operations that will significantly improve checked baggage screening efficiency, and pilot resulting systems. Develop and pilot integrated systems for the detection of improvised explosives devices shipped as air cargo.
- ***Vehicle-Borne Threats*** – Develop a system that provides the capability to detect and identify threats in cars or trucks at remote entry points. Develop more efficient training tools and methods for explosives-detection canines and their handlers.
- ***Personnel Screening*** – Develop an advanced capability to screen people at checkpoints for explosives.
- ***Reduce Infrastructure Blast Debris Hazards and Structural Collapse*** – Develop new techniques and vulnerability assessment tools for shock and damage assessment and mitigation. Develop advanced building design and refortification methods.
- ***Emergency Responders*** – Develop improved detection and diagnostics capabilities to mitigate hazards associated with suspect packages. Develop and demonstrate an advanced remote ground (robotic) system that will detect, identify, access, diagnose, and isolate explosive devices for emergency responder handling
- ***Technology Community*** – Develop standards for systems capabilities. Develop and foster a qualification and certification resource within the Federal community to enhance system quality by standardizing testing practices and ensuring integrity of tests and results.

MID-TERM PRIORITIES

Many operationally suitable solutions will require additional resources and time to develop and evaluate.

- ***Civil Aviation Security*** – An adjunct to the previously noted civil aviation protection goals will be the development of practical techniques to harden aircraft to be used in conjunction with detection methodologies.
- ***Other Transportation Modes*** – Develop concepts of operations and instrumentation to protect passenger-carrying conveyances (other than commercial aircraft) such as buses, rail, ferries, and cruise ships. Develop concepts of operations and instrumentation for protecting the maritime and land cargo infrastructure from the threat posed by large amounts of explosives in cargo containers.
- ***Vehicle-Borne Threats*** – Develop and pilot an integrated system for the detection and interdiction of vehicle bombs before they reach their targets (e.g., buildings, bridges, tunnels, other critical infrastructure, and public gatherings). Develop and begin to implement national architectural standards for blast-tolerant public building design. Exploit the improved understanding of olfaction, neurophysiology, and genomics to develop improved breeding, selection, and training methods and tools for canines in the area of explosives detection.
- ***Personnel Screening*** – Develop and validate instrumentation, methods, and training to identify and interdict suicide bombers.
- ***Emergency Responders*** – Develop and demonstrate an advanced remote ground (robotic) system that will detect, identify, access, diagnose, and render safe or recover explosive devices
- ***Technology Community*** – Reduce system and operational costs, therefore increasing the availability of technologies for the next generation of systems. Integrate system capabilities to reduce impact on operations, such as inconvenience and reduced throughput.

LONG-TERM PRIORITIES

- ***Standoff Detection On-The-Fly*** – Explosive detection at a standoff distance and as the target is moving would provide operational flexibility and enhanced security. The applicability of technologies to detect explosives is currently limited to operations that provide a controlled access point for people, baggage, vehicle, or cargo screening. At those access points, the speed of the interrogated object can be controlled, and the results of the screening can be managed appropriately. The controlled access point in some cases can be remotely monitored and activated, but in other cases the locations are closely tied to the vulnerable target for logistical reasons.
- ***Explosives Marking*** – From a systems viewpoint, reducing the availability of and increasing the detection capability for explosives would be beneficial. Specifically, agents to mark explosive device components would provide a better opportunity to detect the explosive device. Marking agents for explosive device components would be useful if those agents met technical criteria such as limited effect on explosive capability

for commercial purposes, environmental acceptability, cost, and safety in manufacture and use. These markers would be developed and assessed as effective contingency measures if the threat level were to increase. Research has been conducted on marking agents to eliminate the degradation of performance in the explosives to which they are added.

AGENCIES' ROLES AND RESPONSIBILITIES

HSPD-19 requires, “The Secretary of Homeland Security, in coordination with the Attorney General, the Secretary of Defense, and the Director of the Office of Science and Technology Policy, shall coordinate Federal Government research, development, testing, and evaluation activities relating to the detection and prevention of, protection against, and response to explosive attacks and the development of explosives render-safe tools and technologies. The heads of all other agencies that conduct such activities shall cooperate with the Secretary of Homeland Security in carrying out such responsibility.”

HSPD-19 establishes a national policy and call for the development of a national strategy and implementation plan on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States. The DHS Office of Bomb Prevention (OBP) and DOJ, represented by the FBI, are partnered to lead the effort to develop a national strategy and implementation plan. HSPD-19 identifies eleven specific components; three information inventories, one assessment of assets and current capabilities to determine capability gaps, and final recommendations and consolidation of findings. The DHS-IEDWG, chaired by the OBP, is to develop a common understanding of roles and responsibilities with respect to bomb prevention, assist the Office of Infrastructure Prevention to provide a single voice for intergovernmental bomb prevention activities, articulate the DHS position, role, and leadership in prevention and response, and aid in the development and implementation of the National Strategy of Bombing Prevention. The final HSPD-19 report that described the national strategy for IEDs was presented to the White House in mid July.

Considering the prominence of the use of explosives to attack civilian populations worldwide, many U.S. government agencies, as well as numerous international partners and the private sector, have collaborated to develop solutions. These include the DoD, DOE, DHS, Department of Justice, DOS, DOT, Central Intelligence Agency, National Institute of Standards and Technology, and TSWG. The combined use of Federal assets will be necessary to optimize the rapid development and deployment of appropriate defenses. These interagency partners have worked closely together to obtain operationally viable solutions. The Environmental Protection Agency (EPA), along with other Federal agencies, leads or participates in responses to address certain explosives-contaminated sites under the authority of the *National Oil and Hazardous Substances Pollution Contingency Plan* (NCP). Under the NCP, EPA serves as the chair of the National Response Team (NRT), and a representative from the U.S. Coast Guard serves as its vice chair.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Various efforts are underway across the Federal government to help defend the Nation against explosive threats and weapons. These efforts have culminated in the deployed technology and countermeasures that are described below.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Department of Defense (DoD)

- Made significant progress in technologies to protect soldiers and assets from blast effects. IEDs can be sophisticated, and U.S. troops deployed overseas are being attacked by insurgents and terrorists using artillery shells that are triggered by timing mechanisms and remote-control devices.
- Developed coatings that are designed to be operationally flexible to protect vehicles from ballistics and blast effects.
- Deployed advanced body armor to protect soldiers responding to bomb threats.
- Developed strategic plans for explosives countermeasures.
- Chartered a U.S. Army Counter Explosives Hazards Center with the mission to function as the integrator for all countermeasures involving explosive hazards, incorporating lessons learned and providing support to deploying units on use of commercial-off-the-shelf (COTS) equipment, assured mobility, and force protection involving explosive devices.

Department of Energy (DOE)

- Employed tested and verified methods of construction to harden nuclear facilities against vehicle bombs.
- Developed and applied a methodology for quantitatively analyzing the effectiveness of explosives protection systems for mitigating specific threats.
- Determined the role of certain environmental conditions (e.g., sun, rain, wind) in causing a failure of trace systems to detect explosives deposited on vehicles.
- Developed and deployed Advanced Concept Armored Vehicles which afford vehicle occupants increased protection while operating in an environment in which they must engage a hostile force. This system would allow an externally mounted weapon to fire upon a detected IED without exposing the operator to direct fire.
- Published and disseminated an Explosives Protection Technology Transfer Manual which includes technical information necessary to design an explosive protection system properly.

Department of Homeland Security (DHS)

- Recently certified a new type of Explosives Detection System (EDS) for the detection of explosives in aviation checked baggage and began conducting pilot tests in the operational environment. The new EDS is less costly and more compact, making it more appropriate for use in places where larger EDS machines are impractical.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DHS, continued

- Pursued research and development to enhance air cargo screening capabilities by pilot-testing commercial-off-the-shelf (COTS) technology for air cargo screening and issuing research and development grants to inventors of new technologies for screening air cargo for explosives.
- Began an effort to examine alternative solutions that will make aircraft more resistant to the explosive effects of an IED.
- Initiated a pilot test of commercially available and prototype technologies to screen for suicide bombers/leave-behind improvised explosive devices (SB/LBIED) in an urban mass transit rail system environment.
- Developing and field-testing several new explosives detection technologies through the Secure Automobile Inspection Lane (SAIL) pilot on ferries that scans cars and trucks for explosives, the Transit and Rail Inspection Pilot (TRIP) for screening passengers and baggage in a rail environment, and Explosives Trace Detection Portals and Explosives Detection Document Scanners that are being evaluated at multiple airports.
- Initiated development of stand-off explosives detection technologies for SB/LBIED, as well as stand-off and checkpoint explosives detection technologies for vehicle-borne improvised explosive devices (VBIED).
- Began leading development of a national strategy to leverage technology to counter the threat posed by terrorist use of explosives and IED.
- Drafted an explosives effects mitigation RDT&E strategy and began work on various initiatives to improve the resistance of structures to explosive effects.
- Undertaking, in cooperation with the Domestic Nuclear Defense Office (DNDO), an examination of technologies to interdict attempts to smuggle explosives into the US.
- Developed certified explosives detection systems (EDS) based on computed tomography (CT) with over 1,000 EDS deployed at large commercial airports to screen checked baggage, primarily focused on the detection of explosives and explosive devices in relatively small quantities and hidden in suitcase-sized objects
- Developed explosives trace detectors (ETDs), which detect minute quantities of explosive residue, and deployed them widely at airports. ETDs are used to screen passengers, carry-on, and checked baggage. As a result, checked baggage and passenger checkpoints are now being protected to a much greater degree than before against the introduction of explosives aboard aircraft.

Department of Justice (DOJ)

- Developed cooperative efforts with The Fertilizer Institute to exercise caution and increase voluntary control in the distribution of certain agricultural commodities useful in the manufacture of improvised explosive mixtures.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DOJ, continued

- Identified, along with the National Academy of Sciences, the short list of precursor chemicals most likely to be used in improvised explosives.
- Identified emerging threat improvised explosives mixtures and is continuing to characterize their properties.
- Developed polymer coatings for the detection of explosives as well as chemical and biological weapons of mass destruction which are currently being used in detectors and which have been deployed in Iraq and Afghanistan.
- Was involved in passage of the Safe Explosives Act that requires all persons who acquire, transport, or ship explosives to obtain a license or permit.
- Was involved in passage of legislation that requires all plastic explosives manufactured in and imported into the U.S. to contain a detection marking agent.
- Initiated development of a Strategic Plan for U.S. Bomb Squads supported by the National Bomb Squad Commanders' Advisory Board.
- Employed new materials and methods of construction to harden facilities against blast and fragments of a vehicle bomb.
- Employed detection methods to screen vehicles prior to entering sensitive facilities.

National Science Foundation (NSF)

- Supporting research in a number of areas critical to defending against explosives and weapons including research performed in cooperation with the Intelligence Community (Approaches to Combat Terrorism) in areas of mathematics, energy sources, sensors and detectors, image processing and optical spectroscopy. In particular, spectroscopy is a promising approach for stand-off detection of explosives, basic research in computer vision could help spot explosives in carry-on baggage, and basic research on video analysis can help identify unattended bags.
- Supporting basic research in real-time imaging and sensing and rapid detection of improvised explosive devices (IEDs) using terahertz technologies.
- Analyzing the response of new and retrofitted buildings to blast loads.

Federal government, cooperatively

- Established an interdepartmental IED Countermeasures Technology Working Group to share among its members each department's strategies, objectives, and requirements for activities regarding the topic.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

***Federal
government,
cooperatively,
continued***

- Developing a *National Strategy for Explosives Countermeasures Technology*.
- Developed and implemented a proactive Radio-Controlled Improvised Explosive Device (RCIED) Electronic Countermeasure Pilot Program for selected major U.S. cities. This initiative was lead by the Technical Support Working Group (TSWG) in partnership with DHS, the Federal Bureau of Investigation (FBI), the Bureau of Alcohol, Tobacco, and Firearms (ATF), DOJ's National Institute of Justice (NIJ), National Bomb Squad Commanders' Advisory Board, National Telecommunications and Information Administration (NTIA), Federal Communications Commission (FCC), Joint Spectrum Center, select members from State and local bomb squads, and the Hazardous Devices School (HDS).

CHAPTER 5 – CRITICAL INFRASTRUCTURE PROTECTION

INTRODUCTION

The Nation's infrastructure is a framework of interdependent networks and systems that provides a continual flow of goods and services essential to the defense and economic security of the United States. Critical national infrastructures² are those deemed to be so vital that their incapacity or destruction would have a debilitating regional or national impact or severely disrupt the behavior and activities of large numbers of people who depend upon those services. The critical infrastructure protection (CIP) mission is to secure further and fortify the Nation's critical infrastructure and key resources from acts of terrorism, natural disasters, or other high-impact emergencies by developing and deploying tools, technologies, and systems that reduce the risks and mitigate the consequences of an event. This chapter represents work currently underway in the Infrastructure Subcommittee of the National Science and Technology Council and its interagency working groups, which have written the annual *National Plan for Research and Development in Support of Critical Infrastructure Protection* as required by the President's *Critical Infrastructure Identification, Prioritization, and Protection*. The sources used for this chapter include the National Academies study *Making the Nation Safer*, Presidential directives, RAND workshops held in 2001 and 2002 with private industry owners and operators of critical infrastructure, the *Federal Plan for Cyber Security and Information Assurance Research and Development*, Office of Management and Budget's *Combating Terrorism* Report to Congress, and inputs from more than 200 subject matter experts from 24 Federal agencies and multiple government-affiliated research institutions.

Cyber threats pose an ever-growing risk to our national and economic security. We face enormous challenges in our ability to meet or even anticipate those threats. The events of September 11, 2001 made clear that the security of our Nation and our economy are intertwined. The majority of government communications utilize private-sector networks, including critical infrastructures -- such as information technology, communications, financial services, electricity, and oil and gas systems. These networks have proven interdependencies that are critical to response capabilities as well as business operations. The systems of these sectors have converged and are interconnected. For example, if the electrical grids fail, that failure impacts the communications systems, which in turn can hamper financial networks.

The Internet connects all other networks, including our Nation's critical infrastructure. It has become the central nervous system for our government, our citizens and our industries. When it is attacked, the effects can ripple far and wide. Although the Internet was developed to provide "essential minimum communications" in the event of a nuclear attack, it was not designed with security in mind. Thus, the technology that is deployed over most of the Internet today has vulnerabilities that can be exploited, endangering all the connecting networks, including our critical infrastructures.

THREATS AND VULNERABILITIES

Understanding the vulnerabilities of our critical infrastructures, and identifying and validating threats to them, involves the use of in-depth knowledge of each infrastructure and the assets of which they are composed. Although an attack on any one asset can be significant, there may be secondary effects that cascade to other infrastructures as a result of their connectivity and interdependencies, which may magnify the impact.

Threats against physical infrastructure and assets include: high explosive blasts, projectiles, and fire damage; CBRN attacks; physical assaults, intrusions and insider threats; and natural disasters and other

² The National Infrastructure Protection Plan defines the Nation's critical infrastructure as consisting of 17 sectors and resources: Agriculture and Food, Public Health and Healthcare, Drinking Water and Wastewater Treatment Systems, Energy, Banking and Finance, National Monuments and Icons, Defense Industrial Base, Information Technology, Telecommunications, Chemical, Transportation Systems, Emergency Services, Postal and Shipping, Dams, Government Facilities, Commercial Facilities, and Nuclear Reactors/Materials/Waste.

emergencies. The cyber infrastructure is threatened by compromised or corrupted networks, damage to stored data, faulty software applications, or suspect hardware components.

The Nation's ability to contend with these threats is compromised by numerous vulnerabilities. Incomplete understanding of dynamic infrastructure systems and their complex interdependencies makes it difficult to determine the most critical sectors and timing of efforts. The existing infrastructure is impacted by disparate, disconnected physical components and information resources, as well as non-standardized architectures.

There are vulnerabilities to just-in-time manufacturers when their suppliers are vulnerable to interruptions. A tension exists among security and controls, societal openness, privacy concerns, and limitations of surveillance. Commercial and international ownership of U.S. critical infrastructure complicates the government's role in helping to protect it. The age and condition of the Nation's infrastructure makes it vulnerable to threats, while market forces and economic considerations are potential barriers to the investments needed to improve security.

Emerging threats may require scientific and technological approaches previously not considered. For example, new forms of airborne threats may be developed that are tailored to enclosed assets. Electromagnetic pulse, high-energy microwave, or tuned acoustic vibration technologies may be weaponized for disruption or direct destruction of critical infrastructure services and operations. Advances in nanotechnology and biotechnology may bring new threats and vulnerabilities. Each of these new threats will require new designs, technologies, and materials for securing and protecting our critical infrastructure.

REQUIREMENTS

The science and technology necessary for protecting our critical infrastructure must meet requirements in a number of areas. These include: functional needs to support operational missions in awareness, prevention, protection, response, and recovery; solutions to secure infrastructures and reduce vulnerabilities; the ability to understand infrastructure interdependencies and manage the risks associated with them; foundations for economic and risk analysis; and technologies that enable solutions like modeling, simulation, and visualization. Infrastructure owners and operators must also assist in defining requirements and in providing solutions. A partnership among the Federal government, State, local, and tribal authorities, and private sector owners and operators is essential for our success.

In addition to the evolving needs of infrastructure operators, key areas of focus were identified in the President's *Critical Infrastructure Identification, Prioritization, and Protection*, which requires the Federal government to reduce vulnerabilities of the Nation's critical infrastructure and key resources to incidents that may:

- Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;
- Impair Federal departments and agencies' abilities to perform essential missions or to ensure the public's health and safety;
- Undermine State and local government capacities to maintain order and to deliver minimum essential public services;
- Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
- Have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or
- Undermine the public's morale and confidence in our national economic and political institutions.

GAPS

Several key gaps in the ability to protect our infrastructure leave the Nation's critical infrastructure vulnerable to acts of terrorism and natural disasters. Although major programs have been mounted to address many of the following gaps, the solutions will take several years to pass through the phases of RDT&E and then to become commercially viable. One key gap is the incomplete knowledge of our critical infrastructure operations and interdependencies. Advanced simulation and decision-support tools are needed to model natural disasters and terrorist-induced emergencies. Additionally, the inadequate understanding of how to quantify, evaluate, and measure security to enable decision making leads to a lack of investments in critical infrastructure sectors and it contributes to lower overall levels of security. This creates a barrier to the private sector making investments needed to secure the Nation's privately owned infrastructure.

Evolution of the Internet landscape has led to the need for incorporating security concepts into the underlying infrastructure. Infrastructure protocols associated with Internet communications, such as the domain name system and routing protocols, were developed without security as a requirement at a time when trust was assumed and threats were not. For different reasons, protocols used by process control systems were also developed without security in mind, leading to similar concerns over vulnerability.

There are insufficient low-cost, automated monitoring, surveillance, and response systems for critical infrastructure both cyber and physical. Protection from high explosive blasts, projectiles, and fire are needed for all critical assets, especially tall structures, tunnels, dams, ports, and bridges. There are special problems for our infrastructure associated with chemical, biological, and explosives threats, including medical diagnosis, forensic and detection systems, and decontamination processes. There are few non-lethal protection and response systems to prevent loss of life to non-threat intruders. There are severe limits in our ability to perform tracking, logging, and behavior-based analysis to protect against and detect insider threats. In addition, more powerful authentication and authorization capabilities are needed. Personnel surety management and determination of intent tools are needed. We must address access security in the context of an open society while recognizing privacy concerns. Large-scale situational awareness and common operating picture are lacking. These require real-time distributed data collection, fusion, and analysis for physical and cyber infrastructures.

