REVIEW 2010

Combating Terrorism Technical Support Office

Preface

"To be prepared for war is one of the most effectual means of preserving peace."

George Washington

The Combating Terrorism Technical Support Office (CTTSO) knows, firsthand, through its constant communication and involvement with the end users and first responders who bring forth requirements for their technology and capability gaps that preparation is, indeed, key.

In today's combating terrorism (CbT) environment, being prepared means not only having all the right tools in one's arsenal, but also ensuring that those tools are on the cutting edge and well ahead of what the enemy has or can be used against terrorists' constantly evolving tactics, techniques, and procedures. Much like in a game of chess, each "player" in the CbT community must constantly be strategizing and anticipating the opponents' next move.

Being equipped with the proper tools is critical. Whether it's a new and improved Explosive Ordnance Disposal robot with an advanced

U.S. Navy photo by Chief Mass Communication Specialist David Rush/Released

Preface

communications system; an enhanced performance chemical, biological, and radiological boot that provides superior stability, comfort, and protection; a simple, low-cost, reliable wet chemistry or colorimetric-based kit for the detection of homemade explosives; or an advanced surveillance system that provides enhanced area surveillance and an augmented reaction capability for a small, forward deployed operational element in an unconventional warfare/counterinsurgency environment. They all serve to better equip and prepare military forces abroad as well as first responders, law enforcement, and security forces in the United States.

Just as important as having the right tools is having the right tools at the right time. As a rapid prototyping research and development organization, CTTSO understands the imperative nature of ensuring that the end users have the technologies and capabilities they need when they need them. In addition, those end users are involved in each step of the process, from submitting their requirements to remaining involved in the development process and helping to develop the next generation of equipment by telling CTTSO exactly what they want and need to make their jobs easier or safer.

At a time when defense spending is increasingly under scrutiny, CTTSO's interagency scope, coupled with its multiple international partnerships, helps eliminate redundancies while leveraging the support and technologies of other agencies and/or countries to develop the best possible products for all users who require them. The collaborative nature of the CTTSO provides a distinct advantage to the combating terrorism community. Products first prototyped with CTTSO are now in use with military units in combat, Special Operations Forces, Explosive Ordnance Disposal technicians, law enforcement, and by first responders.

DoD photo by Staff Sgt. Angelita M. Lawrence, U.S. Air Force

This annual review book will highlight a few of the new technologies and resources that may improve the effectiveness of military and civilian security forces, law enforcement officials, bomb squads, training instructors, and a host of other individuals who have a single-minded purpose and defined mission to defeat terrorists. It will also highlight those agencies that, by providing their people and their support, help to ensure that CTTSO continues to remain on the cutting edge, providing both material and nonmaterial solutions to those who need it most. The projects included in this book are only some of CTTSO's success stories—successes garnered in the constant effort to be prepared in the CbT domain, and ultimately to preserve peace.

Table of Contents

DoD photo by Lance Cpl. Michael E. Warren, U.S. Marine Corps

Combating Terrorism Technical Support Office

Combating Terrorism Technical Support Office

Overview

Identify requirements to combat terrorism and provide solutions to warfighters, first responders, and other frontline users as rapidly as possible.

The Combating Terrorism Technical Support Office (CTTSO) is charged with providing a forum for interagency and international users to discuss mission requirements to combat terrorism, prioritize those requirements, fund and manage solutions, and deliver capabilities. CTTSO accomplishes these objectives through rapid prototyping of novel solutions developed and field-tested before the traditional acquisition systems are fully engaged. This low-risk approach encourages interdepartmental and interagency collaboration, thereby reducing duplication, eliminating capability gaps, and stretching development dollars. This unique "left of POM" process for rapidly delivering capabilities allows the Department of Defense and interagency acquisition systems and Programs of Record to identify successful capabilities and incorporate them into budget cycles without the risk of long-term development efforts.

Organization

The Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict and Interdependent Capabilities (ASD (SO/LIC&IC)) established CTTSO in 1999 to consolidate its research and development programs previously administered by the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). The research and development effort that supports the interagency Technical Support Working Group (TSWG) was the first program to transition to CTTSO. The Explosive Ordnance Disposal/Low-Intensity Conflict (EOD/LIC) Program, which develops advanced technologies for Joint Service EOD and Special Operations Forces (SOF) missions, transitioned in 2001. In 2007, the Irregular Warfare Support (IWS) Program was initiated to satisfy a growing need to improve the capacity of the United States to counter insurgencies and fight an irregular war. Finally, the Human Social Culture Behavior (HSCB) Modeling Program stood up in 2008 to enhance the understanding of the complex operational problems related to social and cultural terrain.

Combating Terrorism Technical Support Office

CTTSO's International Program

Most terrorist acts are not solely planned and executed in one country. To defeat an international threat, CTTSO has since 1993 pursued international cooperation, where appropriate, to accomplish its mission.

CTTSO cooperates with governmental organizations in Australia, Canada, Israel, Singapore, and the United Kingdom, all of which have the ability, like CTTSO, to reach to the whole of government including military, security services, and first responder organizations. These agreements allow projects that go beyond data exchanges to cooperative development, ensuring a broadly-scoped program with worldwide impact. The results of this cooperation are not only high-quality products and increased communication with key global partners, but also the creation of a global antiterrorist environment.

DoD photo by Master Sgt. Jeremiah Erickson, U.S. Air Force

DoD photo by Gertrud Zach, U.S. Army/Released

Technical Support Working Group

Technical Support Working Group

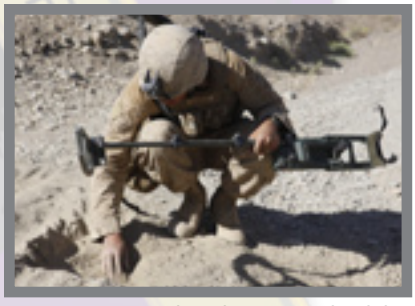
History and Mission

In April 1982, the National Security Decision Directive 30 assigned responsibility for the development of an overall U.S. policy on terrorism to the Interdepartmental Group on Terrorism (IG/T), chaired by the Department of State (DOS). TSWG was an original subgroup of the IG/T, which later became the Interagency Working Group on Counterterrorism (IWG/CT). In its February 1986 report, a cabinet level Task Force on Counterterrorism—led by then Vice President Bush—cited TSWG as assuring "the development of appropriate counterterrorism technological efforts."

Today, TSWG still performs that counterterrorism technology development function as a stand-alone interagency working group. TSWG's mission is to identify and prioritize the needs of the national interagency community through research and development programs for combating terrorism requirements. TSWG delivers capabilities to those on the front lines through rapid research and development, test and evaluation, while providing operational support. TSWG incorporates available expertise and experience from government, commercial, private, and academic sources throughout the United States and the world.

TSWG initiates efforts to influence longer-term research and development initiatives; and, reflecting the shift to a more offensive strategy, balance its technology and capability development efforts among the four pillars of combating terrorism: antiterrorism, counterterrorism, intelligence support, and consequence management.

DoD photo by Sgt. Russell Gilchrest, U.S. Army/Released



U.S. Marine Corps photo by Lance Cpl. Ralph J. Fabbri/Released

DoD photo by Mass Communication Specialist Seaman Martin Carey, U.S. Navy

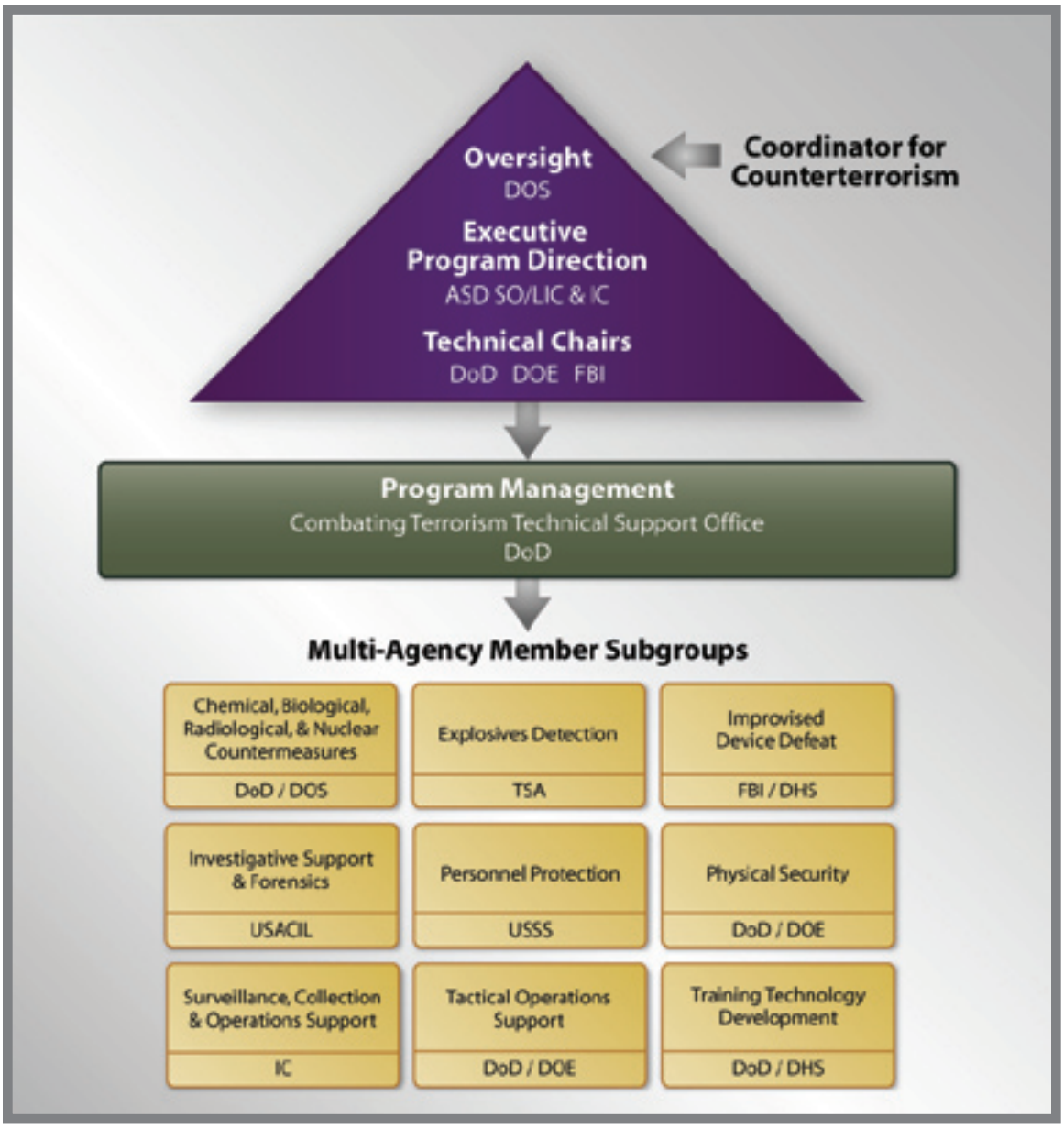
Organization and Structure

TSWG operates under the policy oversight of the Department of State's Coordinator for Counterterrorism and the management and technical oversight of the Department of Defense Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. While TSWG's core funds are derived principally from CTTSO and DOS, other departments and agencies contribute additional funds and provide personnel to act as project managers and technical advisors. TSWG has successfully transitioned capabilities to the Departments of Agriculture, Defense, Homeland Security, Justice, State, and Treasury; the Intelligence Community; the Public Health Service; and many other departments and agencies. Additionally, TSWG has transitioned many systems to state and local law enforcement. TSWG membership includes representatives from more than 100 government organizations. Participation is open not only to federal departments and agencies, but also to first responders and appropriate representatives from state and local governments and international agencies. These departments and agencies work together by participating in one or more subgroups. A comprehensive listing of