Other than general redundancy in interconnectedness, there are few existing principles available for ensuring survivability of large-scale networks and robustness and resilience to allow operations under large-scale attacks. Furthermore, from a recovery and reconstitution point of view, the only approaches available are redundant operational sites and backups. There are currently few technological means for providing rapid recovery and reconstitution of compromised or damaged systems. In addition, there are not sufficiently robust and resilient systems with built-in security.

STRATEGIC GOALS FOR 2015

Three strategic goals have been identified as priority needs for the 2015 time frame. While aggressively pursuing these goals over the next decade will provide clear benefits to the Nation's critical infrastructure, doing so will also create broad-based spillover benefits, enabling non-critical infrastructure to acquire, use, and benefit from new technologies in order to enhance operational, economic, and personnel security.

***National Common
Operating Picture for
Critical Infrastructure***

- Automate and integrate infrastructure monitoring and support systems, as well as decision support systems with dynamic aggregation, fusion, and real-time observation of the Nation's key assets. This real-time situational awareness capability will provide a national Common Operating Picture, and the heart of the system will be a ubiquitous, intelligent, self-healing, and self-monitoring sensor network for 24-7 monitoring and information transfer. It will be coupled directly to feed models, train decision support systems, and provide information to protection/response personnel. Decision makers will use risk-based, decision-support tools to manage asset integrity continuously and perform viability monitoring to minimize loss and maximize safety in natural and deliberate or intentional events. This goal will be enabled by next-generation design and architecture frameworks that deliver systems that take advantage of new and emerging technologies to develop robust, integrated, automated, and aligned information systems across all sectors.

***Inherently Secure Next-
Generation Internet
Architecture***

- Develop a next-generation Internet architecture that is inherently more secure than the existing Internet. This architecture will preserve many of the basic principles that are fundamental to today's Internet but will result in the synthesis of a new Internet for which security is a prominent technical requirement during the design and architecture development phases, rather than existing as a post-development operational issue. Fundamental protocols associated with Internet communications will be revised or replaced to provide confidentiality, authentication, and integrity across multiple communication layers. Rethinking elementary routing and network management approaches will result in a more robust and resilient Internet in which communications can be prioritized and for which operation is sustainable under crisis conditions. The security built into this architecture will provide the basis for an infrastructure that can be relied upon with a far greater degree of trust and confidence than today's Internet. The result will be an infrastructure that not only overcomes many of the risk barriers that exist for today's Internet applications but that also enables new approaches to increasing productivity and enhancing the Nation's economic competitiveness.

***Resilient,
Self-diagnosing, Self-
healing Systems***

- Develop replacement infrastructure that is resilient if attacked, can manage or contain the extent of damage, can continue to provide service (even if at diminished capacity), and can adapt and self-heal damaged areas. Embed these systems with computerized sensors and software agents that can collect, analyze, and report information about the condition of the infrastructure and suggest or implement ways to adapt, reroute, or redistribute loads to reduce damages.

***Resilient,
Self-diagnosing, Self-
healing Systems,
continued***

- Advance material science to produce materials that self-heal fractures, have extreme strength, and can deform and absorb energy but then return to their original shape.

- Advance and develop new manufacturing processes that are patterned after biological processes (this can be either organic or inorganic chemistry) such as those used in self-assembled nanostructures.
- Develop inherently secure, resilient design concepts such as high-strength designs for load reversal or redistribution, sacrificial zones to provide stand-off, optimized use of emerging materials and systems, and design concepts to slow the rate at which failure takes place.
- Incorporate these inherently secure, resilient features in both cyber and physical systems and especially their integration, such as the development of adaptive, intelligent power grids.
- Advance system design concepts and emerging materials to levels of economically sustainable, practical implementation.
- Build intelligent computer software systems and autonomic hardware systems that can mutate and improve to protect and repair themselves or that can withstand a catastrophic event with a minimum of loss or disruption or even avoid damage by adaptation or modification of a portion of the cyber system.

NEAR-TERM PRIORITIES

Since development of the first *National Plan for Research and Development in Support of Critical Infrastructure Protection*, the agencies responsible for critical infrastructure protection of each sector have held workshops with industry, academia, and government laboratories to validate near-term research and development priorities. These priorities include:

Sensor Performance Improvement

- Develop improved physical and cyber monitoring and detection systems that will include improvements in speed, fewer false readings, lower power requirements, increased durability and robustness, and lower cost. These sensor networks will have increased sensitivity, be environmentally aware, and have higher accuracy and will include both active and passive sensors, as well as aerial platforms. Improving the sensitivity of detectors for explosives is particularly vital.

Advanced Risk Modeling, Simulation, and Analysis for Decision Support

- Improve capabilities to address all infrastructure sectors and their interdependencies.
- Create models and algorithms accessible to owners and operators of critical infrastructure that are interoperable and use common inputs and assumptions.
- Standardize the framework of vulnerability analysis and risk analysis of critical infrastructure sectors and key resources.

NEAR-TERM PRIORITIES, CONTINUED

Advanced Risk Modeling, Simulation, and Analysis for Decision Support, continued

- Develop the foundations for quantitative and economics-based security and risk assessment. Test, demonstrate, and pilot projects to inform and train owners and operators.

Improved Cyber Security

- Develop new methods for protection from, automated detection of, and response to attacks on critical information infrastructure systems. Advance the security of communication protocols that underlie the cyber and physical infrastructures. Enhance the ability to share and protect critical infrastructure information. Develop robust and secure process control systems such as SCADA and digital control systems (DCS) technology to retrofit existing infrastructure systems.

Improved Prevention and Protection

- Develop low-cost physical perimeter defense systems for critical infrastructure and key resources, including: systems to mitigate high-explosive blast, projectile, and fire threats; as well as improved portal access and control systems for CBRNE detection, weapon detection, and personnel identification and authentication.
- Develop enhanced monitoring and interpretation systems for automated protection, intrusion prevention and detection, and surveillance in both the physical and cyber domains.

Addressing the Insider Threat

- Improve technologies and understanding for insider threat detection, covering physical and cyber infrastructures separately and working toward integrated methods of personnel surety and document and identification authentication.

Large-scale Situational Awareness for Critical Infrastructure

- Define the architecture to create a national common operating picture of the Nation's critical infrastructure and key resources. Begin to implement multi-database monitoring systems that feed models, train decision support systems, and provide information to protection and response personnel. Use pilots and test beds to begin to integrate communications network architectures consisting of sensors, controls, and systems to have uniform structures and common languages, interoperability, compatibility, and scalability.

MID-TERM PRIORITIES

Advanced Risk Modeling, Simulation, and Analysis for Decision Support

- Improve modeling, simulation, and analysis for initial use in pilots and test beds with real-time decision support and planning. Increase knowledge of infrastructure systems and their interdependencies and begin to catalog decision and consequence chains in natural and man-made disasters. Conduct quantitative risk assessments for better quantification of terrorism and other hazard risks to critical infrastructure and key resources, including an emphasis in the cyber domain.

MID-TERM PRIORITIES, CONTINUED

Addressing the Insider Threat

- Develop technology to address physical and cyber insider threats through the use of methods that integrate information and sensor data from physical and cyber security systems.

Improved Cyber Security

- Accelerate migration to more secure versions of the protocols underlying Internet communications like the domain name system and routing protocols. Improve robust and secure process control systems such as SCADA and DCS technology to retrofit existing infrastructure systems.

Improved Prevention and Protection

- Improve protection, monitoring and surveillance of critical infrastructure (physical and cyber) with inherent anomaly detection and increasingly automated response and recovery. Improve high-explosive blast, projectile, and fire mitigation including walls, windows, structural support systems, surfacing, and post-event management, with special emphasis on protection of tall buildings and critical facilities. Develop better high-occupancy, short-duration, shelter-in-place technology for all threats. Enhance the technology and acceptance of advanced technology for identification, authentication, authorization, access control and tracking of people, systems and agents. Develop cost-effective design and retrofit technologies and will consider life-cycle cost issues in new protective systems.

Large-Scale Situational Awareness for Critical Infrastructure

- Provide prototype common operating picture systems including dynamic situational awareness and interpretation and real-time distributed data collection, visualization, and interpretation. We will provide robust integration of sensing networks with automated infrastructure response systems and the infrastructure attribute knowledge base.

Next-Generation Designs and Architectures

- Develop next-generation infrastructural concepts, architectures and systems, both physical and cyber to include built-in security. Create tools and methodologies to support the development of such systems. Systems must become reliable, autonomous (self-repairing and self-sustaining), resilient, and survivable, so they can continue to operate in a diminished capacity rather than failing under crisis conditions.

LONG-TERM PRIORITIES

Advanced Risk Modeling, Simulation, and Analysis for Decision Support

- Improve modeling, simulation, and analysis for real-time decision support and planning. Increase knowledge of infrastructure systems and their interdependencies and catalog decision and consequence chains in natural and man-made disasters. Provide public awareness of the risks, how they are being addressed, and how decisions are being made involving investment, threats, and value to the Nation.

LONG-TERM PRIORITIES, CONTINUED

Improved Cyber Security

- Guide development of next-generation security for Internet-protocol-based process control systems and services.

Large-Scale Situational Awareness for Critical Infrastructure

- Further refine common operating picture systems including dynamic situational awareness and interpretation. Provide integration of sensing systems with automated infrastructure response systems and the infrastructure attribute knowledge base.

Next-Generation Designs and Architectures

- Improve next-generation infrastructural concepts, architectures and systems, both physical and cyber to include built-in security. Create tools and methodologies to support the development of such systems. Systems must become reliable, autonomic (self-repairing and self-sustaining), resilient, and survivable systems that continue to operate in diminished capacity rather than failing under crisis conditions.

Human and Social Issues

- Improve our understanding of the intimate and complex relationship between humans and their built environment or infrastructure. Develop improved systems that address the human-technology layer and provide an integrated view of societal risks from terrorist events, natural disasters, and other emergencies.

AGENCIES' ROLES AND RESPONSIBILITIES

Protecting our Nation's critical infrastructure will require support, knowledge, and contribution from almost every other office of government, from industry and contractors, and from the military. All elements of the Nation must work together and with international partners to achieve critical infrastructure protection. As part of this effort, many Federal agencies have unique responsibilities to perform homeland security-related activities. Continuous updates on threat information are needed from the intelligence community. The private sector and owners/operators of the critical infrastructures must continue to improve the degree to which they work together and with the Federal government through Sector Coordinating Councils while agencies develop stronger interagency cooperation through the Government Coordinating Councils.

DHS is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. Sector-specific agencies are responsible for some aspects of assessment and protection within their assigned sectors: USDA (agriculture and some food – meat, poultry, and egg products), HHS (public health, healthcare, and all food except that covered by USDA), EPA (drinking water and water treatment systems, as well as decontamination), DOE (energy except for nuclear power facilities which is covered by DHS), Treasury (banking and finance), DOI (national monuments and icons), and DoD (defense industrial base). The remaining infrastructure areas of emergency services, information technology, telecommunications, and chemical and hazardous materials are the responsibility of DHS to protect.

In addition, the directive defines special functions for other Federal departments and agencies as well as components of the Executive Office of the President: Department of State (DOS) (international coordination), DOJ (reduce domestic terrorist threats), DOC (work with the private sector), Homeland Security Council (HSC) (interagency policy), Office of Science and Technology Policy (OSTP) (interagency research and development), Office of Management and Budget (OMB) (interagency

implementation), DOT (coordination with DHS on the transportation sector), and the NRC (nuclear reactors and material).

DHS is responsible for developing and implementing a comprehensive *National Infrastructure Protection Plan* (NIPP) which describes the operational processes and plans that each of the responsible agencies will use to achieve what is required for their respective critical infrastructure. Working with OSTP, DHS is also responsible for developing an annually updated *National Plan for Research and Development in Support of Critical Infrastructure Protection* that is closely coordinated with the NIPP and the sector requirements.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Numerous Federal departments and agencies are involved in the science and technology of protecting the Nation's critical infrastructure. Listed below are a few highlights.

Department of Commerce (DOC)

- Increasing the structural integrity and fire safety of physical systems through development of tools, guidance, and performance criteria for building codes and standards. These efforts are intended to prevent local structural failure from progressing in a chain reaction to larger-scale structural collapse.
- Developed a Federal Information Processing Standard (FIPS 201), Personal Identity Verification (PIV) for Federal Employees and Contractors, as well as a number of supporting biometrics, integrated circuit card interface, and cryptographic guidelines in response to the President's *Policy for a Common Identification Standard for Federal Employees and Contractors*. In the future, DOC will develop identity verification and smart card interoperability specifications and standards necessary for interagency use of personal identification systems.

Department of Defense (DoD)

- Developing components, subsystems, and technologies with potential aerospace combat, special operations, and airlift EC applications. Ongoing projects include development and demonstration of techniques and technologies for integrated EC sensors and systems into a fused and seamless whole, advanced technologies for radio-frequency EC suites, and advanced warning and countermeasure technologies to defeat electro-optical, infrared, and laser threats to aerospace platforms.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DoD, continued

- Reducing the cost and lead time required to protect aircraft from infrared heat-seeking Man-Portable Air Defense Systems (MANPADS) in the near-ground urban and expeditionary environment. DoD's current efforts focus on the development of a ground based, networked electro-optical sensor grid that would provide missile launch detection and warning, including examination of commercially available components to lower costs and to reduce the lead-time for system fielding. By using vehicle mountings and wireless networking, it will be potentially possible make the system readily portable for rapid coverage area reconfiguration.
- Addressing complex agency interactions in Homeland Security through a Homeland Security/Defense Command and Control Advanced Concept Technology Demonstration (HLS/D C2 ACTD). This ACTD is designed to provide DoD's homeland security and homeland defense communities a trusted information exchange environment and the operationally relevant command, control, coordination, and decision making tools required to execute their missions. This ACTD's approach is to provide alerting and shared situational awareness, enhanced ability to analyze information, integrated information gathering and sharing, enhanced command, control, communications, computers, and intelligence (C4I) planning and direction, and enhanced joint and combined interoperability.
- Establishing a wireless weapons of mass destruction (WMD) vessel boarding and inspection system that provides an operational capability to reduce the risk associated with U.S. Coast Guard interdiction operations. This operational capability will enable boarding teams to transmit intelligence such as photos of crew, passports, possible WMD detections, and potential evidence to the host ship and military agencies in near-real time.

Department of Health and Human Services (HHS)

- Promoting bioterrorism other public health emergency preparedness in rural and urban communities with respect to intermediate and long-term health needs, including long-term care, rehabilitation, chronic physical ailments, and mental health. This effort integrates qualitative (key personnel interviews, network analysis, and focus groups) and quantitative (knowledge-based testing) methodologies to assess existing resources and response mechanisms in rural and neighboring urban communities to meet anticipated health needs arising from bioterrorist events. Given the particularly limited resources available in rural communities, HHS will examine how urban providers can serve a supportive role for rural communities following bioterrorist events. The evidence obtained from these assessments will serve as the basis for models and recommendations to policymakers to improve bioterrorism preparedness in rural communities across the nation.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

HHS, continued

- Improving the workforce's protection from urgent non-occupational infectious, environmental, or terrorist threats by improving our basic understanding of effective methods for evacuating individuals, specifically those with disabilities, from buildings and other settings in response to such threats. HHS is developing an Agent-Based Modeling method to examine the effect of evacuation methodologies on the dynamics of mass pedestrian flows (MPFs) during health-safety events in the built environment, as well as the effect of evacuation methodologies on the egress of individuals with disabilities.

Department of Homeland Security (DHS)

- Conducting large-scale modeling of infrastructure interdependencies and cascading effects to help prioritize critical infrastructure and enable planning activities related to national defense and intelligence missions. Under the direction of DHS, a consortium of national laboratories is developing a consequence- and interdependency-based Decision Support System (DSS) that will develop, implement, and evolve a rational approach for prioritizing CIP strategies and resource allocations using modeling, simulation, and analyses to assess vulnerabilities, consequences, and risks. The CIP-DSS will help propose and evaluate protection, mitigation, and response and recovery strategies and options to provide real-time support to decision makers during crises and emergencies.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DHS, continued

- Developing water-, levee-, and dam-related risk reduction models to provide recommendations for improvements to practices, standards, and codes could reduce public risk and economic losses from future hurricanes. A variety of Federal, state, and private organizations will work together to develop these standards and practices, and DHS will seek to develop tools and methods to determine structural integrity of levees and dams, as well as create models to gain understanding of consequences resulting from disasters.
- **2004: Started four Regional Technology Integration (RTI) pilots** in Memphis, Tenn.; Anaheim, Calif.; Cincinnati, Ohio; and Seattle, Washington, to test chem/bio/explosives detection systems; planning and exercise tools to evaluate multi-jurisdictional performance for State and local decision-makers; and technologies for credentialing emergency responders and verifying victims' identities during an incident.
- **2005: Developed a simulation to help prevent cascading electricity blackouts**, such as those that occurred in the northeast in August 2003, in coordination with the Electric Power Research Institute.
- **2006: Established Phase 1 of a cyber security testbed to enable a wide community of researchers to explore threats to network security without risk of compromising the actual internet.** DHS S&T is working with the National Science Foundation (NSF) to create the DETER testbed for test and evaluation of cyber security technologies. The testbed will create a realistic model of the internet on which to test cyber security technologies. DHS will transition Phase 2 in FY2013
- **2006: Developed cost-effective automated detection of unattended objects** (like backpacks left behind on a subway or in an airport) by using video interpretation programs linked to Closed Circuit Television (CCTV) cameras to improve the ability to monitor infrastructure assets.

Department of the Interior (DOI)

- Developed in cooperation with DoD and the Department of Energy a scale model test of embankment dams subjected to high-explosive charges placed on the dam crest. These studies provided all parties valuable data and information on the size of a crater that would form on the crest, the effects of the shock waves and vibration on the underlying embankment materials, and the performance of potential corrective measures. This information is now being applied to an inventory of dams to identify those facilities with the greatest vulnerabilities.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DOI, continued

- Performed in cooperation with DoD numerical analyses on the effects of high-explosives placed underwater and upstream of fixed-wheel and radial spillway gates. The data obtained were used to develop potential protective measures that were included in subsequent analyses by DoD. The analyses performed provided information that can be applied to an inventory of spillway gates to identify those with the greatest vulnerabilities and to prioritize a program of corrective actions to mitigate risk from this type of attack.

Department of State (DOS)

- Participated in agency interview process and provided valuable insights relating to the CIP requirements of its facilities worldwide. DOS is addressing these requirements based on solutions from different agencies, including DOD, DHS, the National Science Foundation (NSF), and the Technical Support Working Group (TSWG).

Department of Transportation (DOT)

- Sponsored a concept study in cooperation with the US Coast Guard that concluded there is a demonstrable need for a cooperative research program, with a strong security component, for hazardous materials transportation. This study resulted in Transportation Research Board Special Report 283, "Cooperative Research for Hazardous Materials Transportation – Defining the Need, Converging on Solutions."

Department of the Treasury (Treasury)

- Initiated an adaptive quarantine research project to ensure that the Federal Aviation Administration (FAA) is prepared to prevent and preempt active, passive, novel, insider and outsider cyber security attacks against safety-critical and mission support networks and systems enterprise-wide. Treasury is identifying an integrated solution that consist of a combination of proactive behavior-based tools and reactive rules-based tools that cover the entire attack timeline and all layers of the protocol stack.