Technical Support Working Group

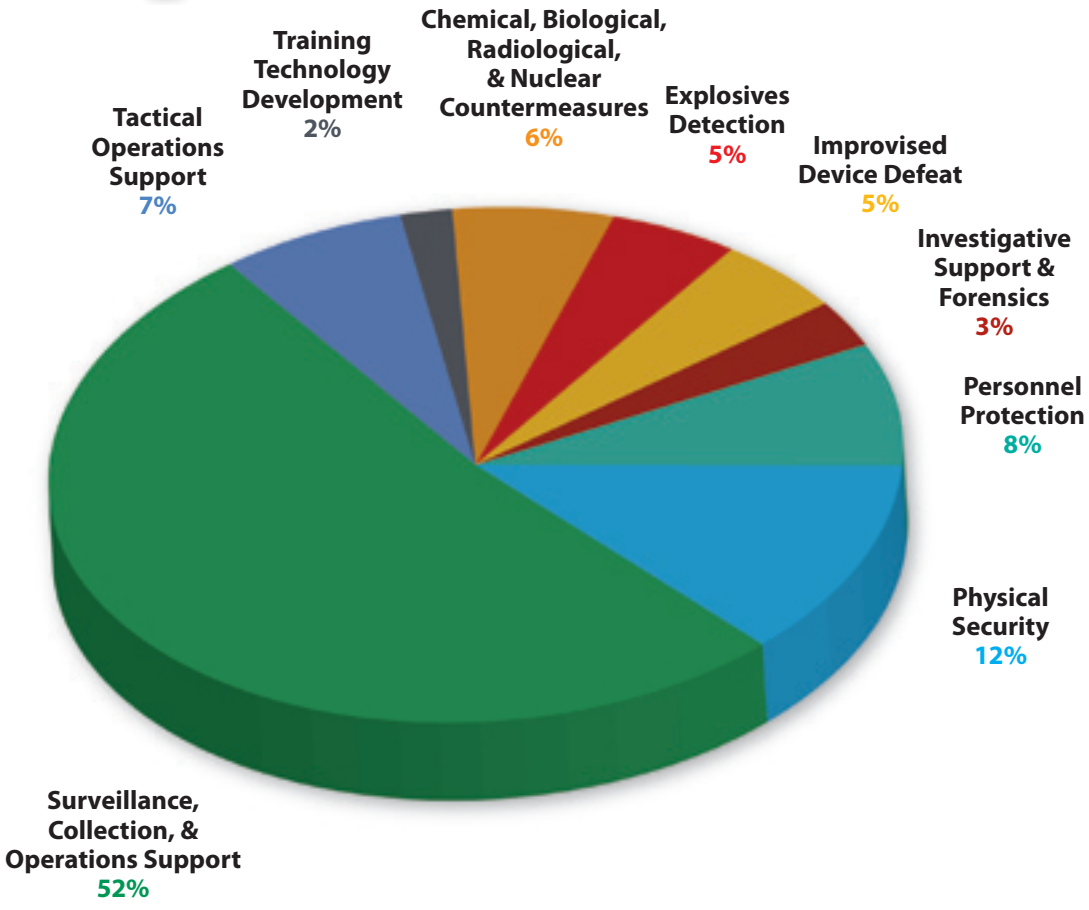
member organizations by subgroup is provided in the appendix.

TSWG's subgroups are chaired by senior representatives from federal agencies with special expertise in those functional areas. Chairmanship of nine subgroups is shared as indicated in the organizational chart below.



Technical Support Working Group

TSWG FY 2010 Program Funding ($193 Million)



DoD photo by Sgt. J.C. McKenzie, U.S. Army

Technical Support Working Group Subgroups

Chemical, Biological, Radiological, and Nuclear Countermeasures

Chemical, Biological, Radiological, and Nuclear Countermeasures

Mission

Identify, prioritize, and execute interagency chemical, biological, radiological, and nuclear combating terrorism requirements, and deliver technology solutions for detection, protection, decontamination, mitigation, containment, and disposal.

The Chemical, Biological, Radiological, and Nuclear Countermeasures (CBRNC) Subgroup identifies and prioritizes multi-agency user requirements and competitively seeks technological solutions for countering the terrorist employment of CBRN materials. Through its participation in the InterAgency Board for Equipment Standardization and Interoperability and in coordination with the Department of Homeland Security, the National Institute of Justice, the Environmental Protection Agency, and other Department of Defense components, the CBRNC Subgroup integrates technology requirements from the fire, hazardous materials, law enforcement, and emergency medical services communities into its process. Senior representatives from the Department of Defense and the Department of State co-chair the subgroup.

Focus Areas

The CBRNC Subgroup focus areas reflect the prioritized requirements of the CBRN incident prevention and response community. During FY 2010, these focus areas were:

Detection

Improve the sampling, detection, and forensic analysis of chemical, biological, and radiological threat agents in the air, in food or water, and on surfaces.

Protection

Improve the operating performance and reduce the costs of individual and collective protection. Develop and enhance personal protective equipment (PPE), including respiratory protection systems and suits. Develop analysis and design tools for CBRN protection for building engineers and architects. Develop and evaluate advanced filter materials.

Consequence Management

Develop technologies and procedures to mitigate the effects of a life-threatening or destructive event. Develop and improve response activities and related equipment to counter a terrorist or accidental release of CBRN materials, to include short- and long-term restoration.

Information Resources

Develop shared information management tools to provide a common operating picture. Facilitate the efficient integration of diverse emergency and consequence management elements from federal, state, and local agencies.

Chemical, Biological, Radiological, and Nuclear Countermeasures

Selected Completed Projects

Advanced Small-Room Chemical and Biological Filtration System

Special and high-profile locations require the capability to provide shelter-in-place in a small room in the event of a chemical or biological incident where evacuation is not the desired course of action. HBM Associates, LLC designed an advanced small-room chemical and biological filtration system that will be installed in the designated safe room of critical facilities and is intended for emergency use. The Advanced Small-Room Chemical and Biological Filtration System (AFS) is capable of operating in tandem with existing heating, ventilation, and air conditioning systems or as a stand-alone system to provide protection against external or internal building airborne chemical or biological agents. The AFS takes outside and/or building recirculated air, filters it through a particulate and chemical adsorber filter, and pressurizes the space to at least five pascals above ambient pressure. AFS is designed as an innocuous, tamper resistant, portable unit capable of being rapidly installed into existing structures and systems. AFS is a true plug and play system ready to operate with the activation of one switch to provide up to six hours of continuous protection against chemical and biological agents. AFS supports a wide range of military, Department of Homeland Security, and civilian operations to protect personnel and key facilities from chemical and biological agents and thus improving operational capabilities. Requests for additional information should be sent to cbrncsubgroup@tswg.gov.

Enhanced Performance Tactical Chemical, Biological, and Radiological Boot

First responders require footwear with superior stability and comfort for use in environments contaminated with chemical, biological, and radiological (CBR) contaminants. Current boots for hazardous materials are heavy, have poor ergonomic design, and increase body temperature. The North Carolina State University Textile Protection and Comfort Center partnered with Globe Firefighter Suits, Falcon Performance Footwear, and W.L. Gore & Associates to develop an enhanced performance CBR boot. The project team of users, material designers, and clothing design experts addressed deficiencies in current tactical footwear. The enhanced boot provides protection against chemical warfare agents, toxic industrial chemicals and materials, and flash fire. The boot meets the component requirements of National Fire Protection Association (NFPA) 1994: Standard on Protective Ensembles for First Responders to CBRN Terrorism Incidents, and NFPA 1971: Standard on Protective Ensembles for Structural Fire Fighting and Proximity Fire Fighting. Requests for additional information should be sent to cbrncsubgroup@tswg.gov.

Radiological Dispersion Device Recognition Guide

A terrorist act using a radiological dispersion device (RDD) in a populated area is considered far more likely than the use of a large-scale

Chemical, Biological, Radiological, and Nuclear Countermeasures

nuclear explosive device. RDDs appeal to terrorists because they require limited technical knowledge, and materials are easily obtainable. RDDs can cause long-term economic and psychological damage. For these reasons, it is critical for response personnel to know how to recognize suspect packages as an RDD. Battelle Memorial Institute developed a clear, concise, and easy-to-use Radiological Dispersion Device (RDD) Recognition Guide for training and operational use by hazardous materials, explosive ordnance disposal/bomb squad, and other public safety personnel. The guidebook focused on two high-priority sources: Cesium-137 & Iridium-192. The guide is a pocket-sized flipbook with an electronic version available for field laptop use. Requests for additional information should be sent to cbrncsubgroup@tswg.gov.

Vehicle Retrofit for Mass Casualty Evacuation

The intent of this capability is to quickly transform various transportation conveyances, including school buses and transit buses, into evacuation vehicles for injured or special needs citizens following a large-scale terrorist attack or natural disaster. The system provides for stretchers or litters, basic life support equipment, and space for minimal essential personal possessions for each passenger. The system is economical and safe and can be quickly installed and removed. Raytheon, the developer, prepared designs for the retrofit kits for transit and school bus configurations. The design complies, to the maximum extent possible, with relevant federal motor vehicle safety standards. Field evaluations of the final prototype design were conducted with the New York City Transit Authority, the Fire Department of New York, and the New York City Office of Emergency Management. Requests for additional information should be sent to cbrncsubgroup@tswg.gov.

Biological Aerosol Test Method and Personal Protective Equipment Decontamination Method

During the first 45 days of an influenza pandemic, it is expected that there will not likely be enough N95 National Institute for Occupational Safety and Health-certified disposable filtering face piece respirators for health care workers. The Air Force Research Laboratory first developed and validated a biological aerosol test method to serve as a standard test platform capable of delivering a reproducible, threat-based virus load to respirators. The American Society for Testing and Materials International test protocol was then used to develop decontamination protocols that kill threat-representative viruses but do not affect the performance of the respirators. The data collected allowed the National Academy of Science to issue effective guidance on the decontamination and reuse of face masks during an influenza pandemic. Requests for additional information should be sent to cbrncsubgroup@tswg.gov.

Chemical, Biological, Radiological, and Nuclear Countermeasures

Selected Current Projects

Modular CBRN Hose System

The traditional approach to CBRN respiratory protection forces operators to select a specific type of equipment for a known threat scenario. A Self-Contained Breathing Apparatus (SCBA) delivers clean air in an unknown/hazardous environment, but wear duration is typically limited to 30 minutes. The use of a CBRN Powered Air Purifying Respirator (PAPR) extends wear duration significantly (several hours) with less user burden; however, they cannot be used in unknown or high risk environments. Therefore, the specialist community accepts a number of performance tradeoffs. This leads to a less than optimum tactical approach to missions and increased user risk. Avon Protection Systems, Inc. will integrate its existing SCBA Compact Demand Valve technology with new PAPR methodology to deliver a universal hose connection system. This provides a standard interface connection for both SCBA and PAPR systems to be used in combination for increased protection and mission time. In addition, the development delivers a unique low profile connection with air purifying respirators with an optional connection for a heads-up display for greater situational awareness. The modular hose will provide interoperability between existing equipment. It is a universal hose able to combine different systems and provides the ability to change protection modes, depending on the environment.

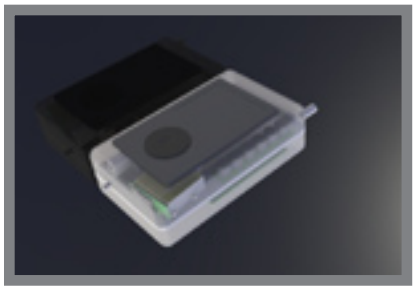
Best Practices Guide for Mail Screening and Handling

Government mail center managers face a wide range of mail-borne threats on a daily basis. As such, they need a comprehensive and concise "Best Practices" manual. The manual will help agencies choose and implement the right technology and screening processes necessary to protect their facilities and their mail center personnel. Pitney Bowes Government Solutions and its teaming partner, Clovis Point Solutions, LLC, will lead the effort to research and develop the Best Practices Guide based on an analysis of the existing literature on mail screening and handling, interviews with key government and industry experts, and onsite audits/examinations of existing mail screening facilities. The information acquired throughout this research process will then be examined by a series of subject matter expert panels and other stakeholders to ensure the best, most cost effective technology and screening practices are implemented in each government mail center. The Best Practices Guide will include chapters that examine risks in government mail streams; technologies, facilities, and processes to combat risks; training requirements for mail center personnel; and emergency response procedures. The guide will also include copies of key regulatory requirements, a risk matrix to help identify the appropriate handling and screening approach for a given location, and a series of short case studies to help mail center managers better understand the approaches being illustrated throughout the guide.

Chemical, Biological, Radiological, and Nuclear Countermeasures

Standoff Patient Triage Tool

The first few minutes after many disastrous events can be critical in determining the effectiveness of treatment protocols key to the survival of victims. Emergency response personnel are required to conduct triage at the incident scene to prioritize rescue and on-scene emergency medical treatment. These actions may need to take place in austere and contaminated environments or in an earthquake or other disaster where people are partially buried in rubble. A handheld device aimed at a victim from a distance of at least five feet that can rapidly and accurately measure selected physiological markers indicative of their current status and potential for survival if provided prompt treatment on the scene would help to solve these limitations. The Boeing Company is developing a handheld emergency response triage device to assist in the on-scene assessment of victim status in a mass casualty incident. The device is usable by personnel wearing Class I/Level A or B chemical protective clothing or fire fighting personal protective equipment. It will reliably provide data on key physiological parameters of the victims from a distance of five feet (threshold) and an objective distance of 40 feet. The ruggedized Standoff Patient Triage Tool instrument is able to provide information on victim condition in less than 30 seconds.



Portable Orthogonal Detection Device for Toxic Industrial Chemicals

Detection and identification of chemical threats is a continuing problem for military, security, and emergency responder personnel. No single detection technology has proven capable of reliably detecting all threats. Some detection schemes are very sensitive but have little or no selectivity and are prone to false alarms. Other schemes are very selective but require high concentrations of the analyte to give a reliable analysis. In an effort to streamline operations and reduce overall cost, teams require a single detector to meet the varied detection needs. The single detector must have the capability to provide a secondary confirmation for chemical identification based upon an orthogonal detection technique. This capability will greatly reduce the false positives found in field operations. Thermo Fisher Scientific (formerly Ahura Scientific) is developing a portable, handheld device incorporating both vapor-phase vibrational spectroscopy and highly sensitive gas sensors. On-board chemometrics will process the output of the sensor array in conjunction with the vibrational spectrum, providing detection, identification, and quantification of hundreds or thousands of chemical vapors. The utility of the portable orthogonal detector will be greatly enhanced with the addition of wireless communication and GPS location.

Gas Adsorber for Capturing Common Gaseous Toxic Industrial Chemicals

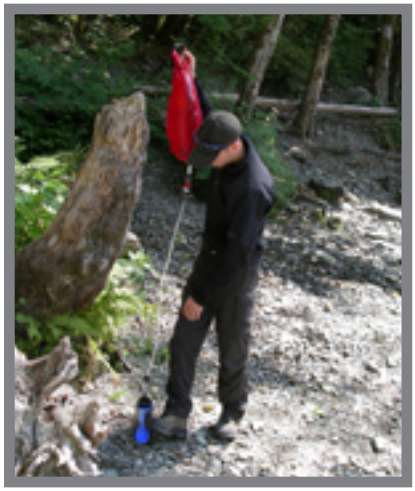
Most buildings currently use activated carbon air filters that do not perform efficiently against low-molecular-weight toxic industrial chemicals (TICs) that could be deployed in an act of terrorism. United

Chemical, Biological, Radiological, and Nuclear Countermeasures

Technologies Research Center, in collaboration with Georgia Institute of Technology, is developing a chemical adsorber (filter medium) that has enhanced capabilities for capturing TICs. A novel filtration media based on metal-organic frameworks in combination with current activated carbon technology will address low molecular weight threats that could be deployed against a building. The new filter medium will also address humidity degradation problems in current filters, as well as reduce the amount of activated carbon necessary to provide improved life safety and indoor air quality for the areas served. Long-term performance characteristics and scale-up synthesis testing are currently being performed.

Selected Project Updates

Personal Hydration System Water Filter

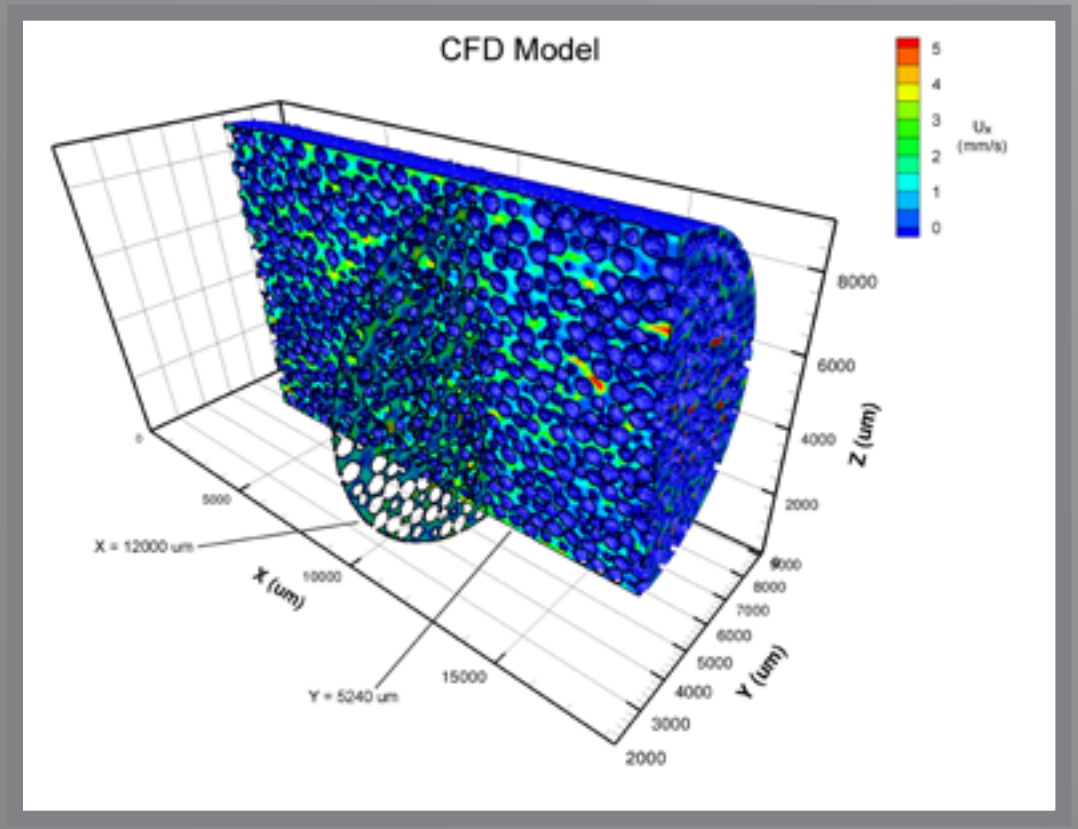


It is of crucial importance that our troops have clean water sources to ensure adequate health and hydration. Water supplies can be indirectly or directly contaminated with bacteria, viruses, and protozoa, which are common causes of diarrheal disease, as well as with toxic industrial chemicals and petroleum derivatives. Direct or indirect contamination may also occur by terrorist use of chemical and biological materials. Providing response personnel with potable water is an ongoing challenge. Depending on the climate, an individual needs to drink between one and three and one half gallons per day to avoid dehydration. This need is compounded if an individual must wear personal protective equipment for extended periods of time. MesoSystems and Cascade Designs developed a filtration system for personal water purification that removes bacteria, protozoa, viruses, petroleum, and select toxic industrial chemicals, as well as chemical and biological warfare agents. The filter is used when water contamination is possible and bottled water is not available. The water filter renders nonpotable water safe for human consumption in accordance with Environmental Protection Agency and Department of Defense drinking water standards. The filter is small, lightweight, and low cost while still providing enough capacity for multiple days of continuous use. To date, 2,400 units have been delivered to military operational units to enhance field capabilities. Requests for additional information should be sent to cbrncsubgroup@tswg.gov.

Contact Information

cbrncsubgroup@tswg.gov

A comprehensive listing of member organizations by subgroup is provided in the appendix.



Explosives Detection

Explosives Detection

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements for explosives detection and diagnostics with emphasis on new and enhanced detection and identification of improvised explosive devices.

Focus Areas

The Explosives Detection (ED) Subgroup focus areas reflect the prioritized requirements of a broad range of interagency customers, including those responsible for incident response, physical security, and forensic analysis. During FY 2010, these focus areas were:

Chemical & Physical Characterization

Produce and analyze chemical and physical scientific information to expand the fundamental understanding of threats. Investigate and identify unique physical and chemical characteristics to enable detection of homemade, military, and commercial explosive capabilities and limitations of sensor technologies. The information provided will allow better focus on the selection of new technology and the optimization of existing technology for explosive detector development. This will deliver new or improved explosive detection capabilities to current and future programs within the explosive detection community.

Enabling Technology Development

Develop enabling technology to detect energetic materials and explosive precursors. Advance technologies that address capability gaps for the detection and diagnosis of person- and/or vehicle-borne improvised explosive devices (PBIED/VBIED). Areas of concern are detection rate, variability of content, safety, and impact on stream of commerce.

Bulk & Trace Explosive Detection Performance Development

Develop new capabilities and improve existing systems for quick improvements in the detection and identification of explosive threats. Improve the detection rate and accuracy of commercial and near-commercial detection systems.

Test & Evaluation

Conduct rigorous independent assessments to confirm the detection capability and performance of commercial and prototype systems. Evaluate the performance of new systems to assure that the needs of the warfighter are met.

Explosives Detection

Selected Completed Projects

Dual-Energy X-Ray to Detect Vehicle-Borne Improvised Explosive Devices

Distinguishing between illegal substances, explosives, and other contraband in vehicles is challenging. Spectrum San Diego developed a dual-energy X-ray system for the detection of bulk explosives that may be concealed in cars and trucks. The system uses a technique that can discriminate between organic and metallic objects that may be concealed or are otherwise difficult to discern. The dual-energy system also allows the operator to acquire quantitative information on organic masses located in the vehicle. The system has a five-mile-per-hour drive-through capability and is also safe for screening individuals. Two prototype systems have been built and undergone evaluation to include safety testing for the Transportation Security Administration by Johns Hopkins University. The CarScan system has been evaluated at a ferry crossing and is scheduled for an operational assessment at a Washington, D.C. area Department of Defense facility. Requests for additional information should be sent to edsubgroup@tswg.gov.

Selected Current Projects

Characterization of Chemical and Physical Signatures of Improvised Explosive Devices

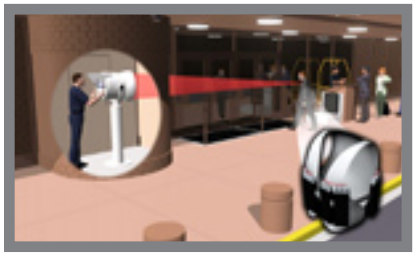
Battelle Memorial Institute and Pacific Northwest National Laboratory are developing databases of chemical and physical signatures of improvised explosive devices. The signatures database will be in a form that will permit secure dissemination to federal agencies and developers of detection systems. This development will enhance standoff explosives detection capabilities. The data may include identification and spectra of chemical compounds related to the presence of explosives or physical signatures of components, such as electronics or materials used to package or conceal the device. Upon completion of the project, database packages will be available for evaluation. The research is supported by the Joint Improvised Explosive Device Defeat Organization.

HME Precursor Wet Chemistry Identification

Clandestine or improvised labs may produce a variety of different end products from drugs to explosives. Identification of precursor materials can distinguish unlabeled and potentially toxic or dangerous compounds for disposal or evidence collection. Current wet chemistry kits are labor intensive and complex in their use. CET, LLC is developing a simple compact wet chemistry kit to identify classes of compounds that may be found in improvised laboratories. The steps for sampling to detection are being minimized to improve the ease of use for general purpose forces as well as allies. The kit will provide improved detection times and accuracy versus currently deployed colorimetric systems. Colorimetric chemistries

Explosives Detection

and lightweight durable packaging are currently being optimized for laboratory testing and evaluation. This project is a joint venture between the CBRNC and ED subgroups. Requests for additional information should be sent to cbrncsubgroup@tswg.gov.



Standoff Sub-Millimeter-Wave Imager for Suicide Bomber Detection

An urgent need for standoff concealed-weapon detection, particularly suicide bomber detection, exists. In response, Pacific Northwest National Laboratory is developing a prototype real-time 350-gigahertz imaging system to address this threat. This system will be able to scan for concealed anomalies on people. Additionally, due to the wideband operation, this system provides accurate ranging information, and the images obtained are fully three-dimensional. A prototype system will be available for operational assessments upon completion.

Comparative Test and Evaluation of Raman-Type Systems

Comparative testing and evaluation of the threat detection capability and usability of commercial and near-commercial detections systems are under way. These methods include spectroscopy and detection of thermal or acoustic effects caused on laser interrogation of surfaces or of the air space above an explosive. Evaluations focus on laser-based standoff detection methods of explosives concealed by suicide attackers. The research is supported by the Department of Homeland Security Transportation Security Laboratory.

Contact Information

edsubgroup@tswg.gov

A comprehensive listing of member organizations by subgroup is provided in the appendix.

Improvised Device Defeat

Improvised Device Defeat

Mission

Identify, prioritize, and execute research and development projects that satisfy mission critical needs, fill capability gaps, and address interagency requirements for advanced technologies to safely and effectively defeat improvised terrorist devices. Emphasis is placed on technologies to enhance the training and support of operational personnel in the location, identification, render safe, and disposal of homemade explosives, improvised explosive devices, and other emerging terrorist threats.

The Improvised Device Defeat (IDD) Subgroup delivers advanced technologies, tools, and information to increase the operational capabilities of the U.S. military explosive ordnance disposal (EOD) community and federal, state, and local bomb squads to defeat and neutralize terrorist devices. In collaboration with military, federal, state, and local agencies, the IDD Subgroup identifies and prioritizes multi-agency user requirements through joint working groups and thorough validation processes. Representatives from the Federal Bureau of Investigation's Bomb Data Center and the Department of Homeland Security's Office of Bombing Prevention co-chair the subgroup.

Focus Areas

The IDD Subgroup focus areas reflect the joint priorities of military and civilian responders. During FY 2010, these focus areas were:

Device Defeat

Develop advanced technologies to defeat the broad spectrum of improvised terrorist devices to include improvised explosive devices (IEDs), vehicle-borne IEDs, person-borne IEDs, and enhanced hazard devices containing chemical, biological, or radiological materials. Develop innovative, cost-effective disruption and precision render safe solutions that increase standoff distance, reduce collateral damage, and decrease risk to the improvised device defeat operator. Improve neutralization techniques for both sensitive and insensitive explosives and enhanced payloads such as flammable liquids and gases.