Central Intelligence Agency (CIA)

- Adapting technology originally developed for the casino gaming industry to identify correlations dynamically across vast amounts of structured data from hundreds or thousands of data sources in near-real time and to alert users to potentially harmful relationships.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

CIA, continued

- Developed a real-time monitoring and event-processing software product to provide solutions for alerting, event correlation, auto-response management, and triggering live visualization across enterprise application integration databases, sensors, streams, and communications systems.

Environmental Protection Agency (EPA)

- Addressed water physical and infrastructure protection by implementing and continuing several extramural projects. Through interagency agreements, EPA is evaluating alternative water supplies and treatment methods for use during an emergency. Ongoing efforts are also evaluating blast protection needs for both stand-off distances and hardening of water infrastructures.
- Is conducting and sponsoring evaluation of water quality sensors for their ability to detect a contamination event in a distribution system and evaluating water sector interdependencies with other sectors.
- Is conducting a critical analysis of cyber security to identify research needs associated with Supervisory Control and Data Acquisition (SCADA) systems that are used for automated operations in both drinking water and wastewater systems.

National Aeronautics and Space Administration (NASA)

- Has and is developing and advancing technologies as part of its overall mission that may also mitigate the consequences from an intentional attack. Additionally, research data from NASA systems may be leveraged by DoD and DHS in support of national and homeland security objectives, as appropriate.

National Science Foundation (NSF)

- Is developing, through its Team for Research in Ubiquitous Secure Technology (TRUST), a deeper understanding of the scientific foundations of cyber security and critical infrastructure systems, understanding the economic and public policy drivers and impacts for cyber security, and assuring the workforce required for research and development.
- Is conducting both fundamental and developmental work for hand-held detection of explosives and nerve agents with extremely low false alarm rate by combining ultra low-energy electron attachment and miniature mass spectrometry.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Technical Support Working Group (TSWG)

- Developed a SCADA cryptographic module that encrypts communications between components of a SCADA network to protect against hackers or other misuse. The SCADA cryptographic module complies with the American Gas Association (AGA) 12-1 Cryptographic Protection of SCADA Communications encryption standard for natural gas systems and can also be used for water and electric power SCADA systems.
- Is exploring technologies necessary to provide a stand-off detection capability of explosives in larger volumes at greater distances for detection of large-vehicle bombs. Efforts include investigating unique physical and chemical phenomena that identify the presence of explosives, the physical limits for sensor technology to respond to these phenomena, and technology enhancements.

CHAPTER 6– EMERGENCY PREPAREDNESS AND RESPONSE

INTRODUCTION

In any disaster, emergency responders are our Nation’s front line of defense, saving lives and reducing property damage. Highly trained responders, armed with proper tools, planning, and resources, can dramatically reduce the devastating effects of emergencies, ranging from natural disasters to terrorist attacks with weapons of mass destruction (WMD).

To ensure that emergency responders have the support they need, our Nation is developing and deploying enabling technologies that improve emergency preparedness and response capabilities to prepare for, respond to, and recover from all-hazards emergencies.

These include, but are not limited to:

- Enhancing and creating tools to assist in planning for, mitigating the effects of, responding to, and recovering from catastrophic events;
- Facilitating the integration of these tools into existing day-to-day responder operations; and
- Sharing best practices and lessons learned that bolster emergency responder and civilian preparedness in order to enhance their effectiveness in responding to large-scale incidents.

Enhancing these capabilities will require addressing the technology-focused research, development, testing, and evaluation (RDT&E) needs of all emergency responder organizations, including paid and volunteer fire services, emergency medical services, law enforcement agencies, and emergency managers. The emergency preparedness and response community has more than 49,000 separate agencies throughout the country of varying sizes, structures, capabilities, and constraints. Within this community, law enforcement comprises approximately 18,000 agencies with the majority having 24 or fewer sworn officers. Fire departments – predominantly staffed by volunteers – comprise nearly 31,000 agencies. Such a vast and diverse community necessitates a broad range of technological capabilities and solutions.

Historically, responder technology and training has focused on natural disasters and industrial accidents. The recent threat of terrorist attacks using chemical, biological, or explosive weapons demands significant changes in responder mindset, protocols, training, and equipment. An effective emergency preparedness and response posture will require science and technology advances to provide new personal protective equipment, hazard detection systems, unified incident command and decision support systems, scalable and interoperable communications systems, and modeling and simulation applications for training and exercising. Incorporating and developing new operational models and enabling technologies to address this threat requires a significant research and development effort which will better secure our Nation and protect our citizens.

The *Federal Response to Hurricane Katrina: Lessons Learned* published by the White House, details shortfalls in Emergency Preparedness and Response during the Federal response to Katrina, four critical flaws in our national preparedness became evident: Our processes for unified management of the national response; command and control structures within the Federal government; knowledge of our preparedness plans; and regional planning and coordination.”

These critical shortfalls identified in the lessons learned following hurricane Katrina validate the focus of effort for science and technology development in developing and strengthening both preparedness and response for the nation.

THREATS AND VULNERABILITIES

Emergency responders must prepare for and respond to a broad range of threats, historically including hurricanes, tornadoes, floods, accidental explosions, chemical spills and building collapses. Recently, the threat of a terrorist attack has been added to these more frequent disasters, presenting a new set of vulnerabilities that require additional training and equipment.

Specifically, the key threats and vulnerabilities identified by the emergency preparedness and response community are as follows:

- ***Radio Interoperability and Communications***
 - Emergency responders require reliable, real-time, secure methods to communicate and share voice, video and data information with their own equipment;
 - Voice, video and data -related communications devices, including computer aided dispatch systems, lack the ability to take full advantage of wireless broadband, Voice over Internet Protocol (VoIP), Emergency Data Exchange Language (EDXL) and multi-band technologies and standards;
 - Emergency responder radio equipment often fails to allow interagency communication;
 - There exists an insufficient number of dedicated emergency radio bands;
 - Many high-rise buildings lack the repeater systems necessary to support portable radios;
 - Most cities lack backup radio systems; and
 - Current radios fail to operate satisfactorily underground or near valleys and canyons.
- ***Personal Protective Equipment***
 - Standard emergency response equipment does not have CBRNE protection;
 - Current equipment places severe physical stress on the emergency responder, particularly in a high heat environment; and
 - Equipment is not uniformly tested to ensure reliability.
- ***Other threats and vulnerabilities identified as research and development focus areas include:***
 - Lack of experience managing large and complex multi-jurisdictional incidents;
 - Lack of affordable, scalable training and exercise capability particularly in the large multi-jurisdictional incident arena;
 - Lack of real-time situational awareness and decision support capability; and
 - Lack of time-critical, networked systems for emergency mass transportation of ill, injured, and special needs populations out of hazard areas to medical destinations.

The focus of our continuing research and development efforts is to research, develop, and deploy solutions to mitigate these vulnerabilities, ensuring that emergency responders have the tools they need to respond safely and successfully when disaster strikes.

REQUIREMENTS

As mentioned above, the responder community represents a broad range of organizations with enormous responsibilities. Fire departments alone answer more than 60,000 emergency calls each day. To respond successfully to the wide range of threats facing our communities, new technologies, capabilities, and protocols are needed. Many of these capabilities are outlined below.

- ***Protect emergency responders from the effects of chemical, and biological agents, as well as blast and incendiary effects.*** This requires unobtrusive Personal Protective Equipment (PPE) that provides body and respiratory protection from all hazards but does not hinder the emergency responder's actions.
- ***Quickly detect, locate, characterize, and assess potential or ongoing terrorist attack.*** Rapid and accurate Detection, Identification and Assessment. This involves sensors and information technologies/capabilities that provide emergency responders with critical information to facilitate appropriate response protocols and decision making after a terrorist event.
- ***Acquire, store, distribute, and protect critical information for use in emergency management. This is a function of Unified Incident Command and Decision Support (UICDS).***
- ***Rapidly locate and rescue trapped or isolated individuals.*** Urban Search and Rescue (US&R) includes the rescue of individuals trapped or isolated by the effects of a terrorist attack or other major disaster, as well as the potential mass decontamination of victims, buildings, and equipment.
- ***Effective emergency planning.*** Emergency planning includes vulnerability analysis of high-risk facilities and locations; planning responses to various natural disaster and terrorist scenarios; performing low-cost, high-impact training and exercise for all types of incident response; as well as pre-event coordination among Federal, State, and local authorities and emergency responders.
- ***Integrated system of systems national plan for interoperable communications.*** The emergency preparedness, response and public safety communities require a national plan for interoperable communications that uses a systems of systems approach to provide Federal, state, local and tribal agencies with the flexibility to select equipment that best fits their technical requirements and meets budget constraints while still achieving interoperability. This will enable distinct systems owned by different agencies to communicate with each other without requiring the agencies to purchase the same equipment from the same manufacturer.
- ***Medical response, veterinary and public health readiness for CBRNE threats.*** Medical response, veterinary, and public health readiness include providing rapid, effective, safe treatment of persons exposed to CBRNE threats, environmental control to limit spread, and preparing public health infrastructure and health care delivery systems for a biological agent release. This includes rapid and effective decontamination of exposed populations and responders as well as establishment of registries and databases and tracking the longitudinal medical follow-up of these persons. It must also incorporate networked, emergency medical transportation systems that will be available when local medical infrastructure is overwhelmed or incapacitated.
- ***Effective and Efficient Logistics and Resource Support.*** This includes the effective and efficient delivery of shelter, equipment, consumables, food, water, and other supplies when and where they are needed in support of an emergency response.
- Enable the earliest possible, specific, and continuing understanding of a threat to support incident command decisions across all phases of a local or regional response. This

capability includes the ability to evaluate potential courses of action for effective decision support.

These and other capabilities are further documented in several studies of emergency responder needs including *Project Responder: National Technology Plan for Emergency Response to Catastrophic Terrorism*.

In addition to supporting the above capabilities, successful technology solutions must be easily and affordably deployable. With this in mind, research and development efforts must strive to provide new tools designed to work within existing operational structures, protocols, and budgets. To facilitate this, new technologies should not require an inordinate amount of specialized or frequent training and maintenance and must be sufficiently inexpensive to allow widespread purchase at the local level, be easily acquired, deployed, and operated by local emergency responders, broadly applicable across multiple hazards or operating environments, durable and reliable, interoperable and compatible with parallel and legacy systems, and must form an integral part of the community's or region's emergency response infrastructure.

GAPS

In the aftermath of natural and terrorist events, existing gaps in responder capabilities – and the vulnerabilities they create – become readily apparent. Assessing these gaps is a key aspect of training, exercises, and the post-incident lessons-learned process. A number of comprehensive studies, plans, and focus groups have also identified critical gaps and science and technology needs for emergency preparedness and response. The summaries below provide a general overview of these gaps.

- **Emergency Response Equipment** – The need for PPE that offers ‘all-hazards’ capability remains a major focus area for emergency response research and development. PPE includes respirators; self-contained breathing apparatuses; bulletproof vests; helmets, visors, and goggles; biohazard suits; and fire and chemical resistant clothing. A second major focus area involves communications support prior to, during, and following a disaster. Examples include the need for technology to determine the location and well-being of personnel and victims (especially inside buildings or collapsed structures); sensor systems to monitor and detect the presence of CBRNE hazards in real-time; interoperable communication systems across jurisdictions and departments; as well as systems with a capability for text, graphics, images or video. Other key requirements include mass decontamination systems for both personnel and equipment to provide rapid, effective, and safe treatment of persons exposed to CBRNE threats in all climates; emergency response systems that can collect and identify threat-relevant information, fuse and analyze information to support threat awareness, identify those who need to know specific types of information, and securely disseminate appropriate information to these people; and cross-modal emergency communications systems and response technologies for CBRNE incidents occurring in the transportation system, especially in tunnels and transportation hubs, such as train and transit stations, as well as airports.
- **Technology Integration** – Existing and emerging technology systems are key elements in increasing our preparedness for CBRNE events. However, technology is only as effective as the operational and management systems that surround it. Local governments are complex entities; there are over 80,000 local governments in the U.S. and each has its own set of governance structures and power relationships. Local governments have diverse baseline technological capabilities and vary in their ability and willingness to be early adopters of new technology. Communities are frequently unable to integrate advanced technology systems with existing infrastructures to achieve long-term sustainability. In addition, emergency response systems are often not integrated across Federal, State, local, and tribal emergency response organizations thus limiting their effectiveness in multi-jurisdictional and joint State and Federal responses.

- ***Training and Exercising*** - We currently do not have scaleable, on-demand, and affordable training and exercise capability containing realistic local community information in virtual, interactive environments, especially in a multi-jurisdictional scenario. Advanced modeling and simulation may hold the key to filling this gap, providing cost-effective, scalable, efficient training technologies ranging from simple training modules to full-scale national exercises. Training and exercise is a cornerstone of effective Emergency Preparedness and Response. There is a demonstrated need for technology to address the volume of responders that must be trained and the complexity of exercises, both of which could be made more cost effective if simulation were more effectively applied. Simulation-based training to enhance incident management capabilities could also facilitate effective implementation of the National Response Plan and the National Incident Management System.
- ***Education & Awareness*** – The emergency preparedness and response community is demanding a one-stop-shop for information regarding acquisition decisions, standards and grant programs, lessons learned, training resources, and other pertinent information. In addition, the public clearly needs better access to and awareness of the information they need to respond appropriately and better protect themselves in the event of an emergency, including a CBRNE attack. This information requirement extends beyond preparatory and initial response phases of incidents to include long-term medical consequences, availability of rapid and chronic therapeutic options, and access to subject matter expertise. Improved education and awareness could minimize loss of life in both civilian and responder communities.
- ***Atmospheric Hazard Predictions*** – IMAAC is providing a coordinated Federal capability for reliable, accurate prediction of atmospheric hazards, but gaps still exist in the understanding of hazardous material within the urban environment. More research is needed on the movement and behavior of hazardous materials within the urban canyons of our cities to provide the level of detail required by emergency managers for shelter-in-place or evacuation recommendations on a building-by-building basis.

STRATEGIC GOALS FOR 2015

By 2015 our goal is to have advanced the capabilities of our Nation’s emergency response infrastructure so that responders have the capability to prevent or mitigate terrorist use of CBRNE devices, State and local communities have the capability to monitor and detect such events, and officials can quickly and effectively communicate risk and protective actions to the public. By providing better tools to our emergency responders, integrating advanced technology systems into State and local communities, and providing robust situational awareness with scientific reach-back capabilities, we will be able to deter effectively and – when necessary – swiftly respond to catastrophic events.

- ***Undertake efforts defined by the Regional Technology Integration Initiative.*** We will work with State and local governments to integrate successfully advanced homeland security technologies and operational paradigms into their existing infrastructures. This initial effort will focus on a small set of diverse and representative locations that will serve as prototypes for other, similar cities. These locations will provide the science and technology community with a realistic environment to test maturing hardware and concepts and help determine how best to choose, deploy, and manage these technologies. Basic research will continue on structural integrity assessments, modeling, and sensors. One envisioned outcome is the evolution of integrated “smart buildings,” with advanced fire panels that provide detailed critical information to responders – including the relative safety and stability of the structure, as well as the location of occupants. Fully interconnected smart buildings would be interfaced with local and regional emergency operations centers to provide a detailed common operating picture. The initiative will also evaluate the utility and success of the

assessments program. In addition, we will work to expand the Regional Partnerships for Technology Integration to additional urban areas.

- ***Enhance IMAAC with an advanced system of tools.*** Integrate into IMAAC's existing suite of tools the capability to model complex atmospheric hazards within the urban environment for all CBRNE hazards. IMAAC predictions will feed into decision-support systems at the Federal, State, local, and tribal levels for a unified incident management approach providing a comprehensive, common operating picture to emergency managers. Predictions will include both atmospheric and waterborne hazards in a unified system of models that incorporate local weather from a systematic network of weather stations located throughout the Nation.
- ***Establish a UICDS nationwide, open architecture for command, control, communications, and intelligence.*** Working from existing systems, we plan to develop a UICDS system that provides all levels of emergency response with the best possible information in a timely, secure manner, including all source situational awareness and threat assessment. The system will advance effective incident command by coordinating logistical, strategic, and tactical information among Federal, State, local, and tribal agencies using interoperable technologies. To ensure success, the UICDS architecture must possess a progressive integration capability for sensors and other developing needs.
- ***Develop integrated all-hazard turnout gear.*** We will pursue the development of a one-suit-meets-all-goals body protection system containing integrated sensors (including portable CBRNE detectors), communications, location determination capability, and vital sign monitoring. While incorporating these new technologies, turnout gear also needs to remain durable, flexible, lightweight, and affordable. To help develop this sophisticated equipment, we will leverage current materials research and capitalize on DoD work for valuable test bed experience and user feedback. In addition to lab-prototyping next-generation PPE for all responders, we will evaluate preliminary research on portable CBRNE devices for responder vehicles.
- ***Provide technologies that will enable emergency responders to know the location and health status of all crew members and victims.*** Working from currently available technologies, we plan to prototype, field test and evaluate candidate location technologies, such as prospective 3-D locator systems, with the expectation that testing and market forces will drive product improvement. Prototype refinement will drive research and development toward a pager-sized unit with inputs to local as well as incident command. Ultimately, PPE should incorporate miniaturized, high-resolution units powered by long-lasting batteries that have vital sign transmission capabilities and CBRNE sensors.
- ***Improve respiratory protection equipment.*** Work in this area will focus on the discovery and demonstration of new materials and filter/mask designs that will prove effective against all toxins. Present improvement goals include achieving longer duration, lighter weight, and low breathing resistance for respiratory protection equipment. Ideally, masks would be responder serviceable and less costly. Another goal is to develop a methodology to transition a re-breather apparatus, which operates by extracting oxygen from the environment.
- ***Demonstrate new ways to neutralize chemicals, bacteria, or toxins on responders' clothing and gear.*** Building upon current DHS and DoD technologies, we will evaluate prototype technologies to provide effective on-scene CBRNE decontamination capabilities for responders and victims. This will include the development of interim sampling and analysis methods in support of a future rapid risk assessment expert system. The system would be based upon a scientific framework utilizing data and new modeling methods for cleanup determinations.

- **Ensure that municipal water systems are monitored and protected for a variety of chemical and biological toxins.** Work in this area will focus on evaluating the effectiveness of various water treatments for chemical and biological agents, as well as enhanced water system distribution models. Such systems should include a capacity for source tracing within distribution systems, as well as aquifer security. To achieve our goal of fully monitored water systems in all major urban areas, we will deploy early warning system designs and operational guidance for water systems.
- **Provide all responders, including reserve corps members, with electronic credentials linked to a national database.** Working from currently available systems and technology, we plan to demonstrate technologies for electronic credentials. This will require the development of a nationwide system confirming the identity, affiliation, and qualifications of responders. Having electronic credentials will help responders by making this information available in a fast, secure, and reliable manner. Research in this area will include investigating the use of biometrics as a universal identifier. In the future, we hope to have a fully tagged and identifiable responder workforce.
- **Develop training and education simulations for civilians and responders.** The focus of this work is on incorporating computer simulations of real-life situations into training for professionals as well as civilians. Efforts will produce online simulations reproducing emergency situations tailored to local environments – from appearance to interdependent critical infrastructure. Customizations for localities would include local maps, conditions, and equipment. In addition to providing responders a more accessible and scalable method to train for multiple scenarios, such systems would allow citizens to educate themselves in appropriate protective actions, thereby reducing the burden on responders. Another pertinent application is specialized training for transportation systems. Initially, to support further training program developments we will compile information about current and developing training programs and technologies, including evaluating and collaborating among Federal partners and other major training stakeholders to inventory existing capabilities.