Identification and Diagnostics

Advance the capability of improvised device defeat operators to interrogate unknown or suspect items and packages. Develop technologies to locate and identify improvised devices and enhanced fillers, and diagnose key fuzing and firing components. Develop tools to assist improvised device defeat operators in the identification of U.S. and non-U.S. ordnance and firing systems incorporated into or modified for use in improvised devices.

Improvised Device Defeat

Emerging Threats
Advance production of effective countermeasures to neutralize or defeat radio-controlled IEDs, and provide safe environments for improvised device defeat operators. Develop, characterize, and test technology solutions to effectively render safe improvised devices using novel fuzing systems that incorporate such items as electronic, sensor, microcontroller, or mechatronic[1] components.

Remote Procedures
Develop advanced application systems to remotely access, diagnose, and defeat improvised devices. Advance development of manufacturer- and model-independent products and robotics with plug and play interface. Develop open architecture, navigation, communication, and operator controls for robotic platforms, tools, and sensors.

Tool Characterization and Information Resources
Improve performance evaluation methodologies, test procedures, and tool characterization models for improvised device defeat technologies. Conduct ongoing evaluation and improvement of tools, methods, and protocols for confirming the accuracy of detection equipment, reliability of diagnostic tools, and completeness of neutralization and render safe techniques. Advance training concepts and information delivery systems that promote the tactical and operational response readiness required to effectively, safely, and efficiently counter improvised devices and emerging terrorist threats.

Maritime Security
Develop technologies to protect ships, boats, docking facilities, offshore platforms, shoreside loading facilities, power plants, bridges, and marine cables and pipelines from any form of terrorist attack, including water-borne and underwater IEDs. Develop and test technologies to include manned or unmanned long- and short-range sensors for detection and tracking; physical barriers and stopping devices; unmanned surface, underwater, and air vehicles; weapons; armor; life support; diving and underwater systems; and mammal systems.

Selected Completed Projects

Critical Incident Response Technology Seminars
In 2010 the Critical Incident Response Technology Seminars (CIRTS) completed the 25th seminar in 22 different cities throughout the United States. Federal, state, and local bomb squad participants from across the country attended the seminars. The seminar themes focused on various

1-Mechatronics adds intelligence to a mechanical design or replaces a mechanical design with an intelligent electronic solution. An example of a mechatronic component is the digital thermostat, which has replaced the much more inefficient mechanical thermostat. Digital thermostats are more accurate and are typically programmable, allowing for increased efficiency.

Improvised Device Defeat

real world scenarios involving improvised explosive devices (IEDs), vehicle-borne IEDs, suicide-borne IEDs, homemade explosives, and the latest threat of water-borne IEDs. The bomb squad participants were presented a scenario in which they had to use their current equipment, experience, knowledge, and training to render safe the IED in a controlled environment. The feedback collected assisted in developing new tactics, techniques, and procedures and addressing new tool development efforts to assist the public safety bomb technicians against IEDs. These seminars will continue in FY 2011 with the support of the National Bomb Squad Commanders Advisory Board. Requests for additional information should be sent to iddsubgroup@tswg.gov.

Tool Characterization Guide

The Tool Characterization Guide will help assist the public safety bomb technician in selecting his disruptor option when faced with a render safe procedure. Ever since the September 11th attacks, bomb squads throughout the country have received more equipment than they can carry on their bomb squad vehicle. This new electronic guide will allow them to access their disruptor tools in real time and select the best tool for the scenario. The guide will provide the bomb technician with background information, references, proper tool emplacement, and the probability of success against certain scenarios. Requests for additional information should be sent to iddsubgroup@tswg.gov.

Land Shark

As the terrorist threats and the use of chemical, biological, radiological, and nuclear measures and explosives evolve, the need for remote systems also needs to evolve. Robotic systems need to have the capability to incorporate a design that is modular and allows for easy integration of additional sensors and advanced technologies through plug and play connections that utilize an open communications architecture. They must also be field configurable by the multi-mission oriented end users. To meet this ongoing need, Black I Robotics, Inc. has delivered the Land Shark EOD Robot to the Massachusetts State Police Bomb Squad for evaluation with the Massachusetts Port Authority at Boston's Logan International Airport through a congressionally funded program. The vehicle provides long-range, high bandwidth connections capable of delivering streaming video and Internet connectivity while moving where other radios cannot operate. The Land Shark communicates using the Assured Wireless Ethernet (AWE) developed by Nomadio under a prior TSWG and EOD/LIC-funded program. The AWE family of routers enables frequency-agile, high-speed, reliable mesh networking. The Land Shark utilizes an open architecture that allows for easy sensor integration that has included illuminators, speakers, optical devices, and the Early Attack Reaction System developed by Qinetiq North America and fielded in theatre by the Rapid Equipping Force. The Land Shark EOD Robot has a vertical reach of 9 feet and can lift 100 pounds at full extension. It is

Improvised Device Defeat

capable of speeds up to 10 miles per hour and can operate in excess of 10 hours utilizing a hybrid generating power system. Requests for additional information should be sent to iddsubgroup@tswg.gov.

Selected Current Projects

Camera Blinder

The use of surveillance technologies has become more prevalent in our day-to-day society as more agencies and companies look to improve their defensive posture. Terrorists and criminal elements have also begun to employ home surveillance systems as a means to detect law enforcement stakeouts and raids. AMP Research has developed the Personal Anonymity Device series of directed energy handheld or tripod mounted devices that can temporarily or permanently disable surveillance cameras from a distance. This device is currently being evaluated by the Collier County Special Operations Integrated Bomb Squad and SWAT team. Requests for additional information should be sent to iddsubgroup@tswg.gov.

Stirling Engine

The current universal problem in robotic platforms is that they operate on a limited rechargeable battery supply to meet any mission requirements. This project will demonstrate the capability of a Stirling engine to provide primary power for robotic application. Current robotic systems typically use batteries, which significantly shorten mission duration due to current battery technology limits. The Stirling engine provides a constant, steady power supply using a variety of available fuels to greatly lengthen the mission capability of a robotic platform. Stirling engines also provide a high degree of reliability and are quiet. This ensures reduced maintenance and repair costs as well as relatively silent operation of the robotic system.

Remote Mobility Platform 400

Military operators and public safety first responders need a cost effective remote capability to increase standoff detection/exploitation capabilities that deliver advanced sensors to check for the presence of hazards. Segway, Inc., in cooperation with the Air Force Research Laboratory, has advanced the Segway Remote Mobility Platform (RMP) 400 with emphasis on the requirements of first responders within their mission areas and provided a robotic platform that utilized multiple mission type sensors. The RMP 400 consists of multi-mission payload decks that are plug and play under the Joint Architecture for Unmanned Systems protocol and will provide varying levels of sensor technology according to the needs of the end user. One RMP 400 will be deployed with U.S. air forces in Afghanistan, and one RMP 400 will be evaluated by U.S. Customs and Border Enforcement and the Pentagon Force Protection Agency EOD technicians. Requests for additional information should be sent to iddsubgroup@tswg.gov.

Improvised Device Defeat

Advanced Manipulators for Remote Control Vehicles

Bomb Technicians need the capability to utilize multiple tools to access and render suspect terrorist devices safe. RE2, Inc. is developing the low-cost, Joint Architecture for Unmanned Systems-based manipulator end effector/grippers for robotic platforms to provide enhanced dexterity and automatic tool changing. The system will allow the operator to change multiple tools while still at the crisis site. Representative tools consist of a prismatic drill, fiberscope, shearers, an abrasive wheel cutting system, and specialized grippers. The advanced manipulator is being developed using the low-risk near-term Recon Manipulator and by leveraging existing technology at Technology Readiness Level 6 or above and integrating this technology into the Andros F6A Robotic Platform in partnership with Northrop Grumman/Remotec.

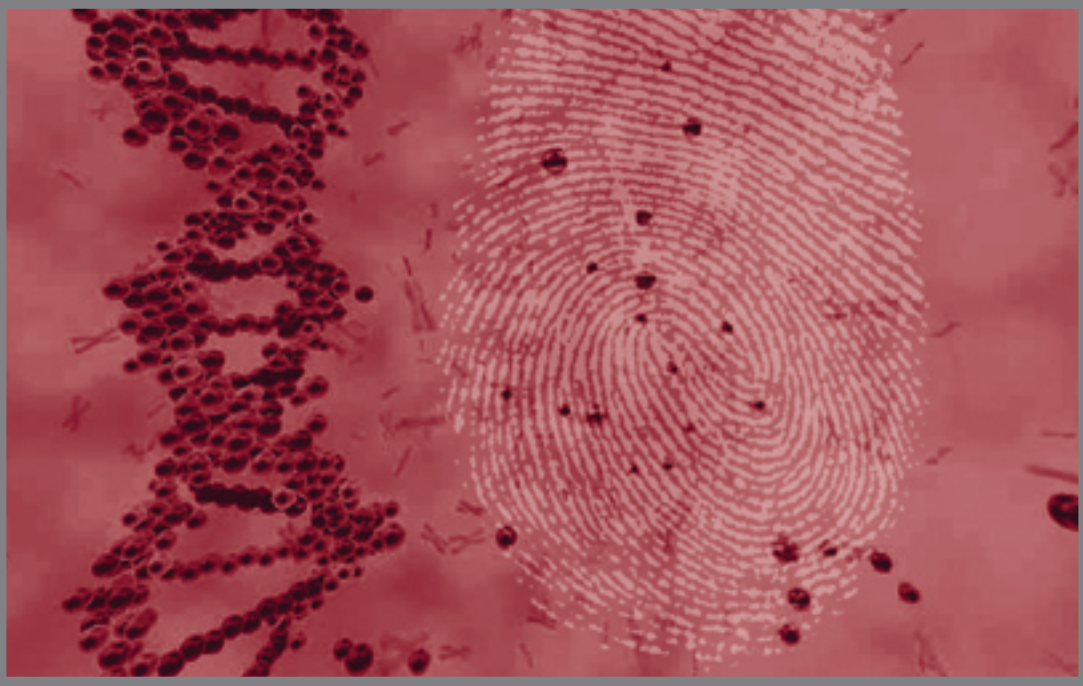
Carbon 10 Disruptor Evaluations

In mountainous theatres of operations, Explosive Ordnance Disposal (EOD) operators are being utilized in foot-borne operations vice vehicle-borne operations. Since foot-borne operations require the EOD operator to physically carry his/her equipment, any reduction in size or weight without a reduction in capability of the equipment is highly desired. The Carbon 10 disrupter potentially offers a significant size and weight decrease when compared to a Percussion Actuated Non-Electric disrupter, the primary EOD IED render safe tool. The Navy Explosive Ordnance Disposal Technology Division will evaluate the manufacturer specifications of the lightweight Carbon 10 Disrupter marketed by the Concept Development Corporation. This test and evaluation program will determine the product's reliability, safety, and suitability for Category 1 Approval for Explosive Ordnance Disposal Use.

Contact Information

iddsubgroup@tswg.gov

A comprehensive listing of member organizations by subgroup is provided in the appendix.



Investigative Support and Forensics

Investigative Support and Forensics

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements for criminal investigation, law enforcement, and forensic technology applications in terrorism-related cases.

The Investigative Support and Forensics (ISF) Subgroup implements research and development projects that provide new capabilities to law enforcement personnel, forensic scientists, and intelligence operatives responsible for investigating and interdicting terrorist incidents. Projects conducted through this group have had a major impact on forensic investigations and intelligence operations throughout the law enforcement community. A representative from the U.S. Army Criminal Investigation Laboratory chairs the subgroup.

Focus Areas

The ISF Subgroup focus areas reflect the prioritized requirements of the military and civilian law enforcement communities. During FY 2010, these focus areas were:

Crime Scene Response

Improve the quality of recognition, documentation, collection, and preservation of evidence as well as the safety of first responders at a scene. Train first responders and forensic examiners and improve their capabilities to process and record terrorist incident scenes for future prosecution. Develop advanced technologies for the analysis of handwriting, verification of documents and forgeries, and document origin. Support scientific and technical efforts not assigned to other ISF focus areas.

Electronic Evidence

Develop computer forensic hardware, software, decryption tools, and digital methods to investigate terrorism. Identify computer systems and media used by terrorists, and extract the maximum amount of evidence from them. Develop advanced methods to extract and enhance audio recordings and video images from surveillance sources. Improve techniques for the analysis of electronic devices to obtain the most forensic information.

Forensic Biology and Chemistry

Develop analytical methods for biological evidence found at terrorist scenes to make identifications and extract the maximum information such as origin or age. Enhance the DNA and other person-specific identifiers to track, identify, or profile persons or other biological material. Use stable isotope ratios to determine the geographic origin of organic material. Improve chemical techniques for analyzing evidence and identifying materials used in explosive devices.

Investigative Support and Forensics

Fingerprint, Impression, and Trace Evidence

Improve and automate latent print and related biometric techniques used in terrorism cases. Create better visualization and development of fingerprint evidence, and support better understanding of the molecular content of print evidence as well as the scientific validation of fingerprint examinations. Develop and enhance methods for the recovery, comparison, analysis, and interpretation of small, often microscopic, fragments of materials that transfer between people, places, and objects during terrorist incidents. Improve methods to identify, collect, and analyze fibers, paint, glass, hair, soil, gunshot residue, and other trace evidence items. Enhance forensic capabilities to examine any impression evidence such as firearms comparisons, tool marks, and physical matches.

Next-Generation Canines

Design, develop, and evaluate systems and methods that enable working canines and handlers to operate more effectively and efficiently. Enhance the ability of canines to perform functions such as explosives detection, tracking, patrolling, and attacking in an operational environment. Explore training tools, protocols, and technologies that support or enhance canine detection, including the development of new training aids that will enable more thorough exposure of canines to different types of scents. Design, develop, and evaluate methods that improve the capability to locate friendly personnel, reestablish contact with enemy combatants, and conduct reconnaissance of an area.

Surveillance and Information Gathering

Produce new advanced surveillance and tracking techniques for law enforcement. Develop better communication capabilities for tactical operations. Improve voice identification and speaker recognition capabilities. Develop better credibility assessments, interviewing techniques, and related technologies. Improve information gathering and analysis techniques through technology, social interaction methods, and training.

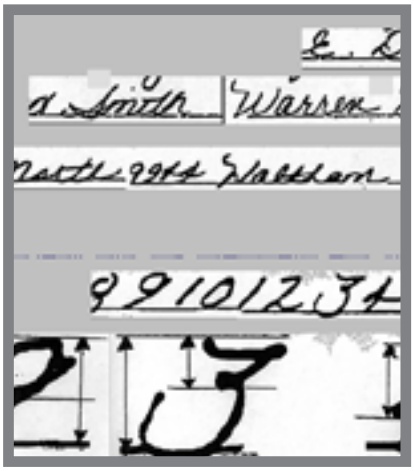
Selected Completed Projects

FireWire Memory Extractor

Accessing and retrieving information from computers and electronic equipment can reveal valuable evidence and intelligence. Frequently, these devices have FireWire ports, which despite conforming to industry standards, contain security vulnerabilities that investigators can exploit to access and extract data even when the equipment is locked or is password protected. Ashlar International, LLC developed a hardware-software system that connects to a FireWire port, bypasses the security measures, and then extracts the data in the device's memory. The system can collect stored memory and random-access memory (RAM) as well as download the running processes and passwords. Modules within

Investigative Support and Forensics

the software can convert the raw data into an easily readable format that investigators can immediately analyze and use. The small, easily portable system operates from a small stand-alone laptop with large storage space or can be placed on other devices to run the extraction and conversion processes. Requests for additional information should be sent to isfsubgroup@tswg.gov.



Forensic Document Analysis

Forensic examinations of documents and handwriting may play a crucial part in the success of a counterterrorism investigation. However, when presented as evidence in court, these analyses frequently undergo legal attacks for not having a sufficiently established scientific basis. Drexel University's Data Fusion Laboratory (DFL) has conducted thorough testing to further support the scientific foundation of several types of document exams. To counter legal attacks, DFL has tested the reliability of certified forensic document examiners (FDEs) to analyze disguised handwriting and then compared their performance to persons who demographically represent those who serve on trial juries. DFL also tested and determined the effects of the context of other evidence on the accuracy of the conclusions of the FDEs. The last phase of testing measured the accuracy of FDEs when examining faxed documents to identify or exclude the machine that printed the document. The DFL efforts have shown that FDE analyses do have a sufficient legal scientific basis and will help thwart future challenges in court. Requests for additional information should be sent to isfsubgroup@tswg.gov.

Selected Current Projects

Integrated Canine System

Since the beginning of the recent U.S. combat operations in the Middle East, the use of military working dogs on the battlefield has escalated to an all-time high. Simultaneously, U.S. forces can gain a significant tactical advantage when they view real-time images of potentially hostile situations in their area of operations. In response, Tactical Electronics is developing the Integrated Canine System. The Integrated Canine System will enhance the soldier's situational awareness on the battlefield by providing real-time video with integrated global positioning data. This new system, which fits in a vest fitted to a dog, will equip military working canines with video cameras and GPS devices that transmit encrypted signals to their tactical teams. From a safe distance the teams can analyze video images of potentially hostile threats and environments before having to engage them. The combat teams receive immediate and accurate tactical information, and they can retransmit the signal in real time to other units or record it for after-action reviews, more comprehensive intelligence analysis, and other reporting.

Investigative Support and Forensics

Remote Viewer for Bullet Comparison

Analysis by forensic firearms examiners critically affects criminal and terrorist cases both domestically and on the battlefield. The need for firearms examinations is increasing, yet the number of those qualified is limited and concentrated at forensic laboratories located far from the scene or combat zone. Quantum Signal, LLC is developing a solution that remotely extends the range of the forensic firearms examiners. Rather than being on site, the examiner can use a "teleoperated" comparison microscope to study the markings and striations on bullets and spent shell casings to make identifications. The system will allow remotely located examiners to manipulate and examine evidence placed in a motorized mount under a comparison microscope by an on-site technician. All of the typically adjustable features of the microscope, such as zoom, focus, and lighting, will be controlled via a user-friendly "teleoperated" interface. This will enable a single firearms examiner to analyze evidence efficiently at a host of different locations directly from their existing laboratory and will take the crime lab to the battlefield or crime scene.

Advanced Log Collector

Despite persistent and conscientious computer security efforts, terrorists still find ways to gain unauthorized access to computers and steal sensitive information. Collecting data from computers to determine who, how, when, and what was accessed becomes critical and normally requires highly trained investigators or forensic scientists. In this project, ID Scientific is creating a system to make the extraction and analysis of the data in these cases quicker, easier, and more complete than ever before. The new advanced system will have the capability to rapidly download stored data including RAM, determine the programs and running processes that were being used, identify passwords, and collect other data pertinent to the incident. Most significantly, the new system will eliminate the need to have physical access to the targeted computer because it will be able to remotely perform its capabilities and evidence collection via the Internet or a local area network. The system will be able to target any Windows, Mac, or Linux-based computer and will be minimally invasive. Modules within the software will analyze the raw data and transform it into thorough and easy-to-read reports.

Trace Evidence from Blast Scenes – Best Practices

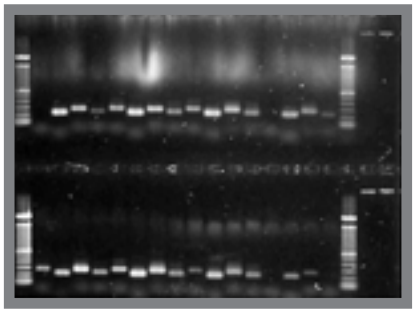
During investigations of terrorist-caused explosions, proper collection and processing of the trace evidence at the blast scene is critical to forensically developing the most information from the site. In addition to possibly leading to the identification of the responsible terrorists, the trace evidence can also characterize the type of explosive device and the materials used. Each scene presents its own challenges, and investigators have many factors to consider. Having access to the latest available information, research, and a well organized best practices guide

Investigative Support and Forensics

is invaluable to those responsible for processing the blast scene. Analytic Services, Inc. (ANSER) is researching and preparing a comprehensive reference for the identification, collection, and preservation of trace evidence at blast scenes as well as the forensic examinations that had been conducted. This reference will then be used to produce a condensed ruggedized trace best practices guide that fits in the cargo pockets of military uniforms and is easily carried to blast scenes. The reference and the pocket guide will emphasize the best practices to use in the non-ideal situations seen in a combat theatre, such as having few persons to process the scene, lack of equipment, security concerns, and short processing times.

Shoeprint Examination

Shoeprints obtained from a crime scene can provide key evidence about the incident. However, to elicit the most value from shoeprint evidence, forensic examiners need better and quicker analytical tools for individual shoeprints. Shoeprints have neither the automated systems nor the established protocols and databases that fingerprint and DNA evidence presently have. This project will develop some tools to assist forensic scientists during their examinations of shoeprints. First, a database of shoeprints will be created similar to those now existing for fingerprints. This database will then be used to set up a validated statistical model for the examinations of shoeprints. Additionally, computer algorithms will be developed to enable shoeprint examiners to quantitatively estimate the evidential value and error rate of defects and individual traits that are used to make a shoeprint identification or exclusion. The new system will support the expert supporting system used in conjunction with the thorough examination and evaluation by the shoeprint examiner.



Phenotypic Information from Crime Scenes Samples

DNA analysis of biological evidence found at crime scenes is now more sensitive and powerful than ever. Despite the advanced DNA techniques and processes, a sample from the person who left the DNA evidence is needed for comparison to make a positive identification. When a DNA profile from the source is not in a database, a positive identification from the DNA is not possible until the subject is identified through other investigative or forensic techniques. This project is developing techniques to offset some of this problem. Bond University of Australia is producing some DNA protocols to use the genetic information within the DNA to determine some of the physical traits of the source. These may include hair color, eye color, ethnicity, and height estimation. With some information concerning the subject's physical traits, investigators can narrow the search for the subject and make the complete identification quicker and easier. The protocols developed will also be useful for the identification of unknown skeletal remains.

Investigative Support and Forensics

Contact Information

isfsubgroup@tswg.gov

A comprehensive listing of member organizations by subgroup is provided in the appendix.

White House photo by Pete Souza

Personnel Protection

Personnel Protection

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements to provide advanced tools, techniques, and guidelines that enhance personnel security.

The Personnel Protection Subgroup develops new equipment, reference tools, and standards to enhance the protection of high-risk personnel (HRP). Projects focus on putting innovative tools such as automated information management systems, communication devices, mobile surveillance systems, and personnel and vehicle protection equipment in the hands of those tasked with the safety of HRP. The subgroup delivers new technologies to military, federal, state, and local law enforcement protection details. Representatives from the United States Secret Service and the Department of Energy co-chair the subgroup.

Focus Areas

The Personnel Protection Subgroup focus areas reflect the prioritized requirements of the personnel protection community. During FY 2010 these focus areas were:

Communications Surveillance and Reconnaissance

Develop technologies that provide military and law enforcement personnel with the capability to covertly communicate and collect surveillance data to identify and mitigate terrorist threats against personnel. Provide personnel with tools to tag, track, and locate mission critical personnel. Develop technologies that enhance situational awareness of mission operations.

Individual Protection and Survivability

Enhance the protection of personnel during blast and ballistic events. Develop technologies that improve the performance of body armor by reducing weight and optimizing material performance. Develop test devices and procedures that provide more biofidelic responses during blast and ballistic testing events in order to mitigate the probability of injury to personnel. Quantify the effects of conventional and enhanced blast damage mechanisms to the human body.

Information Resources

Develop reference materials, information management systems, and analytical tools to enhance preparation, facilitate decision making, and improve incident response capabilities. Enhance software tools to more efficiently exploit intelligence and surveillance data. Generate tools that will enhance the detection of networks, relationship resolution, and tracking of terrorists through large amounts of data.

Personnel Protection

Mobile Security

Enhance personnel protection during vehicular, marine, and air transportation. Develop techniques to enhance protection against blast and ballistic threats during transit. Conduct performance evaluations and studies to assess the protection capabilities of transport mechanisms, and generate solutions to optimize protection.

Selected Completed Projects

Personnel Tracking Device

Agents and high-risk personnel (HRP) routinely find themselves in different parts of the world to conduct business. In order to track personnel while on location, different means of communication are required to overcome the somewhat unreliable coverage. Integrating cellular and satellite communication technologies into one handheld device allows agents and HRP to be readily tracked wherever their mission may take them. Blackbird Technologies, Inc. developed the Personnel Tracking Device, a tri-mode device communicating via the cellular and satellite infrastructures. This device searches for the highest strength signal available and transmits location, specific latitude and longitude details, and battery life data to a designated command center with each communication. Data is transmitted on a periodic basis or immediately upon triggering the panic mechanism. All information is encrypted and transmitted to a government controlled command center. Several federal agencies representing the most likely end users participated in a successful operational assessment of the first run of prototype devices including deployments outside the continental United States. This evaluation identified size reduction as a key area of optimization, and the Personnel Protection Subgroup is currently executing a follow-on contract to enhance this device through weight savings, size reductions, ease of manufacturing, and the inclusion of a vehicle docking station. Requests for additional information should be sent to ppsubgroup@tswg.gov.