The section below provides an overview of the near-, mid-, and long-term activities planned to accomplish these goals.

NEAR-TERM PRIORITIES

Regional Technology Integration Initiative

- Transfer and integrate existing and advanced homeland security technology systems to local governments.

Interagency Modeling and Atmospheric Analysis Center

- Incorporate all Federal modeling capability into a system of tools to address atmospheric CBRNE hazards. Leverage existing research to advance the accuracy of model predictions. Develop the IMAAC federation of modeling capabilities into a service-oriented automated reach-back prediction and analysis capability.

Unified Incident Command & Decision Support

- Establish a command, control, and communications architecture with progressive integration capability for sensors, responder coordination, logistics, scene awareness and other functions. Develop and test a prototype UICDS on a localized level.

Integrated All-Hazard Turnout Gear

- Devise new concepts for a one-suit-meets-all-goals body protection system, including the needs of police, firefighters, and Emergency Medical Services.

NEAR-TERM PRIORITIES, CONTINUED

- Location Technologies***
 - Develop prototypes that enable emergency responders to know the location and health status of all of their crew members, as well as those of victims.
- Respiratory protection equipment***
 - Discover and demonstrate new filter materials and mask designs for all toxins. Achieve a longer duration, lighter weight, and lower breathing resistance.
- Decontamination***
 - Demonstrate new ways to neutralize chemicals, bacteria, or toxins on responders' clothing and gear.
- Water Systems Protection***
 - Monitor and protect municipal water systems against a variety of chemical and biological toxins. This includes source tracing within the system, aquifer security, and early warning systems. Deploy early warning system designs and operational guidance for water systems.
- Electronic Credentials***
 - Provide all responders, including reserve corps members, with electronic credentials linked to a national database.
- Training and Education***
 - Develop training and education to enable civilians and responders to participate in online simulations, which simulate emergency situations.

MID-TERM PRIORITIES

- Regional Technology Integration Initiative***
 - Expand the Regional Partnerships for Technology Integration Initiative to additional urban areas. Integrate new solutions into existing systems to enhance an urban area's ability to prepare for and respond to incidents. Integrate models and sensors to monitor stability and other characteristics from a central location with connectivity to local emergency operations centers.
- Interagency Modeling and Atmospheric Analysis Center***
 - Develop advanced approaches to atmospheric modeling within the urban infrastructure. Establish accredited models for water hazards prediction.
- Unified Incident Command & Decision Support***
 - Working from existing systems, establish command, control, communications, and intelligence architecture with progressive integration capability for sensors and other developing needs.
- Integrated All-Hazard Turnout Gear***
 - Lab prototype next-generation PPE materials and nanotechnology for PPE that can be used by all responders, including firefighters, police and emergency medical technicians. Develop durable, flexible, lightweight, affordable all-hazard personal protection ensembles.

MID-TERM PRIORITIES, CONTINUED

- Location Technologies***
 - Refine prototypes, driving toward a pager-sized unit, with inputs to local as well as incident command. Field the capability to determine the location and well-being of responders and victims.
- Respiratory protection equipment***
 - Respiratory protection equipment
- Decontamination***
 - Provide effective on-scene CBRNE decontamination capabilities for responders and victims.
- Water Systems Protection***
 - Evaluate effectiveness of various water treatments for chemical and biological agents, including enhanced water system distribution models.
- Electronic Credentials***
 - Develop a nationwide system confirming the identity, affiliation, and credentials of responders. Evaluate the use of biometrics as a universal identifier.
- Training and Education***
 - Expand integrated communications systems and drills across all modes of transportation, and prototype response technologies, including specialized training for transportation systems.

LONG-TERM PRIORITIES

- Regional Technology Integration Initiative***
 - Bring to 50 cities fully interconnected smart buildings, interfaced with local and regional emergency operations centers for a detailed common operating picture.
- Interagency Modeling and Atmospheric Analysis Center***
 - Enhance IMAAC capability to include modeling within the urban environment, the incorporation of real-time weather from a national system of weather stations, and directly incorporate hazard predictions into decision support systems at the Federal, State, local, and tribal levels. Integrated hazard predictions will be made that consider all mediums including air and water together.
- Unified Incident Command & Decision Support***
 - Deploy a nationwide, open UICDS architecture for command, control, communications, and intelligence in support of local emergency response, including all-source situational awareness and threat assessment
- Integrated All-Hazard Turnout Gear***
 - Integrate portable CBRNE sensors, communications, and location technologies into all-hazard turnout gear.
- Location Technologies***
 - Integrate durable, miniaturized, high-resolution units with vital sign transmission, CBRNE sensors, and a long battery life into PPE.

LONG-TERM PRIORITIES, CONTINUED

- Respiratory protection equipment*** ▪ Develop methodology to transition a re-breather apparatus, which operates by extracting oxygen from the environment.
- Decontamination*** ▪ Enable a science-based support system for cleanup determinations based on framework data and new model methods. Develop interim sampling and analysis methods in support of a future rapid risk assessment expert system.
- Water Systems Protection*** ▪ Deploy fully monitored water systems in all major urban areas.
- Electronic Credentials*** ▪ Establish a fully tagged and identified responder workforce.
- Training and Education*** ▪ Provide remotely generated, on-demand, training simulations. Include customizations for localities, such as local maps, conditions, equipment, and infrastructure.

AGENCIES' ROLES AND RESPONSIBILITIES

The *Homeland Security Act of 2002* and a number of Homeland Security Presidential Directives lay out department and agency roles and responsibilities in the areas of Emergency Preparedness and Response, as shown below. Additional agencies have incident management responsibilities for prevention, preparedness, response, recovery under the *National Response Plan*³.

- Department of Commerce (DOC)*** ▪ Supports on-demand dispersion model predictions for nuclear, biological, or chemical events.
- Department of Defense (DoD)*** ▪ Works with DHS to leverage defense research and development for emergency response. DoD and DHS have agreed to facilitate the transfer and commercialization of DoD technologies for emergency response through the Emergency Response Networking Initiative.
- Department of Energy (DOE)*** ▪ Maintains National Incident Response Teams, which provide expertise for nuclear/radiological incidents and national security events.
- Department of Health and Human Services (HHS)*** ▪ Responsible for developing a catastrophic event mass casualty plan.
- Department of Homeland Security (DHS)*** ▪ Serves as the principal Federal agency for domestic incident management and is responsible for coordinating Federal operations to prepare for, respond to, and recover from

³ Specific agency roles and responsibilities are outlined in the Emergency Support Functions of the *National Response Plan* (Department of Homeland Security, December 2004). Departments and agencies with coordinating and support responsibilities include the Department of Agriculture, DOC, DoD, Department of Education, DOE, HHS, DHS, Department of Housing and Urban Development, Department of the Interior, Department of Justice, Department of Labor, Department of State, DOT, Department of the Treasury, Department of Veterans Affairs, EPA, Federal Communications Commission, General Services Administration, NASA, NRC, Office of Personnel Management, Small Business Administration, Social Security Administration, Tennessee Valley Authority, U.S. Agency for International Development, U.S. Postal Service, and the American Red Cross.

emergencies. Other Federal departments and agencies that support preparedness research and development activities are directed to coordinate their efforts with DHS.

Environmental Protection Agency (EPA)

- Leads development of decontamination guidelines and plans for recovering from a bioterrorism event.

National Aeronautics and Space Administration (NASA)

- Works with DHS to leverage aerospace research and development programs and facilities for emergency response.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Research and development efforts to support our Nation’s responders are dispersed across a broad range of departments and agencies, placing interagency coordination at the forefront of successful technology development and integration. The Department of Homeland Security (DHS) is actively involved in coordinating Federal research programs to ensure a cohesive structure that will better serve the needs of emergency responders.

An example of this research and development effort is the Interagency Modeling and Atmospheric Assessment Center (IMAAC), a collaborative effort among the Department of Commerce (DOC), Department of Defense (DoD), Department of Energy (DOE), DHS, Environmental Protection Agency (EPA), National Aeronautics and Space Administration (NASA), and the Nuclear Regulatory Commission (NRC). The IMAAC provides the single Federal prediction of atmospheric hazards and their consequences utilizing the best available resources from the Federal government for Incidents of National Significance. In the event of an Incident of National Significance, IMAAC will disseminate these predictions to Federal, State, local, and tribal emergency responders in a standardized, intuitive format that maximizes the utility of such predictions. Through the collaborative environment of IMAAC, developments in atmospheric modeling will be better coordinated and the results leveraged into a unified, national system of tools that address a full spectrum of threats. Many additional Federal government accomplishments and ongoing activities are highlighted below:

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Department of Energy (DOE)

- Continues to provide expertise through emergency response teams for nuclear/radiological incidents and national security. Teams are trained and equipped to respond and assist in many aspects of a nuclear accident or event, including everything from the characterization of radiological contamination to assisting in remediation of radioactive spills and treating radiation exposure victims.

Department of Health and Human Services (HHS)

- Awarded nearly \$3 billion to improve State and local health care capacity and increase hospital preparedness, including the development of CBRNE response plans.
- Maintains the Office of Public Health Emergency Preparedness to coordinate departmental efforts and Federal interagency responses public health and medical emergencies.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

HHS, continued

- Established and maintains the Strategic National Stockpile (SNS) of pharmaceuticals, biologicals, and other medical materiel. SNS assets, which include CBRNE countermeasures, may be required for emergency response to Incidents of National Significance.

Department of Homeland Security (DHS)

- Established the National Response Coordinating Center (NRCC) which now coordinates operational and logistical information among Federal agencies using new information technology tools.
- Working toward next-generation prototype full body protection for firefighters; dramatically improved self contained breathing apparatus; 3-D personnel locator; unified incident command and decision support system; and a new research program to revolutionize materials used in manufacturing Personal Protective Equipment (PPE).
- Developing technologies to facilitate simulation-based training and exercises to enhance incident management capabilities.
- Establishing a virtual “hub” to provide emergency responders and managers with information on equipment standards, test results, and funding options, as well as a forum to participate in peer discussions.
- Established the Office of Interoperability and Compatibility to strengthen the national partnership of Federal, State, local, and tribal and leadership to achieve emergency response interoperability in every community in the country.
- Established the Responder Knowledge Base (RKB). RKB provides emergency responders with a single source for integrated information on available equipment, equipment certification and standards, equipment training, cost resources, and reviews from other equipment users. RKB will also include the Interagency Board's Standardized Equipment List and the Office of Domestic Preparedness' Authorized Equipment List.
- Launched the Prepositioned Equipment Program (PEP). PEP consists of standardized equipment sets that are prepositioned in selected geographic areas to permit rapid deployment to States and localities whose jurisdictions have become the target of WMD terrorism. Highly specialized equipment, as well as off-the-shelf items, is stored in pods that are dispersed nationwide and are transportable by land or air within one-to-twelve hours after the initial request is made by appropriate authorities and approved by DHS.

Department of Transportation (DOT)

- Initiated a comprehensive security training program for local transit agencies.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DOT, continued

- Deployed CBRNE sensors in select transit systems. Provides response training for hazardous materials incidents in all modes of transportation.
- Established a 24-hour Crisis Management Center to bring all transportation system incident and response information into one place, with connections to all relevant Federal, State, and local agencies.
- Established a security notification system to communicate with State, local, and private sector stakeholders in the transportation system.
- Developing quick-response highway/bridge replacement technologies and bridge/tunnel stabilization programs.

Environmental Protection Agency (EPA)

- EPA is cooperating with DHS, DoD, and DOE to conduct research to determine contaminant distribution and dispersion in urban areas including the effects of the urban canyon and in determining how outdoor releases impact the indoor environment.
- EPA has evaluated shelter-in-place methods for residential and commercial buildings and is working with NIST to develop standards for shelter-in-place for commercial buildings. EPA is also conducting research to evaluate technology for improved sheltering in place, for example by using in-room air cleaners.

National Science Foundation (NSF)

- NSF and DoD have collaborated on research and development to advance the use of robotics in search and rescue efforts.

CHAPTER 7 – BORDER AND TRANSPORTATION SECURITY

INTRODUCTION

Historically, the United States relied heavily on two vast oceans and two friendly neighbors for border security and on the private sector for most forms of domestic transportation security. But the growth of the global transportation network, combined with present-day threat conditions, requires the development of a much enhanced border and transportation security infrastructure. One of our highest priorities is to prevent the entry of terrorists and the instruments of terrorism into the United States, while simultaneously ensuring the efficient flow of lawful traffic and commerce.

This responsibility falls squarely on the shoulders of the men and women at the Federal, State, local, and tribal level who support the Border and Transportation Security (BTS) Critical Mission Area, which is to develop and transition capabilities that improve the security of our Nation's borders and transportation systems without impeding the flow of commerce and travelers. There are four strategic objectives that define this mission area: (1) prevent entry of terrorists, criminals and illegal aliens; (2) interdict terrorist instruments and contraband at the earliest opportunity; (3) improve the security of U.S. transportation systems; and (4) facilitate the flow of commerce and travelers – identify, disrupt and dismantle entities that threaten the United States.

Securing our Nation's borders as well as its vast transportation system is no small task. The United States shares a 5,525-mile border with Canada and a 1,989-mile border with Mexico. Our maritime borders include 95,000 miles of shoreline and navigable waterways, as well as a 3.4 million square-mile exclusive economic zone and territories surrounded by water. More than 500 million people legally enter our country annually. An enormous volume of trade also crosses our borders every day. All people and goods legally entering the United States across these borders must be processed through an air, land, or sea port of entry.

Our transportation system is equally vast. International and domestic airports are dispersed throughout the United States. These airports and the thousands of planes that use them transport millions of passengers on tens of thousands of daily flights. Within the surface transportation network, approximately 6,000 agencies provide transit services through buses, subways, ferries, and light-rail service for approximately 14 million Americans each weekday. The U.S. highway system consists of 4 million interconnected miles of paved roadway, including more than 45,000 miles of Interstate freeway. Freight rail networks extend more than 300,000 miles, and commuter and urban rail systems cover some 10,000 miles. Virtually every community in America is connected to the global transportation network by the seaports, airports, highways, pipelines, railroads and waterways that move people and goods into, within, and out of the Nation.

Research and development in this area focuses on producing technologies and systems to enhance and coordinate our border and transportation protection capabilities. This includes improved screening, identification and sensing tools; integrated communication systems with alert capabilities; transportation infrastructure decontamination plans and technologies; and specialized countermeasures. In addition to addressing the vast expanse of our border and transportation networks, new tools and systems must also take into account the unique operational and technological requirements of different locations, such as official border entry and exit locations; the borders with Mexico and Canada; interior transportation routes; coastal areas and other waterways; as well as overseas and the high seas.

THREATS AND VULNERABILITIES

The American way of life is part of our Nation's great strength, but it poses an inherent vulnerability. We have a free and open society with a large, diverse, and highly mobile population. Our economy is based on a free-market system, predicated on the free and rapid movement of goods and services across our borders, as well as through the expansive rail, air, surface, and marine transportation systems within our borders. These economical and societal conditions, combined with vast borders that are in many locations porous, create vulnerabilities. Our society presents an almost infinite array of potential targets that can be attacked

through a variety of conventional and unconventional methods. Our greatest challenge is to protect our Nation while upholding the American way of life.

We face enemies who continue working to obtain and transport chemical, biological, radiological, and nuclear weapons across and within our borders for the stated purpose of killing large numbers of Americans. They also have the ability to use conventional means of attack, such as explosives and firearms, to inflict harm and spread fear.

For example, shoulder-fired MANPADS pose one of the most serious threats to civilian aviation. These systems are lethal, easy to use, and readily available on the black market. MANPADS have already been used against both military aircraft and civilian airliners, and although technology exists within the military to counter these weapons, none exists within the civilian sector. Although the Federal government already employs surveillance radar to monitor and track air traffic, shortcomings exist in monitoring aircraft approaching, crossing, and traveling within our borders.

While we must prepare to counter such threats, it is also important to remember that terrorists do not necessarily need to smuggle weapons into the United States to inflict large numbers of casualties and substantial property damage: sometimes they need only smuggle themselves.

REQUIREMENTS

To achieve mission success, science and technology developments for border transportation and security will need to support a broad range of capabilities. These capabilities are outlined on the following pages.

Surveillance and Monitoring

- Observation of specific targets or areas, continuously or at particular points in time. Remote surveillance is a primary way to monitor the country's vast borders and transportation systems and provides an important tool for law enforcement investigations. Border surveillance addresses land, water, air, and subsurface (i.e., tunnel) domains. The reality of today's security environment makes this area even more crucial. When previously we could be satisfied with simply reducing the influx of illegal immigrants and contraband, the consequences of allowing terrorists into the country means we must dramatically tighten our borders. It is recognized that surveillance is needed to push beyond the Nation's borders in gathering information and intelligence that will neutralize a threat before it materializes on United States soil.

***Communications
and Information
Management***

- Seamless acquisition, storage, distribution, and protection of information. This will allow operators at all levels of government to have a Shared Situational Awareness, which minimizes duplication of efforts between different assets, optimizes responses, and facilitates situational perspectives. This involves providing the following: (1) seamless, reliable, and affordable interoperable communications to all entities; (2) tactical data fusion to analyze multiple-source data; and (3) real-time, multi-modal access to databases of enforcement information. It also involves forming a common Concept of Operations (CONOPS) to establish uniform procedures and training. With shared situational awareness individual agents and officers as well as the operational command center will be able to geospatially locate all involved individuals in relation to potential targets, identifying friend or foe, accurately, in low light and adverse operational environments.

***Apprehension,
Detection, Seizure
and Removal***

- Take and maintain custody or control of items and people of interest. This involves functions such as: pursuit management and prevention, safe entry into unknown situations, arresting and case documentation, transporting, housing, securing and maintaining the integrity of seized and personal property, notification of right and consular notification. Automated, multilingual, real-time performance of these functions in all operational environments is essential.

***Identification and
Assessment***

- Rapidly and accurately determine and validate the identity of people and items and to determine their admissibility or status. This includes the identification of individuals through unique physical biometric attributes, document verification and validation, and the ability to perform veracity analysis. All of these observational tools, capabilities, and techniques are used to validate purpose, intent, and authenticity of people and their claims. Rapid throughputs, non-intrusive, safe, accurate, and reliable with low false positive identifications are essential characteristics.

REQUIREMENTS, CONTINUED

Targeting and Intelligence

- Acquire, analyze, and correlate data into meaningful information for the identification of potential items or parties of interest and disseminate this information to appropriate individuals and organizations. This includes the classification of specific threats. Long-term activities that support threat assessment, data collection, and analysis; intelligence preparation and support to operations; threat relevant data dissemination, and intelligence support to operational command are essential for this function. It should be emphasized that a “shape the battlefield” method needs to be taken, and that targeting and intelligence can not be addressed in isolation from detection, apprehension, and prosecution; therefore, a System of Systems approach is critical.

Officer Safety

- Protect officers from harm related to the border and transportation environment. This involves providing individual body protection in the form of appropriate personal equipment to counter or mitigate a specific threat. It includes specialty and multi-purpose counter chemical, biological, and explosive equipment, as well as lightweight ballistic, respiratory, hearing and vision protection integrated into day-to-day uniforms that are comfortable, flexible, and affordable. Additional needs include tools and equipment that allow for a safe search when trying to detect restricted or endangering items on individuals, their vehicles or possessions and safety and emergency equipment to protect officers or the public in a crisis situation.