Improved Concealable Body Armor

Protective services, including military personnel, often operate in civilian clothing to blend in with the local population. In these situations it is important that they remain as inconspicuous as possible. Traditional concealed body armor can draw attention to an operator when the user sits, bends, or twists. These movements can cause bulges under shirts and crease clothing, indicating that body armor is being worn. A more concealable body armor system is required to minimize these effects. Armorworks, Inc. developed the Improved Concealable Body Armor (ICBA). ICBA is a system that adequately protects wearers with National Institute of Justice (NIJ) Level IIIA protection, yet is not easily noticeable. The system minimizes any bulges and outer clothing crease lines when the user is making routine body movements such as sitting, twisting, or bending. Comfort is an important facet as well, and the ICBA was

Personnel Protection

designed to not cause wearers a distracting amount of discomfort due to bunching, heat stress, or other factors. The ICBA is currently being evaluated by NIJ for certification. Requests for additional information should be sent to ppsubgroup@tswg.gov.

Networked Advanced Vehicle Anti-Tamper and Alert System

U.S. federal agencies with motor pool facilities may be subject to the malicious tampering of the vehicles in those motor pools. Tampering concerns include attempted theft, sabotage of the vehicle or its weapons/electrical systems, the attachment of tracking devices, and the attachment of explosives. Applied Research Associates, Inc. developed the Networked Advanced Vehicle Anti-Tamper and Alert (NAVATA) system, a wireless vehicle security system designed to monitor the activity in a motor pool. Individual vehicles within the motor pool are outfitted with tremble sensors attached to an embedded system that includes a transmitting radio. The vehicle sensors relay any detected vehicle tampering to the embedded system, which in turn sends the data to a monitoring station at a remote command center for action response and event recording. Each vehicle is a node in a wireless mesh network and can act as a repeater for the data until it reaches its final destination. The NAVATA system also allows a remote vehicle kill function. Users at the command center are able to remotely disable vehicles in response to a tampering event. The NAVATA system was operationally evaluated in the field to identify potential improvements or enhancements for future modifications to the device. Requests for additional information should be sent to ppsubgroup@tswg.gov.

Ruggedized Intrusion Detection System

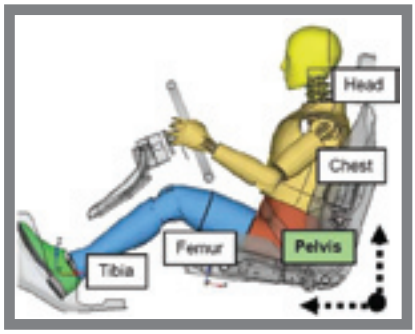
Units and field teams that are deployed to transient locations are potential targets of espionage and terrorism while working and living in temporary places. Electronic tagging, improvised explosive device planting, and intrusions are just a few potential threats to facilities and vehicles. Applied Research Associates, Inc. (ARA) developed the VIP Ruggedized Security Kit (VIPR), an effective, portable, rugged, and rapidly-deployable intrusion detection system equipped for outdoor use. The VIPR system includes tamper detection, remote monitoring, and post-event review capabilities for temporary residences and vehicles. This effort leveraged ARA's previous experience developing the VIP Security Kit (VIPSKIT), a non-ruggedized high-tech sensor and security system for temporary residences and vehicles. VIPSKIT demonstrated the feasibility of providing an effective, portable, and rapidly-deployable detect-and-alert system for temporary residences and vehicles. VIPR then took this capability to the next level, providing a rugged system for use in both indoor and outdoor environments. Another notable improvement is that VIPR allows up to 16 camera feeds with simultaneous playback capability for post-mission analysis. VIPR is deployed in theatre with U.S.

Personnel Protection

military forces for an operational field evaluation. Requests for additional information should be sent to ppsubgroup@tswg.gov.

Selected Current Projects

Light Armored Vehicle Crew Protection



During a blast attack on an armored vehicle, the occupants can sustain injuries from local vehicle deformations and/or global vehicle translation. It is important to be able to accurately predict the injuries in a repeatable and consistent manner. Anthropomorphic Test Devices (ATDs) are used to make these predictions but must be validated against the loading conditions and corresponding human injury caused by the blast event. This study is focusing on armored vehicle side-blast and under-body attacks. For these predefined blast loading conditions, the bio-fidelity of different parts of the ATD is being validated in terms of predicting injury levels. A United Kingdom team led by the Metropolitan Police Service is conducting side and under vehicle blast testing using ATDs to measure the shock loading, while a U.S. team led by Wayne State University is performing ATD testing and post-mortem human subject testing to validate the ATDs. The test results and optimized ATDs that will result from this study will make significant contributions to increase survivability during vehicle blast scenarios through more accurate predictions of injury during the development of protective measures.

Canine Body Armor

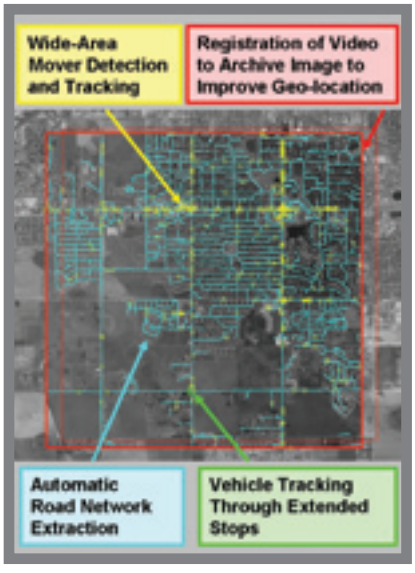
Service dogs have become integral team members of military and law enforcement organizations. These service dogs undergo extensive training for explosives detection and/or attack techniques before being deployed in the field. Many of these service dogs in military operations and law enforcement are encountering hostile fire during their missions. Some service dogs have been severely injured or killed in action due to hostile fire. Had the service dogs been wearing appropriate armor, their chances of survival would have been improved. Armorworks, Inc. is developing the Canine Body Armor (CBA), a solution for military and law enforcement working dogs consistent with NIJ Level III performance. The CBA will be fitted in a carrier that allows for functional equipment attachments so that the dogs are able to perform their duties. In addition to providing chest cavity protection, the preliminary design includes a sternum plate that will not hinder movement. The armor sizing will accommodate a range of different sizes of animals to include small (30-50 pounds), medium (50-70 pounds), and large (70-100 pounds). Overall system weight will not exceed 10 percent of the canine's weight. The CBA is being designed around a price point of no more than $1,500 per unit as a completed product that can be manufactured.

Personnel Protection

Personal Security Decision Aid

Protective Service Details (PSDs) must prepare a Personal Security Vulnerability Assessment for high risk personnel they are assigned to protect prior to their mission. This assessment assists the PSDs in determining the need, size, and scope of a protective detail for approval. Analytic Services, Inc. is developing a Personal Security Decision Aid (PSDA), an automated tool that provides users with the ability to enter threat, vulnerability, risk, and other operational data for HRPs in a standardized format. The PSDA assists in risk-based decision making on appropriate protection measures and will promote consistency across the Department of Defense agencies with PSDs. The application will enable the user to enter information regarding the HRP and the area they will be visiting as well as obtain and evaluate political violence and crime rate and other information pertinent to the area. Based on the entries, the tool will assist the user in critical risk-based decision making for appropriate protection measures to implement, including the need, scope, and size of protective details.

Wide Area Video Exploitation Library



The wide area airborne sensors that are used to harvest large amounts of surveillance data have been leading to major analyst productivity bottlenecks. The volume and complexity of this data presents a significant challenge for human analysts to manage large datasets, integrate data from multiple sources, identify activity of interest, isolate it from background activity, and derive useful intelligence in a timely manner. Advanced algorithms and tools are required to automate or semi-automate the labor-intensive aspects of the information extraction process. The Wide Area Video Exploitation Library (WAVELib), in development by BAE Systems is a set of advanced video exploitation algorithms that overcome limitations with low spatial resolution, low frame rate, and insufficient GPS accuracy faced by current detection and tracking approaches. WAVELib is easily integrated into any Wide Area Persistent Surveillance exploitation application, and developers can easily add new functions to the WAVELib following the design paradigm. The WAVELib routines are capable of ingesting Constant Hawk imagery and metadata and producing accurately geo-stabilized contrast-enhanced imagery, vehicle detections, and tracks. Developed in C++, WAVELib is capable of running on Windows and Linux operating systems and was designed in an open manner to allow for rapid integration with existing exploitation tools.

Contact Information

ppsubgroup@tswg.gov

A comprehensive listing of member organizations by subgroup is provided in the appendix.

Physical Security

Physical Security

Mission

Identify, prioritize, execute, and transition research and development projects and testing and evaluation programs that satisfy interagency requirements for technology to protect personnel, vital equipment, and facilities against terrorist attacks.

The Physical Security (PS) Subgroup identifies, prioritizes, and executes physical security interagency requirements to protect personnel and equipment, execute research and development projects that address those requirements, and transition successful prototypes into programs of record or into immediate field use to meet urgent operational needs. A Department of Defense representative from the U.S. Army Office of the Provost Marshal General, a Department of Energy representative, and a Department of Justice representative from the Bureau of Alcohol, Tobacco, Firearms and Explosives chair the subgroup.

Focus Areas

The PS Subgroup focus areas reflect the prioritized requirements of the physical protection community. During FY 2010, these focus areas were:

Blast Effects and Mitigation

Test and evaluate infrastructure components and systems to investigate and characterize potential damage in order to identify mitigation strategies to protect against current and evolving threats. Components include but are not limited to: fortifications, buildings, bridges, tunnels, and structural members. Develop test protocols to ensure repeatable and consistent results where components and threats require evaluation under unique circumstances. Testing emphasis is on explosives (including homemade explosives) and debris and shrapnel effects. Events may also include gunfire, mortars, and rockets. Mitigation strategies may include hardened infrastructure, improved design standards, retrofit techniques, and new design criteria.

Emerging Explosive Threats

Develop projects to satisfy interagency and international requirements that address the adaptive threat associated with emerging explosives. Emphasize characterization of explosives and novel delivery techniques to combat their use in terrorist activities.

Vulnerability Identification

Develop predictive analysis software and decision aids to identify vulnerabilities and/or determine preventive courses of action. Emphasize pre- and post-event planning and assessment of emerging threats.

Physical Security

Screening, Surveillance, and Detection
Develop technologies and techniques to survey and analyze facilities; improve situational awareness; detect, identify, and locate advancing threats; control access to critical assets; and neutralize confirmed threats. Emphasize automatic alerting, expeditionary kits, and exportable variants.

Integrated Solutions
Integrate technologies into force protection solution packages that will improve the effectiveness of security systems, reduce manning requirements, and offer increased affordability and survivability of operators and responders.

Subterranean Operations
Develop capabilities to detect, locate, surveil, and disrupt subterranean operations in semipermissive and nonpermissive environments to allow tactical forces to conduct operations and counter hostile and/or criminal networks.

Waterside Security
Develop technology for use in the protection of ships, boats, docking facilities, offshore platforms, and shoreside facilities from any form of terrorist attack. Technologies will address the following categories: detect, classify, identify, warn, deter, and engage.

Working Groups
The Physical Security Subgroup has regularly scheduled working group meetings that bring together scientists, researchers, intelligence officers, operators, and academia from the interagency and international communities to collaborate on efforts, identify capability gaps, and build a collective path forward. The following five areas have active working groups: Blast Community Forum, Counter-Tunnel Operations, Homemade Explosives, Vehicle Barriers, and Waterside Security.

Selected Completed Projects

Blast Simulator
Terrorist bombings of critical infrastructure worldwide have demonstrated the nation's vulnerability and created a mandate for research on the deployment of new blast resistant construction as well as hardening techniques. This project developed a simulation tool that can better predict blast load effects and the effectiveness of hardened technologies and be used to augment current information on structural design and response. The University of California at San Diego (UCSD) developed the Explosive Loading Laboratory Test Program to identify and validate blast mitigation and hardening optimization technologies, including computational blast physics codes. Tests on full-scale components and systems are performed using a hydraulic/high pressure nitrogen-based

Physical Security

blast simulator, which simulates full-scale explosive loads up to 12,000 pounds per square inch per millisecond without using live explosives and producing a fireball. Energy deposition takes place in time intervals of two to four milliseconds, the same as in a live explosive event. Blast simulator test results have been validated against full-scale live explosive field tests. Fully controlled, fully repeatable, simulated blast load tests have been performed since 2005 on a wide variety of critical structural elements and systems. As a part of this effort, UCSD used the blast simulator to investigate structures such as steel column systems, steel cellular bridge tower components, fortified construction materials, and high performance and ultra high performance concrete panels. Requests for additional information should be sent to se-faculty@soe.ucsd.edu.