Mine Countermeasures

- Processes, procedures, and techniques used to verify the presence and remove potential mine threats. The use of, or threat to use, mines (both at sea and on land) have already demonstrated pronounced economic impacts. Without any proof of their activities, terrorists can easily claim to have mined a particular area, creating large areas of access denial. Verification of mine presence and mine removal processes must be improved to minimize the time required to reopen the closure zone to free trade and travel.

Non-Intrusive and Non-Lethal Technologies

- To counter the increasingly sophisticated techniques of concealment for contraband, narcotic, and human smuggling in commercial cargo and conveyances with little or no economic impact, research and development of detection capabilities is required for mission success. Less-than-lethal ways for personnel and vehicle stopping to interdict illegal trafficking across the borders, which include automobiles, snowmobiles, and boats must also be researched.

Decontamination Technologies

- To develop and test decontamination, cleanup, and waste disposal technologies and to establish strategies to return contaminated pieces of critical transportation infrastructure to a pre-attack status as efficiently and quickly as possible.

GAPS

As threats to our borders and our transportation systems become more prominent, existing gaps will become vulnerabilities. These include:

- ***Surveillance and Monitoring*** – Although individual CBRNE sensors are currently being deployed and demonstrated in many border and transportation venues, a need exists for an integrated capability that is affordable and provides rapid CBRNE screening (both point and stand-off) with high detection probability and low false alarms across all transportation modes. In addition, better long-range detection of people and vehicles on land, surface and subsurface maritime platforms, and aircraft of all types approaching and crossing the border is needed.
- ***Communications and Information Management*** – Major challenges and gaps exist in providing the capability for seamless, interoperable communications and information management systems. Incompatible communications and information systems are just part of the problem: other challenges include multilevel information security requirements and independent and incompatible sensor data and information databases. The lack of a common, real-time picture of the location and status of operational units and threats exacerbates the situation.
- ***Apprehension, Detention, Seizure, and Removal*** – Gaps exist across all operational environments in the capability to apprehend, detain, seize, and remove items and people of interest. The capability to perform these functions on the high seas and in overseas locations is particularly challenging. In addition, although commercial equipment is available to address many of these needs, information on the performance of these systems in all operational environments is lacking.
- ***Identification and Assessment*** – Improved methods are required to determine personal identity and validity of documents or items presented to agents and officers.
- ***Targeting and Intelligence*** – Real-time intelligence fusion and improved predictive capabilities are needed.
- ***Officer Safety*** – Apprehending terrorists and criminals who possess and use increasingly sophisticated weapons and methods have placed our agents and officers supporting the BTS Critical Mission Area at risk. Gaps exist in all types of protective systems against hazards such as chemical, biological, radiological and firearms. Needs also exist for lightweight infrared and night vision systems and integrated communications.
- ***MANPADS Countermeasures*** – Technology exists within the military to counter the MANPADS threat, but the technology is costly to purchase and maintain. The need exists to determine the economic and operational viability and effectiveness of adapting this existing technology from the military to commercial aviation use.
- ***Mine Countermeasures*** – Neither mine countermeasure technology nor awareness have been integrated into State, local, and tribal emergency management plans.
- ***Transportation Infrastructure Decontamination*** – Strategies and technologies are under development to cleanup and decontaminate transportation infrastructure after a possible release of CBRNE materials.

STRATEGIC GOALS FOR 2015

By 2015, we aim to have advanced the capability of BTS Critical Mission Area agents and officers to instantaneously understand when a threat presents itself at borders or in the transportation system; and to

provide all relevant information to the appropriate decision makers and security forces, so they can mount an effective response.

This will allow us, through advanced surveillance and monitoring systems, to detect potential threats (people, land vehicles, surface and subsurface maritime platforms and aircraft of all types) at a great distance from our shores.

It will permit the integrated, rapid, accurate, and transparent non-intrusive inspection and associated information systems for point and stand-off detection of CBRNE materials, illegal drugs, illegal aliens, and other contraband in cargo-loaded trucks, in containers, on maritime vessels, and in aircraft.

It will allow us to seamlessly communicate and share information and knowledge at the Federal, State, local, and tribal levels. It will foster a shared awareness of the operational and tactical situation and a common understanding of the course of action among interagency operational forces.

To accomplish this goal, the following near-, mid-, and long-term activities will be undertaken:

NEAR-TERM PRIORITIES

Surveillance and Monitoring

- The Federal agencies concerned with securing our borders and transportation systems are making significant investments in increasing the overall national surveillance and monitoring capability. CBRNE detection, in particular, is receiving significant near-, mid- and long-term investments, as demonstrated by the establishment of the Domestic Nuclear Detection Office (DNDO). These capabilities will be transferred to Federal, State, local, and tribal officers and agents supporting the BTS Critical Mission Area. Investments in programs such as Border Watch and Transportation Watch will support surveillance needs.
- Border Watch – Develop an integrated land-based detection sensor network (augmented with airborne platforms and sensors for long-range, wide-area detection) to detect people and vehicles approaching/illegally crossing the U.S. border. Operationally demonstrate the capability of UAVs in a border application. Initiate an effort to integrate and expand the capability of first generation portal sensors to detect people and contraband coming through ports-of-entry.
- Transportation Watch – Initiate the development and operational demonstration of systems to detect threats to the transportation system, including integrated rapid screening and monitoring systems for all modes of transportation. Research how to address the threat of using transportation vehicles as weapons. Demonstrate an air cargo screening system and an enhanced air passenger screening system. Federal partners will work to maintain existing radar surveillance coverage and on possible replacement surveillance systems.

Communications and Information Management

- Interoperable and assured communications is a high priority at all levels across government. SAFECOM, the communications program shared by the Office of Emergency Communications and the Office for Interoperability and Compatibility, is intended to address interoperable wireless communications across all Federal, State, local, and tribal agencies supporting the homeland security mission. In addition, the BTS Critical Mission Area will focus on developing the architecture and processes to provide BTS officers and agents an integrated Shared Situational Awareness (Common Operational Picture) as well as allow them an enhanced ability to access information from all relevant Federal agency databases (Info Access).

Common Operational Picture (COP)

- Continue interagency efforts to integrate operational and tactical data (geo-location, identity, intent, characteristics, etc.) into a COP for all forces supporting the BTS Critical

Mission Area by providing real-time operationally relevant situational awareness information. This program will ultimately integrate DHS, DoD, Department of Transportation, DOJ, and Maritime Domain Awareness information and make it available to Federal, State, local, and tribal agencies. This Phase I effort will demonstrate real-time shared tactical situational awareness and a COP. Subsequent phases will expand the capability to other applicable Federal, State, local, and tribal entities.

- Info Access – Accelerate the development of and enhance the capability to query data across all relevant Federal agency databases to allow timely decisions and actions by agents and officers. Phase I efforts will demonstrate an interagency-wide ability to query high-priority databases such as DOJ criminal history databases. These databases provide fingerprint and other biometrics for visa adjudication, entry decisions at ports of entry, and apprehension of immigration violators. Phase I will also include an interagency effort to develop a set of common information elements for a Global Information Grid (GIG).

Apprehension, Detention, Seizure, and Removal (ADSR) Technologies

- Evaluate existing, commercial, off-the-shelf equipment to address high priority ADSR challenges such as a safe and effective means of pursuit management, automated detainee monitoring and tracking, and air filtering systems to remove potential airborne diseases brought in by detainees.

Targeting and Intelligence

- BTS Net – Initiate a program to fuse intelligence data across all BTS Mission Area organizations into a regional and national information understanding system. Demonstrate the Border Intelligence Fusion and Prediction System, which will incorporate relevant data held in other agency databases such as DOJ's Terrorist Screening Center.
- Safe Trip – Develop a program to enhance hazardous cargo safety through tracking and monitoring, as well as improving containment systems used for transporting hazardous cargo on roadways. Study methods of enhancing the survivability of passengers in a terrorist attack on any mode of transportation (air, rail, roadway, and maritime).

Officer Protection Technologies

- Accelerate programs to evaluate safety and emergency equipment for operational personnel. Evaluate technical characteristics and operational suitability of door breaching, night vision, hazardous material detection, and non-lethal disablement technologies.
- Hijack Stopper – Initiate a study to define the operational needs and identify potential alternative solutions to the problem of identifying, tracking, and non-lethally stopping non-compliant hijacked cars, trucks, ships, trains, or aircraft. Develop and demonstrate a near-term solution to identify and track hijacked trucks.

MANPADS Countermeasures

- Complete Phase II of the MANPADS Countermeasures program and provide the Administration and Congress with a recommendation for the most viable solution to defend against shoulder-fired missiles. Phase II will include development of prototype demonstrations using existing military or commercial technology, which will undergo a rigorous test and evaluation process.

Mine Countermeasures

- Develop a nationwide strategy to pre-position mine countermeasure equipment for seaborne and land based de-mining operations.

MID-TERM PRIORITIES

Surveillance and Monitoring

- Border Watch – Continue development of an integrated network to detect people and vehicles approaching and crossing the U.S. border. Expand this detection capability through the use of earth science applications. Demonstrate the capability to detect tunneling across border areas and low flying/slow aircraft at long range. Ultimately, Border Watch will help us to identify threats early and at a distance, providing maximum time to determine the optimal course of action and enabling a flexible response.
- Transportation Watch – Continue the development of systems to detect threats to internal transportation systems. Extend surveillance capability through automated scene understanding technologies for transportation hubs, including advanced, transparent, and rapid CBRNE screening systems for all modes of transportation. Integrate these systems and capabilities into regional command and control centers through Federal, State, local, and tribal cooperation. Work with the interagency Joint Planning and Development Office (JPDO) to integrate air security imperatives into its design of the Next Generation Air Transportation System.

Communications and Information Management

- COP – Continue a program to provide relevant, integrated, operational information to all BTS Critical Mission Area forces. Develop and deploy infrastructure, collection system, collaboration, and analysis technologies, including a common CONOPS (pre-planned responses, uniform processes, and procedures) that make Shared Situational Awareness a reality across all Federal, State, local, and tribal agencies supporting the BTS Critical Mission Area.
- Info Access – Enhance query and response capability across all relevant databases in Federal agencies. Particular emphasis will be on providing the capability to supply timely information that can be shared, consistent with multi-level security authorizations across all Federal, State, local, and tribal agencies supporting the BTS Critical Mission Area.

ADSR Technologies

- Evaluate existing commercial equipment addressing high priority ADSR requirements.

MID-TERM PRIORITIES, CONTINUED

Targeting and Intelligence

- Targeting System Program – Complete development of a next generation Automated Targeting System that fuses all source data into a knowledge-based system to target high-threat individuals, containers, and cargos.
- BTS Net – Develop and demonstrate technology to fuse intelligence data across all BTS Mission Area organizations into an information understanding system.
- Safe Trip – Enhance hazardous cargo safety through tracking and monitoring as well as improving containment systems used for transporting hazardous cargo. Develop systems and technologies that will enhance the survivability of passengers in a terrorist attack on vehicles in any mode of transportation.

Officer Protection Technologies

- Continue the evaluation of safety and emergency equipment for BTS personnel.
- Hijack Stopper – Develop a system capable of identifying, tracking, and non-lethally stopping non-compliant hijacked cars, ships, or railcars. Assess technologies to contend with hijacked aircraft, including aircraft diversion or detection of an aircraft no longer

under a legitimate pilot's control. Develop a means to remotely regain control of such an aircraft.

Mine Countermeasures

- Perform a technology refreshment assessment and execute procurements for low-risk technology enhancements.

LONG-TERM PRIORITIES

Surveillance and Monitoring

- Complete development of an integrated, rapid, accurate, transparent, non-intrusive inspection system for point and stand-off detection of CBRNE materials, illegal drugs, illegal aliens, and other contraband in cargo loaded trucks and containers. Current, near- and mid-term technology advances are focused on individual systems for the detection of specific threat material. A more integrated approach is needed to deal with the ever-increasing amount of traffic crossing our borders and with the ever-expanding list of potential terrorist threats. High throughput, high detection probability, and a low false alarm rate are just a few of the technical characteristics of such a system. Operational considerations such as size, cost, reliability, and maintainability will be considered.

Communications and Information Management

- Complete the development of a full scale, real time, interagency and international information sharing system that allows all participants to communicate knowledge and have a shared understanding of the security situation. This system would allow a collaborative response insuring that the right people and infrastructure are tasked, and would be supported by robust decision models to help people organize information and respond to an event. Development will include a robust and interoperable infrastructure, instituting multilevel security and privacy protection, and developing verified and validated decision models.

AGENCIES' ROLES AND RESPONSIBILITIES

The interagency community is working together to pursue research investments supporting the BTS Critical Mission Area. Some agencies, such as DoD, Department of Energy, National Aeronautics and Space Administration, DOJ, and DHS sponsor a wide range of research in BTS-related technologies. Research areas include surveillance and monitoring, communications, and information technology. These agencies and others, including Department of Commerce and DOT, sponsor mission-directed applied research in surveillance and monitoring technology development. In addition, DoD, DHS, the intelligence community, and law enforcement agencies support mission-directed applied research in areas of communication, information technology, targeting, and intelligence systems technology development. Coordination of these activities will continue to be performed through interagency working groups, such as the Technical Support Working Group (TSWG) and the newly formed BTS Science and Technology Interagency Working Group, the Joint Planning and Development Office (JPDO), and the Domestic Nuclear Detection Office (DNDO).

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

A number of new technology initiatives are underway at Federal departments and agencies, as described below.

***Department of
Homeland Security
(DHS)***

-

- Deployed advanced air passenger and baggage screening systems and initiated several pilot programs for Explosive Trace Detection Systems (ETD) of rail passengers.
- Deployed advanced non-intrusive inspection systems and radiation detection systems at ports of entry to screen trucks, vehicles, and cargos for terrorist devices and illegal contraband. Non-intrusive inspection and radiation detection systems, in many cases, give Customs inspectors the capability to perform thorough examinations of cargo without having to resort to the costly, time consuming process of unloading cargo for manual searches, or intrusive examinations of conveyances by methods such as drilling and dismantling.
- Established maritime intelligence data fusion centers where intelligence data from many different agencies is collected, correlated, and analyzed. A key element of maritime intelligence fusion is the fusion and discovery of data related to cargo security. DHS has implemented the National Targeting Center (NTC) and the Automated Commercial Environment (ACE) and is providing advanced data discovery and targeting algorithms. DHS has established Maritime Intelligence Fusion Centers (MIFCs) on the east and west coasts for both military intelligence and law enforcement sensitive information. The MIFCs fuse data from national sensors (National Security Agency [NSA]), National Geospatial-Intelligence Agency (NGA), and National Reconnaissance Office [NRO]) and theater sensors along with intelligence data from the joint Coast Guard and Navy National Maritime Intelligence Center to conduct analysis in coordination with Federal, State, local, and tribal enforcement and Intel agencies. They are “joint” in the broadest senses providing a critical top-down and bottom-up information and intelligence.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DHS, continued

- Developed and operated Hawkeye, a prototype to track and identify small boats in ports and coastal waters to prevent a terrorist attack stem the flow of illegal migrants and dangerous materials, weapons and illicit drugs into this country. This effort leveraged previous Coast Guard investments, and was used to support the 2004 election Republican and Democratic conventions in Boston and New York. Various aspects of Hawkeye are now being used at a total of six (6) ports: Miami, FL; Hampton Roads, VA; Charleston, SC; San Diego, CA; New York, NY; and Boston, MA.
- Developed an end-to-end model for border security operations, which provides insights to the overall economic and operational impact of proposed changes to border security procedures and policies.

- Deployed initial phase of Border Network (BorderNet) prototype, enabling Border Patrol officers to remotely access databases, sensor alerts and geo-spatial information via vehicle-mounted computers and handheld devices. Once fully deployed, this system will substantially increase the effectiveness and efficiency of the Border Patrol by providing border agents the information they need, when they need it.
- Tested a lightweight shipping container with embedded security features within its walls, doors and floor to detect intrusions. Shippers benefit from weight savings by allowing them to load more goods per container, encouraging the use of these more secure containers.
- Deployed the US-VISIT program, DHS's electronic entry and exit system, which also collects and matches biometric (e.g., fingerprints) information, on Jan. 5, 2004, to 115 airports and 14 seaports. In September 2004, it was expanded to include Visa Waiver Applicants. On Dec. 29, 2004, it was deployed to secondary inspection areas at the 50 busiest land border ports of entry. The program helps to secure our borders, facilitate the entry and exit process, and enhance the integrity of our immigration system while respecting the privacy of our visitors. US-VISIT checks biometrics (digital finger scans and photographs) for visa and admission applicants against a database of known criminals and suspected terrorists. This type of identity matching helps DHS personnel make better admissibility decisions and ensures the overall integrity of our immigration system. To date, more than 25 million visitors have been processed through US-VISIT without adversely impacting wait times, and over 600 criminals or immigration violators have been denied admission to the United States because of US-VISIT. The Department of State has used US-VISIT data to help deny over 3,000 non-legitimate visa applications.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DHS, continued

- Continuing Phase II of the Counter-Man Portable Air Defense Systems (MANPADS) Program is focused on demonstrating the viability, economic costs, and effectiveness of adapting existing military technology to protect commercial aircraft from the threat of Man Portable Air Defense Systems (MANPADS). The major thrust of this program is to demonstrate and evaluate the possible migration of existing technologies to the commercial airline industry, not to develop new technologies. The Development and Demonstration program will provide completed design solutions that will be fabricated, installed, tested, and certified for commercial aircraft to ensure the systems will be effective in the commercial aviation environment. The resulting countermeasure systems must have minimal impact on air carrier and airport operations, maintenance, and support activities.
- Recently procured an unmanned aerial vehicle (UAV) capability. Anticipated missions include many associated with border surveillance and assisting with transnational threats like illegal immigration, terrorism, drug trafficking, and customs violations.

Department of Justice (DOJ)

- Initiated a program to share criminal history and terrorist information with border agencies so that consular officers overseas, DHS inspectors at ports-of-entry, and DHS agents in the field can make better-informed decisions.

CHAPTER 8 – THREAT AND VULNERABILITY ANALYSIS

INTRODUCTION

Understanding the global threat environment and the scope of the Nation's vulnerabilities is essential for the United States to be successful in assuring the security of the homeland. Such understanding requires up-to-date and accurate knowledge of potential emerging threats as well as the actual, current, or presumed capabilities, operations, and objectives of known terrorists. Information is needed on the type of threat, what might be exposed to that threat (for example, people, agriculture, infrastructure, or economic sector), and the susceptibility to damage (that is, the vulnerability) of the element exposed. Furthermore, such knowledge must be available to guide a comprehensive response to the threat environment on three levels; namely, on a strategic or long-term basis to enable planning and preparation; for interdiction and investigation, as a tactical response to a coming threat; and on an urgent or immediate basis prior to and after a terrorist incident, so that proper forensics and remediation actions can be taken.

The knowledge and capabilities required for threat understanding must be multifaceted and wide-ranging, as well as timely and highly specific. The objective is to manage risk proactively by adopting knowledge-based measures that reduce the likelihood that threat agents are developed, vulnerabilities are exploited, and incidents develop into crises. Threat and vulnerability analysis is a new and different requirement for science and technology from that now being presented by the traditional intelligence and law enforcement communities. Tailored information, made available to a broad range of planners, analysts, and responders, among others, and informing their decision-making processes, is the distinguishing aspect of threat and vulnerability analysis for homeland security.