Electrical Power Transmission Line Security Monitor System

The energy infrastructure is a critical target that, when disrupted, can cause major economic, safety, and national security impacts to the U.S. government, military, private industry, and general public. Having the ability to alert local and regional utility transmission operators of attacks in real time may provide sufficient warning to allow for preemptive system control, thereby preventing regional outages and giving the military and/or law enforcement agencies a chance to terminate the attack in progress or capture the adversaries in the area of the attack. The Electrical Power Transmission Line Security Monitor System ("Power Pill") provides a means for real-time monitoring of physical threats or damage to electrical power transmission towers and conductors, as well as operational characteristics such as conductor temperature and sag. The system is designed to monitor long stretches of transmission lines in remote areas where security infrastructure does not exist, with the sensors taking power from the transmission line and relaying, by radio frequency, basic health or impact information to a control site or substation for operator awareness or action. The system is based on a prototype developed by the Idaho National Laboratory and is currently installed for operational test and evaluation on transmission lines in the United States. Requests for additional information should be sent to John.Svoboda@inl.gov.

Explosive Synthesis Laboratory

The proliferation of unique and novel explosive mixtures and methods of employment against transportation targets are a credible threat both domestically and internationally. A growing need exists to increase knowledge of the characteristics of novel explosive mixtures that threaten safety and security of transportation assets within the United States and abroad and how environmental conditions influence their destructive capacity. To better understand the threat and establish metrics needed for the development of countermeasures, TSWG—in collaboration with the government of Israel—constructed the Explosive Synthesis Laboratory. The Explosive Synthesis Laboratory is a dedicated resource

Physical Security

designed to allow characterization of novel explosive mixtures and how they act under conditions of interest. This information will allow further development of refined screening processes, infrastructure upgrades to transportation assets, and more robust containment measures to better secure safe passage for goods and personnel. Requests for additional information should be sent to pssubgroup@tswg.gov.

Foreign Vehicle Characterization

Existing vehicle barrier selection guides were developed based on vehicle characteristics such as acceleration speed, height, weight, and the turning ability of vehicles at various speeds of now outdated, U.S.-only vehicle data. The Foreign Vehicle Characterization project was initiated to update this data given changes in the automotive industry, the variation of vehicles found worldwide, and the evolution and movement of terrorist threats and locations of U.S. assets abroad. TSWG, in collaboration with its United Kingdom partners, analyzed the availability and characteristics of vehicles operated in selected countries and regions of interest. The final Worldwide Vehicle Identification Report analyzes vehicle fleets by category (light vehicles to large, rigid vehicles), documents the availability of vehicles operated outside the U.S., identifies and characterizes the vehicle population by region, and identifies commercial vehicles by region. Requests for additional information should be sent to pssubgroup@tswg.gov.

Joint Airborne Network Security

The increasing interconnectedness of aviation systems raises concerns about potential cyber security vulnerabilities that may have an impact on aircraft safety. To combat such threats TSWG, in collaboration with the United Kingdom, developed the Joint Airborne Network Security (JANS) project to assess vulnerabilities and provide recommendations to government and industry on security issues associated with increasingly "e-enabled" aviation. This project produced best practice guides distributed to government and industry on specific issues of concern, as well as the creation of the Airborne Network Security Simulator (ANSS). The ANSS integrates industry and government aeronautical simulators utilized to test, calibrate, exercise procedures, and assess potential weaknesses and vulnerabilities in a controlled environment without endangering safety and/or unnecessarily allocating resources. Requests for additional information should be sent to pssubgroup@tswg.gov.

Omni-Directional Flash & Launch Detection, Positioning, Classifications and Observations System (MEGA)

Instantaneously locating the source of incoming attacks from a concealed or overt position is crucial in protecting forces deploying into austere, nonsecure locations. Through CTTSO's bilateral agreement with the Israeli Ministry of Defense and funding sponsorship from the Defense Advanced Research Projects Agency, a muzzle flash detection system

Physical Security

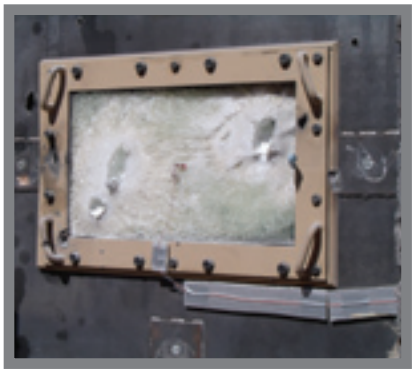
was developed. MEGA is a system that uses infrared sensors that, when configured onto a vehicle platform, will provide 360-degree imagery of its surroundings to detect, locate, and classify weapon discharges from effective sniper, anti-tank guided missile and rocket-propelled grenade ranges. The information can then be communicated to other elements of the unit to target potential and confirmed threats. MEGA will decrease the number of casualties by significantly increasing the response time of the troops in seeking protection and providing counter fire. System development is complete and will be integrated onto a vehicle platform for final testing and certification. Requests for additional information should be sent to pssubgroup@tswg.gov.

Outpost Surveillance System

The Outpost Surveillance System (OSS) provides enhanced area surveillance and an augmented reaction capability for a small, far-forward deployed operational element in an unconventional warfare/counterinsurgency environment. OSS is a day and night thermal imager designed to be used at austere outposts that have little infrastructure to support larger and more sophisticated systems. This simple, short-range imaging system detects the presence of human-sized targets out to approximately 400 meters. The system is portable, network capable, easy to install and operate, and requires minimal logistics support. OSS imagery can be viewed on location via a handheld or mounted monitor and/or relayed to a remote command post via a WaveRelay™ mesh radio. The system includes a power solution designed to keep the imager operating for at least 12 continuous hours on battery power and can utilize local indigenous power sources when available. Requests for additional information should be sent to pssubgroup@tswg.gov.

Selected Current Projects

Composite Glass Development



Current armor windows for expeditionary structures such as outposts, entry control buildings, and vehicles interfere with targeting and detection sensors and high powered long range reconnaissance and observation devices. Existing windows do not provide adequate levels of protection against blast, fragmentation, and multi-hit events. This research effort will develop a new transparent armor solution that is sensor compatible, allowing employment of operational technologies without exposing operators to hazards accompanied by opening windows or removing protective glass panes during targeting or observation activities. Advanced Transparent Glass Ceramic Armor (DiamondView® Armor) transmits infrared light leading to superior compatibility with night vision or infrared sensors and can be formed into curved windows for mobile or fixed asset applications. This clear armor solution is lighter in weight and higher performance when compared to traditional soda lime glass armor, demonstrating 20 to 40 percent weight savings and superior multi-hit bullet and fragmentation protection during realistic testing scenarios.

Physical Security

Detection of Rocket Attacks

Massive civilian and military casualties occur daily as a result of rocket and mortar attacks. These losses lead to poor morale, loss of battlefield effectiveness, and combat fatigue. The first few seconds of an attack can be critical to survival. CTTSO and the U.S. Army Research, Development and Engineering Command co-funded Detection of Rocket Attacks (DORA) through a bilateral agreement with the Israeli Ministry of Defense to develop a system for early warning of rocket and mortar attacks. The objective of the system is to detect, track, and localize tactical rockets and mortars being fired at stationary ground targets such as camps, posts, or towns. The system will also transmit detection data to a central processing unit capable of issuing an alert signal and a response.

Integrated Ruggedized Checkpoint Container

An array of effective screening and inspection technologies exist to assist the warfighter and domestic first responder. However, these capabilities have not been integrated in a single, ruggedized, and reconfigurable package. Multiple stand-alone systems increase manpower requirements, reduce the operational effectiveness of the responding unit, and create logistical burdens, which reduce the overall effectiveness of the individual systems. The Integrated Ruggedized Checkpoint Container (IRCC) will integrate a suite of modular ruggedized inspection systems into one mobile container to provide a turnkey entry control checkpoint with a single, easy-to-use graphic user interface. The container will be C-130 transportable and towable by a Mine Resistant Ambush Protected or similar vehicle. The ruggedized container system will function as a modular, reconfigurable checkpoint that will house the latest proven technologies in screening equipment for personnel, baggage, vehicles, and footwear. In addition, the IRCC will be capable of integrating other technologies of interest, such as camera systems and sensors, into a more operationally relevant system.

Night Vision Glasses

Current night vision (NV) optics are heavy, bulky, and are difficult to employ in confined spaces. The NV Glasses project will design, develop, and test cutting edge technology utilized in the medical field to produce an instantaneous, low profile, lightweight, night vision capability. The NV Glasses are intended for tactical use in a variety of environments including urban, desert, and mountainous terrain where sand, dust, and salt spray may have an adverse impact. Weight, durability, battery life, and clarity of the prototype will provide an enhanced capability to U.S. troops, bomb technicians, and law enforcement personnel.

Pipeline Blast Mitigation Technologies

As a critical part of the nation's infrastructure, damage to pipelines could have a great impact on the U.S. economy and environment. This effort identified existing research and technology specifically for blast protection of pipelines, identified and evaluated the vulnerability of

Physical Security

pipeline systems and infrastructure, and identified and evaluated generic blast-mitigation technologies that may be applied to the specific case of pipeline protection. Blast mitigation products were evaluated with numerical modeling methods to estimate their capacity for reducing vulnerabilities of pipeline components. The modeling data will be verified through explosive testing on pipeline components, with and without blast-mitigation retrofits. The results of this testing will be used to define the types of pipeline components, the explosive threats, and the most promising blast-mitigation technologies. The study findings were shared with the Department of Homeland Security and, at their request, will be combined into a book and available for purchase via the Government Printing Office.

Portable Seismic Acoustic Sensor Kit

Smuggling operations are increasingly using tunnels to avoid interdiction on both the northern and southern borders of the United States, and tunnels are being used internationally both against foreign partners and in U.S. theatres of operation. Denying the use of border tunnels and the terrorist use of the subterranean environment has become a strategic necessity, and the Portable Seismic Acoustic Sensor Kit (PSASK) is being developed to address those needs. The PSASK is a seismic-acoustic sensor system that will enable operators to detect and locate tunnel operations. This system will be portable for use in remote locations and will not require external power for forward deployment. The system alerts the operator to tunneling operations by sensing, identifying, and reporting on-foot traffic, digging with hand tools, or digging with power tools and is able to eliminate background noise and clutter in a signal-rich environment in both urban and rural settings. The sensors communicate wirelessly with the monitoring station and require a minimum user interface until an alert is received. The PSASK system not only detects and localizes tunnel activity below the surface but can also be programmed to detect and report on ground level foot and vehicle traffic and on helicopters, airplanes, and ultra lights above ground.

Security Observation Set

The Security Observation Set (SOS) project improves upon a previously funded TSWG effort, the Digital Observation Guard (DOG). The DOG system was operationally evaluated by U.S. Special Forces and federal law enforcement agencies in live situations. Based on feedback received, TSWG initiated the SOS project. The SOS system employs more covert and easily deployable and recoverable video surveillance systems that are compatible with the currently used DOG components. The new system will support new cameras, sensors, alarm, and wireless capabilities along with enhanced intrusion detection monitoring and annunciation. The SOS system is highly modular with a number of configurations to suit various security and surveillance scenarios and environments. In its full configuration, the SOS system will be able to provide surveillance out to one kilometer, perimeter breach detection, large area intrusion detection,

Physical Security

and building and interior intrusion detection in both wired and wireless or hybrid configurations. The system is capable of audible and visible alarm annunciation, video display, recording, playback and export, and cursor on target processing.

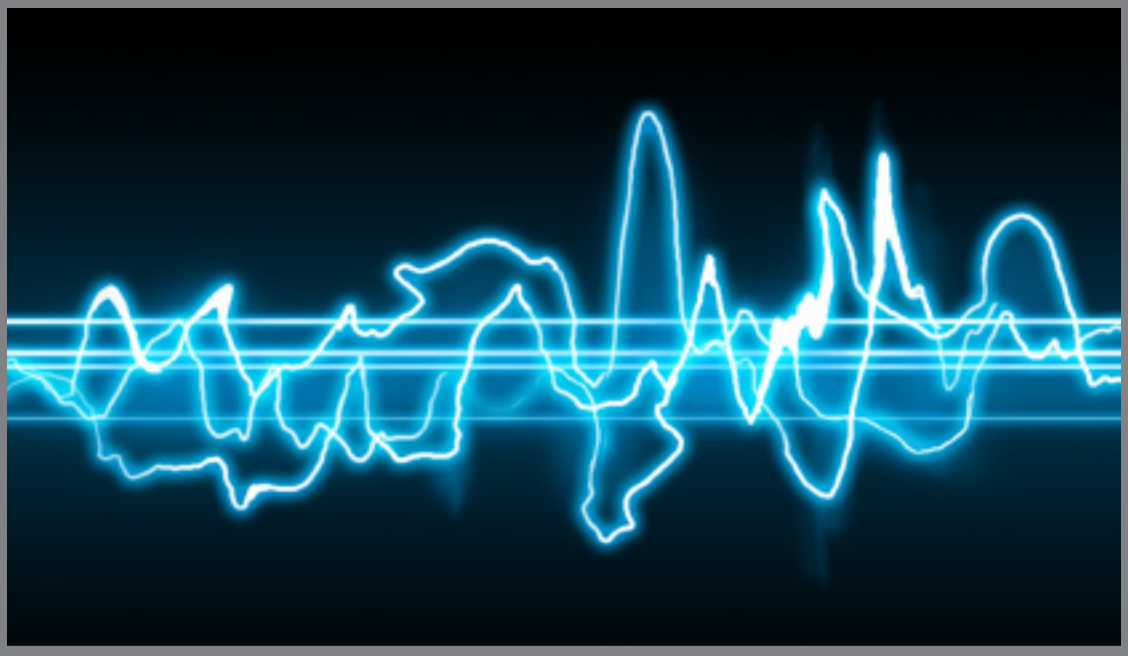
Universal Biometric Translator

Forward deployed personnel require the ability to transfer information between multiple handheld biometric devices they employ. The Universal Biometric Translator (UBT) will allow for the "transparent" transfer of information between all fielded biometric devices. Based on input from deployed end users, five fielded devices have been identified to be utilized with the UBT. However, the architecture of the UBT will allow for incorporation of new systems as they are developed. The UBT processor will be run in the command-and-control node and will receive data individually from the various handheld devices. The UBT will place the data received into a common data repository, which will allow for an aggregate view of all data collected on various handheld devices, as well as transfer this integrated data back to the various handheld devices. The UBT will also manage electronic biometric transmission transactions between the devices and higher headquarters level systems.