REQUIREMENTS

The catastrophic potential of today's threats to the homeland demands a new approach to security, warning, and defense that is more dynamic than the current intelligence analysis process and is specifically aligned with the decision-cycle times of those charged with the homeland security mission. The challenge of clearly understanding threats that may be as complex and potentially devastating as an explosion caused by an improvised nuclear device or a widespread attack with a deadly biological agent (potentially within the operational timelines required to act against such a threat) requires the Nation to exploit existing and developmental technologies comprehensively so that scientific knowledge and expertise can be brought to bear immediately. Reaching out to that expertise and accessing that information in the timeframes appropriate are essential.

In analyzing threats and vulnerabilities, the science and technology supporting the proposed enterprise will need to serve both planning and management functions and to provide multiple types of information to a correspondingly broad range of customers. System capabilities can be seen to support five distinct functions and activities which form a concept of operations:

- **Prepare** – Threats or attacks must be addressed through policy-making and strategic analysis; here, threat and vulnerability analyses must provide comprehensive strategic information that enables long-term planning for allocation of resources, countermeasures, and, if necessary, remediation measures.
- **Anticipate** – Accurate intelligence analysis and information synthesis as well as surveillance, performed by a diverse group of analysts, will enable the homeland security community to anticipate specific types of attacks or threat agents.
- **Prevent** – Analyses can prevent or halt planned attacks through active investigation and interdiction, by various Federal, State, local, and tribal law enforcement agencies.
- **Detect** – Threat and vulnerability analyses can inform the development and deployment of environmental detection capabilities for forensics and medical countermeasures.

These will be used by emergency responders, medical personnel, as well as investigative personnel.

- **Restore** – Rapid, effective restoration through decontamination and remediation requires understanding of vulnerabilities to and the consequences of various threat agents. The infrastructure, tools, and interactions available must be sufficiently developed to enable diverse types of actions to be undertaken by various Federal, State, local, and tribal government agencies either immediately or over a longer term.

GAPS

The *Homeland Security Act of 2002* specifically addresses the need for ongoing threat and vulnerability analysis. An integrated set of such knowledge synthesis tools, which is capable of handling massive amounts of data of multiple types and distributed among many disparate information sources, does not exist. Furthermore, capabilities for providing timely, relevant information to the diverse users constituting the homeland security community are lacking. In that regard, the Nation does not possess enough genuine scientific and technical expertise to instantiate multiple research activities or centers in support of multiple organizations charged with the homeland security mission. Furthermore, the scientific and technical workforce upon which such research and analytical activities must draw is declining.

Additionally, mechanisms for evaluating and integrating technologies with processes in real operational scenarios do not exist throughout most of the diverse national and local assets that are responsible for homeland security. Understanding threats and vulnerabilities on such a manifold basis requires large-scale test beds, pilot programs, and demonstration projects, which do not currently exist. Also lacking are venues in which systems engineering activities are directly and immediately incorporated into research and development efforts. Likewise, despite the staging of occasional, locally or regionally focused exercises in which investigators, public safety and health, and emergency responder communities, among others, evaluate their coordinated responses to terrorist incidents or national disasters, there has been an obvious lack of exercises focused on the coordination of analytical, investigative, and interdiction activities required for predicting, anticipating, and interdicting terrorist attacks.

STRATEGIC GOALS FOR 2015

This plan envisions for 2015 a nationwide enterprise providing the knowledge required to maintain an awareness of threats to the homeland and also to understand its vulnerabilities to a broad range of attacks. This enterprise will include computing, telecommunications, and expert services that ensure its continued operation, as well as a research and educational infrastructure to support its continuing growth. Analogies to this enterprise are the current National Weather Service and the National Aeronautics and Space Administration.

To achieve the vision described in the opening paragraphs of this chapter, a science and technology program building upon many ongoing federally directed efforts but requiring new scientific and technological discoveries is proposed. That program is structured to create a national-level capability providing all those charged with the mission of homeland security a single, authoritative source of scientific and technical knowledge for understanding threats and vulnerabilities. Enabling this capability is a complete end-to-end system that provides immediate, local- or national-level awareness of the threat and vulnerability environment.

The system includes a geographically distributed network of information sources, computer-based tools, and subject matter expertise linked through a secure, flexible, and privacy-enhancing high-performance communications architecture, coordinated by a control center that ensures users have immediate access to the knowledge necessary for the successful execution of the homeland security mission. More importantly, this concept not only capitalizes on existing expertise but makes the sustained investments required to educate and train the future generations of experts, as well as support research dedicated to supporting the real-world missions of homeland security practitioners.

Science and Technology

To implement this proposed threat and vulnerability analysis program, science and technology efforts will focus primarily in four areas: visual analytics; knowledge discovery and synthesis; modeling and simulation; and information security and privacy. The goal of such efforts, especially the first three, is to transform an awareness of past events and current situations into an understanding of the potential, future threat environment so as to marshal appropriate, effective countermeasures.

- ***Visual Analytics*** – Make accessible and enable analysis of massive amounts of disparate, distributed data of multiple types to create the timely, highly specific or in some cases comprehensive threat and vulnerability understanding required for diverse homeland security purposes. Pattern and link analysis tools and modern data visualization techniques represent the current generation of advanced capabilities available.
- ***Knowledge Discovery and Synthesis*** – To anticipate, prepare for, preempt, and protect the Nation’s people, assets, and resources from terrorist attack requires building a strong capability for prospective understanding of threats rather than retrospective analysis of collected information. Such understanding, coupled with precise knowledge of vulnerabilities, will enable both an accurate determination of risks and a realistic allocation of resources to counter potential terrorist actions.
- ***Modeling and Simulation*** – These efforts develop simulation and knowledge management capabilities for a myriad of homeland security applications. These capabilities will be used to improve scenario planning and emergency response, design better chemical, biological, and energetics detectors for border protection, enable vulnerability assessments and consequence analyses for infrastructure protection, and accelerate information extraction and knowledge discovery for threat identification and analysis.
- ***Information Security and Privacy*** – Securing the communications and exchange of data and other information among the various members of the homeland security community, whether they are intelligence agencies or law enforcement agencies or public health organizations, will be critical to timely threat understanding and response. Likewise, ensuring the privacy of the information potentially available in the many, distributed databases and information sources will help guarantee that our values are protected, and ensure continued public support of the Nation’s counterterrorism efforts.

Supporting Infrastructure

Supporting the science and technology efforts will require establishment of a technical and knowledge base. The National Homeland Security Support System (NHS3), comprising three fundamental components, would be established as a venue for the application of the new science and technology. The NHS3 capability will serve, among other functions, as a homeland security knowledge clearinghouse. It will support data analysis, synthesis, and integration to provide targeted information dissemination and net assessment support.

- ***Distributed Knowledge and Expertise*** – This is the scientific and technical knowledge that resides across the country in universities, industry, national laboratories, and Federal, State, local and tribal government organizations. Such knowledge and expertise must be identified, organized, focused, and networked against the threats the country faces.
- ***Enabling Infrastructure*** – Practical realities dictate existing and future expertise be nurtured in place, wherever it resides, requiring dedicated infrastructure that allows real-time access to that expertise as required by the operational timelines of any given homeland security mission. A dedicated, robust, flexible, and secure infrastructure – primarily built on computational and communications capabilities and supported by extensive modeling and simulation – must be built unlike any that currently exists in the homeland security context. That infrastructure should provide a seamless, interoperable

information exchange environment which is based on a common enterprise architecture supported across the homeland security community. Success will require new, and perhaps novel, concepts of operation to be effective.

- **Mission Support Center** – Arguably the component of the proposed homeland security support capability that likely is the most difficult to develop is the requisite decision support center for coordination and control of response to users of the capability. This Mission Support Center (MSC) is unlike anything that exists today, staffed with specialists yet to be recruited and trained, equipped with state-of-the-art supporting technology, and building on relevant capabilities of command and control capabilities in use by DoD as well as highly specialized intelligence analysis centers.

To accomplish these goals, the following near-, mid-, and long-term activities will be undertaken:

NEAR-TERM PRIORITIES

In the near-term, science and technology efforts will focus on developing a Federal-level enterprise for threat and vulnerability analysis. Visual analytics, knowledge discovery, and modeling capabilities appropriate to federally managed information sources and information security and privacy tools required to share information and collaborate among the various Federal government organizations involved with homeland security will be investigated and implemented. The NHS3 will become the focus of the threat and vulnerability analytical enterprise. It serves as the main contact point at DHS for providing direct support to those operational elements that require expert and authoritative support to critical decision making. These decisions span the gamut – from determining the proper mix and level of a national vaccine stockpile to assisting an officer at a border crossing (as that officer examines suspicious cargo and requires support to decide if that cargo can pass, or should be subjected to, additional security screening). In this timeframe, NHS3 will capitalize on existing expertise and begin to apply existing and developmental support infrastructure (e.g., advanced communications concepts, modeling and simulation, visual analytics tools, and decision-support systems).

Science and Technology

- **Visual Analytics** – Develop capabilities for 3-D clustering, timeline analyses, and dynamic updating of information collections containing hundreds of thousands to millions of documents. Establish five-to-ten regional centers at universities, industry, or government facilities to support the national visual analytics capability.
- **Knowledge Discovery** – Develop automated extraction from data sets of at least one billion records and inclusion of audio and image data with currently available text data. Develop pattern learning capabilities for historical data and near real-time application to new data and automated correlation of characterized threats with known vulnerabilities.

Science and Technology, continued

- **Modeling and Simulation** – Develop high-resolution dispersion modeling for indoor, surface water, and urban environments and scalable knowledge management architectures.
- **Information Security and Privacy** – Develop real-time auditing capabilities to ensure information security and privacy, trusted technologies for interchange of data across networks of dissimilar classification levels, and extension of virtual private network technologies to wireless devices.

Supporting Infrastructure

- Establish cross-agency facilities for technology evaluation, transfer, and insertion and stage joint exercises that enable coordination of investigators, analysts, and responders. The first will provide formalized, coordinated methods for evaluating and integrating current and emerging technologies for potential implementation across the threat and

vulnerability analysis complex. The latter will test, through exercises and experiments, the interactions of the personnel and technologies responsible for understanding and responding to threats and vulnerabilities.

Development of Accurate and Rapid Response Systems to Intelligence on Terrorist Threats

- The Federal government will develop communications and intelligence capabilities that coordinate intelligence assessments between local law enforcement and Federal intelligence sources. Accurate assessment of locally gathered intelligence depends critically on local context and other local intelligence inputs. Regional intelligence networks are best able to connect and respond to emerging intelligence warnings. Timely and coordinated intelligence communications between Federal and regional units will enable enforcement agencies to marshal and deploy forces to prevent potential terrorist acts.

MID-TERM PRIORITIES

In the mid-term, the threat and vulnerability analysis enterprise will begin to mature its infrastructure and operational concepts as well as more clearly define technological and scientific requirements to support homeland security operations. Established is a threat and vulnerability analysis complex of widely distributed, public and private sector interconnected experts who share information freely and who undertake advanced cognitive analyses in a collaborative way, across domains of any scale, using a shared service-oriented architecture capable of functioning in both a web-services-like “center-based” mode, as well as in an “edge-based,” peer-to-peer manner.

The complex would rely on a platform hosting shared data and applications that would enable its users to work within secure, virtual environments across traditional organizational boundaries; a platform for sharing data and information processing resources to enable users to easily and securely expose shared resources to the larger community; and a collection of security, registry, and other services that will permit the interaction of enterprise services and edge-based collaboration.

Science and Technology

- ***Visual Analytics*** – Develop and implement the next generation of capabilities. These rely on multi-dimensional visual analytics to present simultaneously historical and current information and depict possible threat situations. The focus of visualization becomes the real-time synthesis of multiple information sources and data types to allow quantitative projection of threats, rather than analysis of static data sets. Capabilities for real-time imagery analysis are particularly important here.

Science and Technology, continued

- ***Knowledge Discovery*** – Focus efforts on developing capabilities for automated extraction from structured data sets of up to one trillion records, including video and other scientific data; automated group detection and graph matching capabilities; automated, dynamic pattern learning for real-time analysis; and high-speed transaction processing of metadata.
- ***Modeling and Simulation*** – Develop high-resolution dispersion models operating in near real-time and probabilistic risk assessment capabilities with accurate confidence measures for all CBE threats, as well as establishment of shared, high-performance computing resources.
- ***Information Security and Privacy*** – Develop new data architectures encompassing information security and privacy attributes, which are usable for multiple data types and modes; asymmetric cryptographic labeling schemes; and real-time encryption and decryption capabilities for cross-domain information sharing.

Infrastructure Protection

- Establish the processes, facilities, and networks that constitute the NHS3 (as described above); an automated capability for prioritizing incident reports for asset allocation and tactical/strategic response (based on the next-generation data science, pattern recognition, high-speed transaction processing, and advanced computing resources being developed under the science and technology efforts described above); as well as a common, high-bandwidth network infrastructure linking all members of the homeland security community.

LONG-TERM PRIORITIES

In FY 2010 and beyond, science and technology efforts focus on refining and integrating the capabilities developed. The new functionality will encompass, among other capabilities: automated collection, conditioning, and full-language processing; data transformation; entity detection/ identification/ resolution; large-scale analysis; link and pattern detection; as well as structured and unstructured database integration with efficient searching, filtering, categorizing, and converging functions that facilitate reasoning about the capabilities and intents of individuals or groups.

The system will support hypothesizing probable futures even in the presence of incomplete data, assessing risk, reasoning and model-building, evidence examination and structured argumentation for sharing, discussing, and debating a diversity of possibly very different viewpoints among users. The tools will facilitate predictive estimation; developing, visualizing, publishing, and presenting options for decisions; and virtual collaboration. Meanwhile, the system will provide functional yet easy-to-use security across domains of varying classification levels, strengthen encryption algorithms, include immutable audit-trail capability for investigatory purposes, and ensure full privacy protection for U.S. persons.

Also established is an ongoing support activity which will include sponsoring educational programs in areas where national expertise is thin or does not exist, supporting scientific research in key areas to include advancing requisite tool development, and continuously interacting with the intelligence, law enforcement, and public health communities to ensure a meaningful information collection effort. Finally, MSC staff will respond daily to tasking from operational elements and continuously refine policies, procedures, and response capabilities while comprehensively collecting data from users seeking expert guidance that will be used to identify needs and continuously improve the system.

By 2015, the threat and vulnerability analytical enterprise will become a mature, nationwide, and operationally responsive organization staffed by specially trained professionals and supported by a rich network of the country's experts in all areas relevant to contemporary threats. University programs will be producing the next generation of experts and homeland security science and technology leaders, technology developers will be providing needs-driven solutions as determined by the gaps definition process, and homeland security operators will have high confidence in the authoritative support they are receiving.

AGENCIES' ROLES AND RESPONSIBILITIES

The *Homeland Security Act of 2002* assigns coordination responsibilities for threat and vulnerability analysis within the Federal government to the DHS. Furthermore, various Homeland Security Presidential Directives also require such analysis to be performed to ensure the security of the homeland. The specified role of DHS in such activities is to access, receive, and analyze information and intelligence from other Federal, State, local, and tribal agencies and private sector entities and to integrate such information to identify threats and then better understand them in light of the Nation's vulnerabilities. The recently established NCTC, the CIA Counterterrorism Center, and the various national assets now managed by DoD and the intelligence community represent just a few of the organizations with contributory roles for homeland security.

Just as threat and vulnerability analysis depends on the activities of a broad public and private sector coalition, establishing and implementing the science and technology program is best shared among the members of the intelligence and law enforcement communities. A steering group has already been

established within the Federal government for guiding future research in threat analysis. Current members include the following agencies: CIA, DoD, DHS, DOJ, Department of State, National Security Agency, NCTC, Department of Energy, and the National Institute of Standards and Technology. This group should be charged with developing the program and sharing authority for implementing the various research and development efforts.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

The Federal government has already taken some steps focused on providing a threat and vulnerability analysis capability. Several organizations have also established research and development programs focused on information analysis. There are many research efforts underway within the intelligence and law enforcement communities focused on information analysis.

Department of Defense (DoD)

- Created a Homeland Defense Domain Awareness Working Group which has worked for the past year on developing recommendations on the roles and responsibilities of the DoD in homeland security.
- Established the Joint Intelligence Task Force-Combating Terrorism to collect, analyze, and disseminate terrorist threat information.
- Responsible for homeland defense and has established the Combined Intelligence Fusion Center to provide analysis and fusion of terrorist-related information.
- Operates a Combined Intelligence Watch Center (CWIC) (also known as the Combined Intelligence Center [CIC]) that serves as the indications and warning center for worldwide threats from space, missile, and strategic air activity, as well as geopolitical unrest that could affect North America and U.S. forces and interests abroad.
- Operates a Space and Warning Systems Center (SWSC) that is responsible for the maintenance and evolution of mission-critical software meeting operational requirements for DoD centers responsible for national attack warning and assessment and space surveillance, defense, and control.
- Operates a National Warning Facility that is the US civil defense warning center to provide FEMA with access to warning information at the same time it is available to DoD. In case of attack, the center would relay the message over the civilian alerting circuits of the National Warning System (NAWAS).

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DoD, continued

- Developed software to provide analysts with automated tools and methods to process, analyze, and integrate information drawn from any U.S. Government, commercial, or public domain database. This software enables drastic reduction in the time spent on projects by exploiting significantly larger amounts of information than was possible before. Users are able to sort, arrange, compare, retrieve, and visualize the contents of thousands of documents at a time.
- Develops and manages DoD Counterintelligence (CI) programs and functions that support the protection of DoD, including CI support to protect DoD personnel, resources, critical information, research and development programs, technology, critical infrastructure, economic security, and U.S. interests, against foreign influence and manipulation, as well as to detect and neutralize espionage against DoD.
- Provides continuous intelligence analysis of cyber threats, operates a network of Computer Emergency Response Teams which are staffed 24/7 to identify, mitigate, and, if necessary, respond to cyber attacks, and coordinates DoD's law enforcement and counterintelligence organizations in response to cyber incidents.
- Deployed a Central Intelligence Agency web-based, collaborative common virtual workspace that provides secure dissemination of both raw and finished intelligence to military commands and selected US government agencies. This capability provides timely intelligence and warning of terrorists' actions against US forces.
- Performs the engineering development of software and automated information operations (IO) techniques to streamline the processing, integration, exploitation, display, and dissemination of strategic and tactical threat assessment intelligence information from to produce integrated, predictive air and space intelligence to enable military operations, force modernization decisions, and policymaking.

Department of Homeland Security (DHS)

- Established a National Visualization and Analytics Center supported by a consortium of regionally based university, industry, and government centers to explore and transfer new technologies for visually analyzing massive amounts of multimodal data from disparate sources.
- Established an Institute for Discrete Sciences, also supported by a university and industry consortium, to research and develop new data management techniques for handling massive, diverse data sets and high-resolution modeling tools for use in complex urban and indoor environments.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DHS, continued

- Created a specialized Biodefense Knowledge Center which will be a component of the National Biodefense Analysis and Countermeasures Center. It will encompass analytical capabilities, a bio-encyclopedia, modeling and simulation capabilities, a situational awareness center, visualization and collaboration tools, as well as communications capabilities for involving biothreat subject matter experts in biothreat assessments.
- Established a unique coalition of homeland security stakeholders from across government research, intelligence, and law enforcement agencies through the Interagency Center for Applied Homeland Security Technology (ICAHST). This coalition is tasked with developing a broad-based technology research, testing, and prototyping capability.
- Developed and implemented a Threat-Vulnerability Integration System, to support DHS's mandated mission to compile threat and vulnerability information. This system includes modern analysis tools as well as collaboration and visualization capabilities.
- Maintains nuclear assessment and weapons of mass destruction assessment programs to provide analysts with information on the credibility of communicated nuclear threats and the capabilities of various state and non-state groups to develop and deploy threat agents.
- Established a comprehensive social-behavioral research program to understand and model the radicalization and motivations of terrorists and their intent to commit terrorist acts. Combined with assessments of the all-weapons of mass effect capabilities of terrorist groups, this program enables accurate determination of terrorist threat.
- Exploring and implementing new science and technology that enable comprehensive analysis of chemical, biological, and explosive threats.

Department of Justice (DOJ)

- Established an Office of Intelligence as well as a Counterterrorism Division, both of which include cells of analysts working counterterrorism issues.
- Established the National Joint Terrorism Task Force. It is staffed by Federal, State, local, and tribal agencies and will serve as the "point-of-fusion" for terrorism information by coordinating the flow of information across the country.

Central Intelligence Agency (CIA)

- Established the National Counterterrorism Center (NCTC). The NCTC includes analytical staff from the intelligence community, the Federal law enforcement community, and DHS.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

CIA, continued

- Established and currently manages the Intelligence Technology Innovation Center (ITIC), which is funding multiple programs seeking new approaches to information analysis and threat understanding. The ITIC and DHS are supporting a large research and development effort in knowledge discovery and dissemination for the intelligence community. The multi-agency Technical Support Working Group has ongoing efforts in similar areas.
- Has operated the CIA Counterterrorism Center for many years, which has recently taken on new importance and a significant role in the analysis of intelligence related to terrorism.

Environmental Protection Agency (EPA)

- Established an Office of Homeland Security (OHS) to serve as the Agency's central liaison for homeland security matters. OHS works closely with the White House Homeland Security Council, Department of Homeland Security, and other Federal agencies as it coordinates overall EPA homeland security strategy.
- Established the National Homeland Security Research Center (NHSRC) within its Office of Research and Development. The NHSRC research focuses on enhancing the ability to detect, contain, and clean up in the event of such attacks. NHSRC has developed threat assessments to determine research priorities related to indoor and water environments and is currently developing a threat assessment for outdoor environments.
- Developing an Emergency Consequence Assessment Tool (ECAT) through the NHSRC to enhance the ability of risk managers to respond to potential terrorist attacks more quickly and efficiently by functioning as a defensive "playbook" that is based on a series of priority threat scenarios and allows site-specific applications in the event of an attack.
- Provides decision makers with appropriate, effective, and rapid risk assessment guidelines and technologies to prepare for, detect, contain, and decontaminate chemical and biological attacks against buildings and water treatment systems through NHSRC.

National Science Foundation (NSF)

- Supports research on visualization, knowledge discovery, and modeling, information privacy and security, and modeling and analysis of dynamic systems to anticipate and prepare for threats and vulnerabilities.
- Supports research performed in cooperation with the intelligence community in areas of mathematics, energy sources, sensors and detectors, image processing and optical spectroscopy.

CHAPTER 9 – SOCIAL, BEHAVIORAL AND ECONOMIC SCIENCES

INTRODUCTION

The knowledge and methods of the social, behavioral, and economic (SBE) sciences are directly applicable to the design and implementation of an effective homeland security strategy. The SBE sciences can enhance the understanding of the behaviors of both terrorists and their targets, improve the ability to anticipate and detect threats, support the development of optimal short-term and long-term preparation and response strategies, and provide guidance in remediation and restoration of those communities and areas affected by an attack or catastrophic event. The SBE sciences contribute directly to our responses to terrorism and our understanding of terrorist networks and the social environments in which they operate. These sciences also complement other science and technology RDT&E that addresses topics related to homeland security. In some instances, the SBE sciences amplify the strength and effectiveness of the countermeasures described in preceding chapters; in other instances, they enable such countermeasures. The SBE sciences are uniquely suited to produce an informed, science-driven knowledge base that can serve to counter potential adversarial behavior, provide the means to reduce or remove its precipitating factors, and prepare for and respond to its potential impact.

REQUIREMENTS

The considerable operational experience gained by the law enforcement, intelligence, and counterintelligence communities in the United States is relevant to confronting various homeland security challenges. The application of current capabilities and knowledge within the SBE sciences to develop effective threat, risk, and vulnerability assessments and communications, response and recovery capabilities, and countermeasures requires testing of such capabilities and knowledge within the venues of concern to the homeland security community. Where current knowledge is lacking, further application of the SBE sciences will depend on advances in the theoretical and empirical domains of these sciences.

GAPS

Policies, strategies, and tactics to combat terrorism should seek to preserve American values while simultaneously reducing terrorist threats, U.S. vulnerabilities, and the potential consequences of terrorist attacks. Unfortunately, gaps exist in our application of the SBE sciences to further these efforts.

- ***Integration of SBE Sciences Into Response and Operational Capabilities*** – There exists in Homeland Security inadequate consideration and integration of the SBE sciences in the efforts to confront and prepare for terrorism. Consequently, deterrence efforts against individual adversaries and potential adversary networks may fail for lack of understanding about how these are formed, function, thrive, and deteriorate. In addition, lives may be lost, casualties may increase, and productivity and quality of life may suffer in the near- and long-term if preparedness, response, and recovery plans fail to model accurately or otherwise take into account basic human behaviors under conditions of extreme stress and threat. They do not sufficiently do so now.
- ***Insufficient Database Infrastructure*** – Homeland Security SBE researchers and decision makers reliant on SBE research outcomes are hindered by the lack of robust data sets that are relevant to the current terrorist threat, especially data on precursor indicators and after-effects. The amount and nature of information available to the scientific, intelligence, and law enforcement, communities is growing exponentially so that the potential for the construction of robust data sets has become a reality. However, this information often is not collected systematically which reduces its potential to form the basis of scientific endeavors, inform policy, or take advantage of knowledge mapping tools and the computational and dynamic models that are being developed.

- ***Insufficient Access to Information Management Tools and Modeling Capabilities*** – The current substantial investment in data collection, processing, and visualization may yield payoffs that quickly overwhelm analysts’ ability to absorb, capitalize, and put information to traditional and novel uses. Researchers in the SBE fields need further development of information management and modeling tools to aid in the interpretation and usefulness of information contained in large and diverse data sets on terrorist incidents.
- ***Insufficient Evaluative Data*** – An understanding of how individuals assess trade-offs between productive efficiency and security, and private incentives and broader societal benefits of security investments is required. Tools such as risk assessments may be necessary to translate individual choices and security measures into calculations of productivity and protection for the Nation as a whole. Such evaluative data would allow policy makers to understand better the elasticity of implemented and planned response strategies, particularly with regard to the public’s desire for such measures and willingness to comply.
- ***Insufficient Understanding of the Basic Mechanisms of Behavior at the Individual and Group Levels*** – There are various knowledge deficits that may be remedied by advancements in the SBE sciences. Such advancements may provide insight regarding how to measure and understand the basis of individual differences; construct and evaluate models of brain functioning that usefully map onto known behaviors; make explicit the principles governing interactions among individuals, groups, and populations; and integrate effectively robotic and artificial sensing, motor, and cognitive enhancement technologies with humans at the individual and group levels.

STRATEGIC GOALS FOR 2015

The Federal government has already undertaken and plans to invest further in building a science-driven knowledge base to counter potential adversarial behavior, provide the means to reduce or remove its precipitating factors, and prepare and respond to its potential impact. It seeks to make better use of existing SBE research on threats and vulnerabilities, while simultaneously advancing the state of the SBE sciences and our understanding of terrorist behaviors and society’s responses to them.

By 2015, the goal is for the U.S. government and its academic and private sector partners to have put in place strategies to prevent, deter, prepare for, and respond to terrorist events. To ensure that these strategies are informed by the SBE sciences, investments in the following capabilities will be made in the near-, mid-, and long-term.

NEAR-TERM PRIORITIES

- ***Understanding the Threat of Terrorism*** – Federal government efforts are underway today to apply SBE knowledge, tools, and models to the formation, development, activity, and demise of terrorist networks and their targets as a means to exploit existing fissures or create new ones in the threat environment. Models that may prove particularly fruitful include dynamic game theory; cognitive and emotional schemas to create intellectual empathy; models of communications processes and media uses and effects; behavioral and neurobiological measures and models of motivations, intent to harm and deceive; and determinants of migration politics. The role of economic, political, and cultural globalization in the development and maintenance of terrorist groups is a corollary line of inquiry, as are efforts to understand consequences of a terrorist threat or incident. We aim to be able systematically to apply basic economic research and forecasting techniques, such as time series analysis of financial data, rational expectation, and other decision-making models, and tools to analyze economic dynamics to reduce the likelihood of a severe economic shock in the aftermath of an attack.

- ***Application of SBE Science to Preparedness, Response, and Recovery Capabilities*** – The creation of a solid infrastructure for SBE sciences data collection, analysis, and dissemination is central to the development of a robust capability to conduct threat assessment and to prepare, respond to, and recover from a potential adversarial attack. Geospatial, demographic, economic, and health-related longitudinal and experimental data are essential to this enterprise. Preparedness efforts can take advantage of improved research methods to assess vulnerabilities and hazards in order to address the consequences of terrorist attack operations. Absent intrusive and costly government command and control regulation, incentives to encourage adequate security investment in the private sector must be developed using principles of economic science. Inexpensive and powerful information technologies, in conjunction with micro- and nanotechnologies, can significantly enhance public health and safety, provide for timely, accurate, and reliable emergency response, and enhance training and learning opportunities including the training of emergency personnel. Response and recovery efforts can take advantage of capabilities regarding early indicators of short- and long-term impairment following exposure to a traumatic event; the identification of vulnerable and resilient individuals, groups, and communities; methods for encouraging adherence and compliance to public health guidelines during disasters; and connecting urban and rural health care facilities for health surveillance and health care.

- ***Application of Decision Science Methods to Risk Communication Strategies*** – The Federal government will improve capabilities to assess risk perception among the public at large and among Federal, State, local, and tribal emergency responders. Improved capabilities will generate mechanisms to ensure that assessments keep pace with public perceptions and are readily available to those who disseminate risk messages. Assessment of public perceptions of risks and strengths can be used to construct public messages that facilitate appraisal of risk and guide public behavior to maximize personal and public safety and vigilance. Research on effective communication strategies among various groups, including diverse cultural, language, and ethnic populations, will ensure that all messages reach all segments of the population.

MID-TERM PRIORITIES

- ***Development, Evaluation, and Application of Methods that Enhance the Use of Information*** – The Federal government will develop enhanced tools and systems for information extraction, pattern discovery, and visualization from structured and unstructured data sources. Desired capabilities are to convert information into standardized formats and increase information-sharing while effectively managing confidentiality and information security issues.

- ***Determination of Intent to Harm or Deceive*** – The Federal government will evaluate and further develop biometric and bio-imaging technologies to identify individuals, and to use in conjunction with behavioral sensors to provide insight into the relationship between motivation and behavior. These will include an assessment of how measures vary as a function of individual characteristics, such as age, gender, ethnicity, and personal history, and across situations, including those of high threat and in cultures outside our own. A related capability is the development and deployment of techniques and technologies to detect deception or hostile intent exhibited by individuals.

- ***Resistance to Terrorist Recruitment and Human and Community Resiliency*** – The Federal government will pursue SBE science to elucidate further basic neural and behavioral mechanisms and how these are modified by context and experience. The development of robust, valid models of the psychobiological and psychosocial mechanisms of distress, resilience, and psychopathology across groups, including children, can advance these objectives, as can the

development of robust, valid, cross-cultural models of social behaviors, social prejudice, and stigmatization. The Federal government also will explore the linkage of information and technology systems to machine language processors for real-time language translation, making available to domestic and foreign publics tools to support positive interaction across borders, cultures, and languages.

LONG-TERM PRIORITIES

- ***Deterring Terrorism*** – The accurate prediction of low-probability, singular events that occur within complex systems, such as behavior of an individual terrorist, may be difficult with the capabilities and technology currently in existence. We are not likely, therefore, to eliminate completely the threat of terrorism, just as uncertainty is not likely to be eliminated even from our routine business and personal decisions. Nevertheless, if there is adequate information we can at least assess the likelihood of a range of feasible outcomes and make decisions that balance expected costs and benefits. In the same way, advances in the understanding of the bases of individual differences, and the relationship of these to the principles of group or crowd behavior, especially within known cultural, ideological, political, and economic domains, will lead to useful probability statements about the likelihood and magnitude of terrorist threats. Corresponding longitudinal trend analyses will identify groups, locations, cultures, institutions, and beliefs that are more or less likely to encourage and sustain the growth of terrorist groups and networks.

AGENCIES' ROLES AND RESPONSIBILITIES

As described in the opening of this chapter, the Federal government is pursuing investment and application of research in the SBE sciences in support of preventing, deterring, combating, and preparing for and recovering from terrorism. Agencies' interests fall into three core and complementary areas: basic research in the SBE sciences; mission-directed applied research; and applied research aligned with agency missions.

Agencies, such as DoD, HHS, and NSF, sponsor basic research in SBE sciences in addition to work in clinical science relevant to recovery capabilities and development of countermeasures. Other government and non-governmental organizations, such as those that form the intelligence and law enforcement communities sponsor mission-directed applied research to support detection, prevention, and preemption strategies and improve the effectiveness of countermeasures.

Additionally, agencies sponsor applied research aligned with key agency missions in preparedness, response, and recovery, including DoD, the Department of Education, HHS, DHS, Treasury, and the Department of Veterans Affairs, as well as EPA and all agencies either concerned with critical infrastructures and their interdependencies or responsible for operational response and interventions in order to maintain mental health when working in adverse environments and in the potential aftermath of a terrorist attack.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Homeland security accomplishments and ongoing activities of agencies across the Federal government are detailed below:

Department of Agriculture (USDA)

- Enhances the protection and safety of the Nation's agriculture and food supply by providing economic analyses of both potential acts of agricultural bioterrorism and naturally occurring animal diseases and conducting research on cost impacts of implementing food safety requirements.

Department of Commerce (DOC)

- Researches and develops standards for emergency response, control systems, safe building materials and designs, and threat detection technology. This includes biometrics as well as fire, chemical, radiological, and nuclear detectors.
- Conducts research on human factors including developing effective technologies for emergency responders, as well as, egress and evacuation strategies. This research also includes the development of software that enables facility owners to evaluate the cost and effectiveness of various options for mitigating threats to building infrastructures.

Department of Defense (DoD)

- Conducts a broad portfolio of SBE-related research in its human systems technology area, with the goal of increasing national security capabilities of U.S. military forces. Specific SBE research strengths can be found in the areas of training systems, leadership selection and development, cognitive modeling and simulations of decision-making for decision support systems, human systems integration into operations technologies, threat predictability, indicators and warnings, crowd assessments, and metrics of performances, among others.
- Researches combat stress and vulnerabilities of personnel in various humanitarian venues. Ongoing research programs on sustained performance in adverse environments are relevant to homeland security preparedness, response, and recovery objectives.
- Researches threats and decision-making models associated with operations security (OPSEC), to provide better understanding of human behavior and performance at the individual, social, and crowd or group levels.
- Researches indicators for addressing adverse behaviors in crowds, groups, and cultures, such as deception and intent.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DoD, continued

- Researches and develops modeling and simulation to understand and detect threats to personnel and defense critical infrastructure. This research is intended to refine decision making, develop a comprehensive, multidisciplinary approach to understanding international, regional, and cross-cultural behavior, and create advanced assessment methodologies (e.g., integrated behavioral analysis capability, integration of diverse models, agent-based modeling, computer-assisted qualitative analysis) in support of these efforts.
- Researches behavioral responses in urban environments to weapons of mass destruction events and conventional attacks.
- Conducts studies in social behavioral analysis of infectious diseases and identification of risk and protective health behavior factors.
- Established numerous centers and programs involving SBE, including the Threat Anticipation Program, a Joint Staff-Cultural Preparation Environment an Integrated Behavioral Analysis Capability Training Program, a Non-Lethal Weapons' Crowd Control Program, a Strategic Deterrence Analysis Lab, and a Joint Integration and Analysis Planning Center that incorporates a behavior component and much more throughout the DoD community.

Department of Health and Human Services (HHS)

- Translates social and behavioral research into public health practice including infectious disease surveillance; identification of risk and protective health behavior factors; public health intervention guidance; research on health communications and individual, organizational and community adherence to public health guidelines during emergencies; assessment of mental health and behavioral responses to uncertain, stressful, and traumatic situations; and other factors important to community resilience.
- Sponsors and conducts research on mental and behavioral consequences of trauma and chronic threat; the needs of children, youth and families after catastrophic events; cognitive, neurobiological and behavioral factors important to resilience; the functioning of distressed victims and survivors and the health and human service workforce; the consequences of perceived and actual exposure to weapons of mass destruction (and by extension, weapons of mass effect); the basic processes involved in forming and shaping attitudes, affect, and behavior; the formation and extinction of fear-induced memory and behavior; and clinical and public health countermeasures.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Department of Homeland Security (DHS)

- Established the National Center for the Study of Terrorism and Responses to Terrorism through a competitively awarded grant to the University of Maryland and its partners to focus on terrorist group formation and recruitment, terrorist group persistence and dynamics, and societal dimensions of terrorism. Similarly, DHS funds The Center for Risk and Economic Analysis of Terrorism Events run by the University of Southern California and its partners and The Center for the Study of High Consequence Event Preparedness and Response run by Johns Hopkins University and its partners. Established the Human Factors Division within the Science and Technology Directorate, which examines terrorist motivation and intent; suspicious behavior detection; community preparedness, response, and recovery; as well as biometrics and personal identification systems; and the integration of human factors into the development and deployment of DHS technologies.
- Models the behavioral, linguistic, and psychological cues that indicate whether an individual is being deceptive and ultimately intends to do harm. The more than 30 cues being examined include various microfacial expressions, language content and usage, heart and respiration rates, among others. All will be assessed using high-resolution remote sensing systems, eliminating the need for the direct contact required by cumbersome polygraphs or functional MRI systems. The capability being designed and developed, which can be used for either primary or secondary screening at various US checkpoints, will improve government personnel's ability to detect human threats and accurately assess risk when granting individuals' entry to the United States or admittance to airplanes and other controlled points of entry. Potential users of this technology include TSA, ICE and CBP.
- Sponsors research that draws on social science data and theories to develop analytic models aimed at determining a group's likelihood of engaging in violence taking into consideration such things as ideological, organizational, and contextual factors.
- Sponsors research to provide temporal and geospatial mapping of the different needs for shelter, food, and other assistance that were identified by callers into the 2-1-1 Information and Referral System in Texas before, during, and after Hurricanes Katrina and Rita. The results of this research will inform future preparedness and response activities for catastrophic events.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

DHS, continued

- Sponsors research evaluating the impact of emergency public information communications during a simulated terrorist attack on the public's understanding of a radiological dispersal device; the public's awareness of the recommended preparatory, response, and recovery actions they may undertake; the public's reactions, fears, and concerns; and the public's understanding, trust in, and compliance with government directives and other communications issued during such an emergency situation. The results of this research will be used to improve future crisis communications.

Department of the Interior (DOI)

- Develops methods related to natural hazards applicable to risks associated with homeland security; develops quantitative risk models integrating physical science and economics information for natural hazards such as earthquakes and landslides, to assess the protection of private and public property and infrastructure; studies how communities anticipate, prepare for, and respond to natural hazards such as wildfire events; develops web-based economic experiments for risk communication, including an experimental analysis of threat communication for national security using the Homeland Security Advisory System; and is currently designing the Institutional Response Index System to analyze the resilience of local communities in the face of natural hazards for the maintenance of social capital and democratic decision processes.

Department of Justice (DOJ)

- Awards grants on topics including, but not limited to: links between organized crime and terrorism; pre-incident indicators of terrorist activities; tactical and operational learning by terrorist groups; terrorist financing; preparedness of private security in shopping malls; coordination of law enforcement and industrial security to protect America's ports; human factors to improve police performance; biometric and DNA research for identification of individuals; and the role of law enforcement in protecting American agriculture from bioterrorism.

Department of the Treasury (Treasury)

- Develops and implements U.S. government strategies to combat terrorist financing domestically and internationally, develops and implements the National Money Laundering Strategy as well as other policies and programs to fight financial crimes, and conducts studies mandated by *The Terrorism Risk Insurance Act of 2002* (Public Law 107-297) to assess, among other things, the cost, supply, and demand for terrorist risk insurance with particular emphasis on high-risk industries and geographic regions.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

Environmental Protection Agency (EPA)

- Conducts workshops on how to communicate with the public during emergencies; Develops message maps identifying key messages and supporting facts for anticipated critical questions; Develops a web-based risk assessment, risk management and risk communication tool that provides critical information to emergency responders, health advisors, and senior emergency management officials.

The National Science Foundation (NSF)

- Sponsors research in human and social dynamics, decision and risk management science, and behavioral and cognitive sciences.
- Conducts Security Evaluation Workshops that are attended by many government agencies and that have led to a collaborative effort with DoD on intercepting explosive devices.
- Initiated a new five-year program in the area of human and social dynamics to advance the understanding of human behavior and performance at the individual, social, and population levels; refine knowledge of decision making, risk, and uncertainty and translation of this knowledge into improved decision-making and risk communication processes; develop a comprehensive, multi-disciplinary approach to understanding human and social dynamics, incorporating international, regional, and cross-cultural approaches; create accessible large-scale data resources; and advance methodological frontiers (e.g., agent-based modeling, complex network analysis, non-linear dynamics, computer-assisted qualitative analysis, multi-level, multi-scalar analysis and measurement research and technologies).

CHAPTER 10 – FUTURE HOMELAND SECURITY SCIENCE AND TECHNOLOGY WORKFORCE

INTRODUCTION

Successful execution of the Federal government's research, development, testing, and evaluation (RDT&E) mission requires a full complement of science and technology professionals dedicated to homeland security issues. Toward this end the Federal government is responsible for, and must provide leadership in, establishing and sustaining an appropriately trained workforce. A multidisciplinary and dedicated workforce is necessary to accomplish the monumental tasks we face. This requires nurturing, recruiting, retaining, and ongoing professional development of the best and brightest personnel who possess the technical breadth necessary to anticipate and preemptively address present and future threats. Through these efforts the Federal government will make great strides in providing the scientific and technical edge needed to secure the Nation.

THREATS AND VULNERABILITIES

The Federal government's science and technology agencies are faced with an aging workforce. Fifty-one percent of the workforce will be 40 or older in 2010, an increase of 33 percent since 1980. For example, in DoD the average age of the laboratory technologist is about 45, and it is estimated that 66 percent of the civilian workforce will be eligible to retire by the end of 2006. Two-thirds of these potential retirees represent experienced information technology, science and technology, and engineering workers. Uniformed personnel face a slightly different issue, in that military rotation requirements make it difficult to keep uniformed scientists in place long enough to complete long term research and development efforts. For these reasons, the interagency community anticipates that the hiring of appropriately trained science and technology professionals may not keep pace with the retirement, attrition, and reassignment of the current workforce.

GAPS

Absolutely critical to our country's national security, economic strength, and intellectual vitality is maintaining a strong foundation in the infrastructure and scientific talent needed for fundamental research across all disciplines, but most specifically in the physical and biological sciences. Scientific expertise is required in many fields, including microbiology, pathology, molecular biology, genetics, chemistry, epidemiology, and statistics. Applications as diverse as medicine, telecommunications, and nonproliferation all increasingly rest on a bedrock of advances in our fundamental knowledge of biology, physics, chemistry, and computer sciences.

Beyond core disciplines, the Nation must address the shortage of students of diverse background and experience pursuing advanced degrees in specialized fields and the lack of appropriately trained faculty to guide them. To illustrate this point, the community of experts in radiological sciences is exceedingly small. Few universities maintain viable training programs in this strategic discipline; for the past couple of decades, few new scientists have entered the field. As a result, the pool of experts can be expected to shrink dramatically as current experts retire.

Biodefense agencies are finding it increasingly difficult to hire employees with the required scientific and medical expertise. The overall demand for biodefense talent will continue to rise for the foreseeable future – by as much as 25 percent through 2010 – while the supply of such talent will likely decline. The government is ill-equipped to prevail in the intensifying competition for such talent. Federal biodefense agencies are losing some of their most talented employees as a result of the limitations of current government pay systems at the same time that an alarmingly large percentage of current staff reach retirement age; nearly half of the Federal employees in occupations critical to our biodefense will be eligible to retire within the next five years.

Another gap is a general lack of multidisciplinary and interdisciplinary studies programs which could, if designed properly, combine subject matter expertise in one's discipline with core competencies in homeland security studies. The existing mechanisms available to the interagency community to manage research and development funding do not easily accommodate – and may even create disincentives to – independent investigator proposals that rely on work in multiple disciplines.

STRATEGIC GOALS FOR 2015

By 2015, the Nation will have a cadre of scientists and engineers dedicated to homeland security. To maximize their productiveness, the Federal government's science agencies and organizations will have achieved a seamless integration of programmatic and budgetary funding mechanisms across homeland security agencies that sponsor academic research and support workforce development.

Agencies managing chemical, biodefense, and radiological programs and laboratories will increase outreach efforts to educational systems and will collaborate with State public education systems to create science centers of excellence for the mutual benefit of the agencies, the laboratories, students, and faculty. The interagency community will collectively increase scholarship funding for students in exchange for their working at a government facility or laboratory for a period of time commensurate with their scholarship and will establish an integrated system of recruitment, training, and retention to address a shortage of expertise in the physical and biological sciences.

To foster interaction among disciplines and create new disciplines, DHS will sustain the network of university-based Homeland Security Centers of Excellence.

To recruit and retain highly trained scientists and engineers in mission-critical positions, DHS will better utilize executive-potential training programs and seek to maximize capabilities resident in minority-serving institutions in support of homeland security missions and operational end-users that are essential to the success of these missions.

The interagency community collectively will seek to develop and evaluate methods of allowing for the free exchange of science across national and international borders and groups in furtherance of the security mission and in ways that ensure the workforce is not only populated by the best scientists, but has the language, communication, and social skills needed to operate in the global security environment.

NEAR-TERM PRIORITIES

- To increase the number of students entering mission-critical, specialized fields, DHS will achieve a steady state of approximately 100 to 150 Undergraduate Scholars and Graduate Fellows and continue growth of the American Association for the Advancement of Science Homeland Security Fellows Program. Agencies managing chemical, biological, and radiological defense programs will increase outreach efforts to educational systems located near their facilities and laboratories and will collaborate with State public education systems to create science centers of excellence for the mutual benefit of the laboratories, students, and faculty.
- To foster interaction among disciplines and create new disciplines, DHS will sustain existing university-based Homeland Security Centers of Excellence and incrementally increase the number of Homeland Security Centers joining its network. DoD, HHS, and DHS will explore collaborative efforts, with a particular eye toward programs at the Uniformed Services University of the Health Services, such as the newly established Department of Radiation Biology.

MID- AND LONG-TERM PRIORITIES

- To increase the number of students entering mission-critical, specialized fields, DHS will support university and professional society efforts to integrate area studies and homeland security studies, and extend homeland security studies to postdoctoral education programs. The interagency community will collectively increase scholarship funding for students in exchange for their working at a government facility or laboratory for a period of time commensurate with their scholarship. The interagency community will establish an integrated system of recruitment, training, and retention to address a shortage of expertise in the biological and physical sciences. Strategies include new training programs, partnerships between universities and Federally Funded Research and Development Centers (FFRDCs), establishment of university training centers, and use of FFRDCs as user facilities to encourage broader academic involvement in radiological sciences.
- To foster interaction among disciplines and create new disciplines, DHS will continue to expand its network of university-based HS Centers of Excellence to reach its goal of 10 Centers, each leveraging its homeland security research activities to support educational and training programs and outreach initiatives.
- To increase faculty members' visibility into homeland security research requirements, DHS will institute a summer faculty study program for homeland security.
- To recruit and retain highly trained scientists and engineers in mission-critical positions, the interagency community will partner with academia and work with legislative bodies to develop and evaluate methods of allowing for the free exchange of science across national and international borders and groups in ways that ensure the workforce is not only populated by the best scientists but has the language, communication, and social skills needed to operate in the global security environment. DHS will better utilize executive-potential training programs and seek to maximize capabilities resident in minority-serving institutions in support of homeland security missions and operational end-users.

AGENCIES' ROLES AND RESPONSIBILITIES

Numerous Federal departments and agencies that conduct homeland security RDT&E have programs that invest in the facilities and education that are necessary to establish and sustain an appropriately trained workforce. Additionally, NSF is the primary Federal agency responsible for science education from kindergarten through graduate studies and plays a vital role in developing the science and technology workforce of the future. The NSF also provides the metrics and data that are essential in tracking the size and capability of the U.S. science and technology workforce.

RECENT ACCOMPLISHMENTS AND ONGOING ACTIVITIES

The interagency community is fully engaged in education and workforce development programs emphasizing the core competencies necessary for a sustaining national homeland security science and technology strategy: science, technology, engineering, and mathematics. Federal agencies pursue coordination and planning on education and workforce development through the National Science and Technology Council's (NSTC) Education and Workforce Development Subcommittee of the Committee on Science.

Agency programs to sustain and expand the Nation's science and technology workforce include the:

- Department of Defense Science and Engineering Apprentice Program and Student Training in Advanced Research Skills;

- Department of Labor's High-Growth Job Training Initiative and Community-Based Job Training Grants;
- National Aeronautics and Space Administration's Science Engineering Mathematics and Aerospace Academy and Administrator's Fellowship Program;
- National Oceanic and Atmospheric Administration's National Sea Grant College Program;
- National Science Foundation's investments through its Education and Human Resources portfolio (especially the Computer Science, Engineering and Mathematics Scholarships Program and the Scholarships for Service Program to develop a Federal Cyber Service) and its Integrative Graduate Education and Research Traineeship (IGERT) program;
- U.S. Department of Agriculture's Food and Agricultural Sciences Education programs directed toward institutional capacity building and human capital development; and
- Department of Health and Human Services' Epidemic Intelligence Service directed toward training epidemiologists.

More specific to building an enduring national capability to meet homeland security mission requirements, the Department of Health and Human Services (HHS) has generated new biodefense scientific positions through the award of 720 extramural projects and more than 60 intramural grants, creation of three new offices related to coordination and oversight of biodefense research and resources, establishment of Regional Centers of Excellence for Biodefense and Emerging Infectious Diseases, and planning for National and Biocontainment Laboratories and Integrated Research Facilities, the latter expected to support 500 new positions in FY 2007-2008. In addition, HHS has also established and sustains a training program through the U.S. Public Health Service (PHS) Office of Force Readiness and Deployment which includes training for PHS commissioned officers in the management of casualties resulting from disaster and terrorist events.

DoD is currently developing an educational program for conducting vulnerability assessments on DoD critical assets. The Full Spectrum Integrated Vulnerability Assessment Program consists of assessment processes, requirements, methodologies and standards, a database system capable of supporting the recording and archiving of asset vulnerability data, and a tracking mechanism designed to capture all applicable reported vulnerabilities and associated remediation efforts. In addition, the DoD has also established and sustains a training program in medical management of chemical and biological casualties, including training for Theater Army Medical Laboratory personnel. Students have included State Department, Federal Bureau of Investigation, Central Intelligence Agency, Secret Service, military services, PHS-commissioned officers, emergency responders, and select foreign countries. For its part, the Department of Homeland Security (DHS), through the Federal Emergency Management Agency, operates the Noble Training Center – the only mock hospital facility in the United States dedicated to medical training in disaster preparedness and response for hospital and healthcare professionals.

DHS has founded the Homeland Security Scholars and Fellows Program to support the development of the next generation of scientists as they study ways to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize damage and speed recovery efforts from a terrorist attack. In addition, DHS is expanding the number of faculty and students directly engaged in homeland security-related research and development through its university-based Homeland Security Centers of Excellence. DHS is also seeking to maximize capabilities in minority serving institutions by continuing the Summer Research Team Program for Minority Serving Institutions by providing student and faculty member teams the opportunity to conduct collaborative research projects with Homeland Security Centers of Excellence. Through a number of consortia unique to each Center, DHS expands its research partnerships within the academic community and to the private sector. DHS will also implement two new programs to support the development of a Homeland Security workforce. The Homeland Security Science, Technology, Engineering, Mathematics Career Development Grants (HS-STEM) Program will enable colleges and universities to award scholarships to qualified students in HS-STEM disciplines, and the Scientific Leadership Awards for Minority Serving Institutions Program will enable colleges to support the

development of HS-STEM teaching initiatives and curriculum development, as well as to award scholarships to students studying HS-STEM disciplines. Both programs will be implemented in FY 2008.

APPENDIX

ACRONYM LIST

ACE	Automated Commercial Environment
ADSR	Apprehension, Detention, Seizure, and Removal
AFRRI	Armed Forces Radiobiology Research Institute
AGA	American Gas Association
ANSI	American National Standards Institute
APEC	Asia-Pacific Economic Cooperation
ASME	American Society of Mechanical Engineers
ATF	Bureau of Alcohol, Tobacco and Firearms
BSL	Biosafety Level
BTS	Border and Transportation Security
CCTV	Closed-Circuit Television
CIA	Central Intelligence Agency
CIP	Critical Infrastructure Protection
CIP&CP	Critical Infrastructure Protection and Compliance Policy
CONOPS	Concept of Operations
CONPLAN	Concept of Operations Plan
COP	Common Operating Picture
COTS	Commercial-Off-The-Shelf
CSI	Container Security Initiative
CT	Computed Tomography
CTCC	Counterproliferation Technology Coordinating Committee
CWA	Chemical Warfare Agent
DCS	Digital Control System
DHS	Department of Homeland Security
DNA	Deoxyribonucleic Acid
DND PCC	Domestic Nuclear Defense Principals Coordinating Committee
DNDO	Domestic Nuclear Detection Office
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DoEd	Department of Education
DOI	Department of Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
EDS	Explosives Detection Systems
eLEXNET	Electronic Laboratory Exchange Network
EMS	Emergency Medical Service
EP&R	Emergency Preparedness and Response
EPA	Environmental Protection Agency
ESSENCE	Early Notification of Community-Based Epidemics
ETD	Explosive Trace Detector
EUA	Emergency Use Authorization
FBI	Federal Bureau of Investigation

ACRONYM LIST

FCC	Federal Communications Commission
FERN	Food Emergency Response Network
FFRDC	Federally Funded Research and Development Center
FMD	Foot-and-Mouth Disease
FY	Fiscal Year
G-8	Group of Eight
GEIS	Global Emerging Infections System
GIG	Global Information Grid
GIS	Geographic Information Systems
GPS	Global Positioning System
GSA	General Services Administration
HDS	Hazardous Devices School
HEU	Highly Enriched Uranium
HHS	Department of Health and Human Services
HSC	Homeland Security Council
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Initiative
HSSP	Homeland Security Standards Panel
IA	Information Analysis
IAB	Interagency Board for Equipment Standardization
IAEA	International Atomic Energy Agency
IC	Intelligence Community
ICC	International Chamber of Commerce
ICSP	Interagency Committee on Standards Policy
IDLH	Immediately Dangerous to Life or Health
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
IMAAC	Interagency Modeling and Atmospheric Assessment Center
IND	Improvised Nuclear Device
IPP	Guardian Installation Protection Program
ISO	International Organization for Standardization
ISO	Independent Systems Operator
IT	Information Technology
ITIC	Intelligence Technology Innovation Center
JPDO	Joint Planning and Development Office
LRN	Laboratory Response Network
MANPADS	Man-Portable Air Defense Systems
MIFC	Maritime Intelligence Fusion Center
MPC&A	Material Protection Control and Accounting
MSC	Mission Support Center
NASA	National Aeronautics and Space Administration
NBACC	National Biodefense Analysis and Countermeasures Center
NBAF	National Bio and Agrodefense Facility
NBFAC	National Bioforensics Analysis Center
NBIS	National Biosurveillance Integration System
NBSCAB	National Bomb Squad Commanders' Advisory Board
NCTC	National Counterterrorism Center
NFPA	National Fire Protection Association
NGA	National Geospatial-Intelligence Agency

ACRONYM LIST

NHS3	National Homeland Security Support System
NIJ	National Institute of Justice
NIOSH	National Institute for Occupational Safety and Health
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NRCC	National Response Coordinating Center
NRO	National Reconnaissance Office
NRP	National Response Plan
NSA	National Security Agency
NSABB	National Science Advisory Board for Biosecurity
NSC	National Security Council
NSF	National Science Foundation
NSPD	National Security Presidential Directive
NSTC	National Science and Technology Council
NTA	Non-Traditional Agent
NTC	National Targeting Center
NTIA	National Telecommunications and Information Administration
NVS	National Veterinary Stockpile
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PAG	Protective Action Guide
PAPR	Powered Air Purifying Respirator
PDD	Presidential Decision Directive
PEL	Permissible Exposure Limits
PEP	Prepositioned Equipment Program
PHIN	Public Health Information Network
PHS	United States Public Health Service
PIADC	Plum Island Animal Disease Center
PL	Public Law
POE	Ports-of-Entry
PPE	Personal Protective Equipment
RCIED ECM	Remote-Controlled Improvised Explosives Device Electronic Countermeasure
RDD	Radiological Dispersal Device
RDT&E	Research, Development, Testing, and Evaluation
RKB	Responder Knowledge Base
rPA	Recombinant Protective Antigen
S&T	Science and Technology
SAR	Supplied Air Respirator
SBE	Social, Behavioral, and Economic
SCADA	Supervisory Control and Data Acquisition
SCBA	Self-Contained Breathing Apparatus
SLD	Second Line of Defense
SNM	Special Nuclear Material
SNS	Strategic National Stockpile
TIC	Toxic Industrial Chemical
Treasury	Department of Treasury
TSWG	Technical Support Working Group
UAV	Unmanned Aerial Vehicle

ACRONYM LIST

UICDS	Unified Incident Command and Decision Support
US	United States
US&R	Urban Search and Rescue
USCG	United States Coast Guard
USDA	United States Department of Agriculture
VA	Department of Veterans Affairs
VACIS	Vehicle and Cargo Inspection Systems
WMD	Weapons of Mass Destruction
WMD MCM	Weapons of Mass Destruction Medical Countermeasures Subcommittee
WMD-CST	Weapons of Mass Destruction Civil Support Team