Contact Information

pssubgroup@tswg.gov

A comprehensive listing of member organizations by subgroup is provided in the appendix.



Surveillance, Collection, and Operations Support

Surveillance, Collection, and Operations Support

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements supporting intelligence gathering and special operations directed against terrorist activities.

The Surveillance, Collection, and Operations Support (SCOS) Subgroup identifies high-priority user requirements and special technology initiatives focused primarily on countering terrorism through offensive operations. SCOS research and development projects enhance U.S. intelligence capabilities to conduct retaliatory or preemptive operations and reduce the capabilities and support available to terrorists. A representative from the Intelligence Community chairs the subgroup.

Focus Areas

The SCOS Subgroup focus areas reflect the prioritized requirements of the Intelligence Community. During FY 2010, these focus areas were:

Traditional Surveillance

Improve the quality of intelligence collection. Develop and advance capabilities for the collection and enhancement of video, imagery, and audio surveillance.

Analytical Surveillance

Improve automated tools for terrorist identification using biometrics, pattern recognition, speech and speaker recognition, and information retrieval from multiple sources.

Intelligence, Surveillance, and Reconnaissance

Develop and improve the capability to locate, identify, and track terrorist activities. Support programs and initiatives critical to intelligence operations, such as tagging, tracking, and locating; special sensors; and clandestine communications.

Information Operations

Develop and improve tools to degrade, disrupt, deny, or destroy both analog and digital adversary and information systems.

Human Language Technologies

Respond to emerging needs for advanced language solutions in the operational environment including data exploitation and analysis of information in languages other than English and technology to enhance language proficiency and cultural skills. Develop new approaches to triage multisource, multigenre, and multilingual data in order to increase actionable intelligence at all levels of operational mission.

Surveillance, Collection, and Operations Support

Program Highlights

SCOS projects are classified or highly sensitive. Program requirements, the success of projects, and specific capabilities cannot be discussed in an unclassified document.

Contact Information

scossubgroup@tswg.gov

TSWG SUBGROUPS

Tactical Operations Support

Tactical Operations Support

Mission

Identify, prioritize, and execute research and development projects that enhance the capabilities of Department of Defense and interagency special operations tactical teams engaged in finding, fixing, and finishing terrorists. This includes the development of capabilities for state and local law enforcement agencies to combat domestic terrorism.

The Tactical Operations Support (TOS) Subgroup provides technology solutions to assist "direct action" operational personnel in a variety of tactical missions and environments. Most often these solutions are in the form of rapidly prototyped and specialized equipment. Each material solution is specifically designed to provide enhanced mission effectiveness while assisting operational personnel in maintaining "situational awareness." The subgroup is co-chaired by representatives from the Department of Defense and the Department of Energy.

Focus Areas

The TOS Subgroup focus areas reflect the prioritized requirements of offensive counterterrorism forces. During FY 2010, these focus areas were:

Communications Systems

Develop flexible and enhanced communications capabilities specifically designed for tactical forces. Emphasize reducing the size of equipment while improving operator mobility and efficiency. Consider durability, concealment, innovative power sources, range, reception, battery life, ease of use, and low probability of detection/interception. Develop assured tactical communications connectivity in challenging environments such as buildings, caves, tunnels, below deck, or underground bunkers.

Intelligence, Surveillance, Target Acquisition, and Reconnaissance Systems

Develop technologies to assist tactical teams in conducting intelligence, surveillance, target acquisition, and reconnaissance missions. Develop systems that enhance the visual perception or other imaging capabilities of tactical operators in all conditions and environments. Develop independent, vehicular or weapon-mounted systems for enhanced aiming, target designation, illumination, range detection, or surveillance.

Offensive Systems

Develop equipment and capabilities that enhance the effectiveness of small offensive tactical teams engaged in specialized operations. Develop specialized weapons, munitions, detonators, distraction/diversion devices, and other unique tactical equipment. Develop systems to support sniper and countersniper operations. Develop man-portable

Tactical Operations Support

sensor systems to enhance operator security during tactical missions.

Specialized Access Systems

Develop technologies that assist tactical assault forces in gaining rapid access to objectives, improve evaluation of tactical options, and support efficiency and stealth of operations. Develop enhanced manual and dynamic breaching technologies for tactical assault teams. Develop clandestine defeat or override devices for building and vehicle entry points.

Survivability Systems

Develop clothing, individual equipment, mobility platform enhancements, and man-portable systems that provide protection from or identification of ballistic, fragmentation, explosive, and thermal threats during the conduct of tactical missions.

Unconventional Warfare, Counterinsurgency Support

Develop innovative solutions for small specialized tactical operations teams conducting a broad spectrum of military and paramilitary operations including counterinsurgency and foreign internal defense missions through, with, or by host nation indigenous forces building partner capacity to support U.S. objectives.

Selected Completed Projects

Night Vision Security Enhancer

Tactical operators had a requirement for a wireless infrared (IR) illuminator and motion sensing system to enhance temporary site security. The Night Vision Security Enhancer (Night VISER) system was developed by Applied Research Associates to be used during tactical operations in urban and suburban environments as well as in rural or wilderness environments. The system's primary function is to increase the ability of a sentry with a night vision device to monitor both open terrain and limited avenues of approach and provide early warning of potential threats. Independent nodes alert the sentry that human-sized motion has been detected in the area of interrogation and illuminates the area with IR light. The nodes operate on a mesh network and can be deployed at distances beyond 100 meters from the sentry. The system consists of four nodes and a handheld remote control that is compact, rugged, and rapidly deployable. Requests for additional information should be sent to tossubgroup@tswg.gov.

Tactical Survey System

The response time for tactical teams during an emergency is a critical aspect to mitigating a crisis scenario. In order to respond in a rapid manner, tactical teams must have the critical building information to formulate response plans and procedures. The Tactical Survey System is an incident preplanning and response solution that was developed by the Tactical Survey Group. The Tactical Survey System is an HTML-based

Tactical Operations Support

digital mapping software application for managing crisis situations and improving emergency response and preparations at critical installations. The system captures detailed information such as utility shutoff locations, building construction information, 360-degree interior and exterior imagery, floor plans and other site-specific information required to reflect the characteristics of the specific facility. The Tactical Survey System provides the tactical teams with an enhanced training tool, a database of information on a facility, and aids in recovery by providing a reliable point of reference for every room in a facility. Requests for additional information should be sent to tossubgroup@tswg.gov.

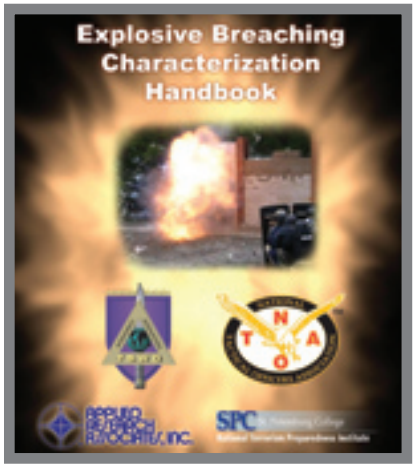
Selected Current Projects

Law Enforcement Tactical Ballistic Helmet

Domestic law enforcement and special response teams face threats from high-velocity, high-caliber ballistic threat rounds and require a helmet that provides protection from these rounds. In 2008 the TOS Subgroup worked with Artisent, Inc. to develop the Law Enforcement Tactical Ballistic Helmet as a testing prototype. As materials in ballistic protection have increased in strength and decreased in weight, the TOS Subgroup has remained engaged in developing a functional ballistic helmet that is affordable to the law enforcement community. In 2011 Artisent, Inc. will deliver an enhanced pre-production prototype helmet that will be capable of stopping .44 Magnum rounds with minimal backface deformation, have an internal drop-down ballistic visor, and include an adjustable head fit-band retentions system for comfort.

Multifunctional GPS/Emergency Device

In order to effectively operate on the battlefield, Special Operations Forces (SOF) operators have unique requirements for communication and navigation. When working in small teams, SOF elements are reliant on the equipment they carry in order to execute missions in austere and dangerous environments. The Multifunction GPS/Emergency Device (MGED) provides the SOF operator with one ubiquitous device that integrates the functionality of the Blue Force Tracking system, the capability of the Combat Survivor Evader Locator radio, and the ease of use of a commercially available GPS device. The MGED will allow users to communicate intra/inter-team and have over-the-horizon reach back to command infrastructure. The MGED is currently being developed by Trident Systems.



Maritime Breaching Handbook

As a continuation of prior work in providing a functional handbook for explosive breachers, the TOS Subgroup is developing a Maritime Breaching Handbook to aid tactical teams with breaching in the unique maritime environment. The Maritime Breaching Handbook will give the end user a comprehensive guide to attacking and defeating targets on ships. In addition to providing specific data related to attack methods,

Tactical Operations Support

the handbook will cover the inherent dangers and considerations found in maritime environments.

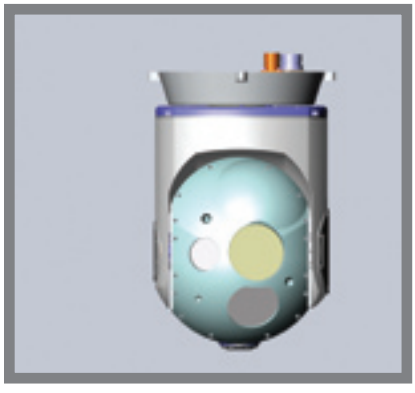
Special Timer Activated Restraint and Release System

The Special Timer Activated Restraint and Release System (STARRS) is a simple, low-cost device that will enable tactical teams to temporarily restrain individuals for a predetermined amount of time and automatically release them after the time has expired. STARRS has a simple-to-use interface and features a slip-on design that will work with any flex-cuff currently available on the market. Once the device is installed and activated, the person being restrained is reassured in his native language that he will be released soon, and the tactical team can make a safe exit from the area. The STARRS will increase the safety of both tactical teams and the individuals who are restrained in the process of operations.

Air to Ground Mobile Mesh Network

Currently, Special Operations Forces do not have the ability to receive digital, encrypted full motion video directly from Unmanned Aerial Systems (UAS) to a dismounted operator at the target location. The Air/Ground Mobile Mesh Network (AGMMN) uses a man-wearable tactical mobile ad hoc network called WaveRelay™, which allows dismounted operators to receive and view full motion video with AES-256 encryption and is encoded with H.264 commercial compression (other compression standards are available). Additionally, since the AGMMN is a tactical mobile ad hoc network, the full motion video and other data can be automatically routed to any user within the network without the need for a direct connection to the UAS.

Triple Sensor/Designator-Stabilized Miniature Payload



The Triple Sensor/Designator-Stabilized Miniature Payload (TD-STAMP) is a state-of-the-art UAS payload, which is the smallest and lightest at less than 4.5 kilograms total weight, available offering the following sensors and mechanical features: Cooled Mid-Wave IR Camera with Optical Zoom, High-Definition Color Day Camera with Optical Zoom, 30mJ Laser Designator, IR Laser Pointer and three gyros for mechanical stabilization. The TD-STAMP is being integrated with an optical tracker card that will provide the ability to select and autonomously track targets without the need for software post-processing at the UAS Ground Control Station. Additionally, the TD-STAMP can create geo-rectified aerial imagery stitched from either the mid-wavelength infrared or high-definition color day cameras.

Enhanced Mortar Targeting System

The Enhanced Mortar Targeting System (EMTS) was developed to address the critical capability gaps of providing precision indirect fire 360 degrees from a single firing position using existing U.S. mortar tubes (120 millimeters or 81 millimeters adjusted by mortar tube collar) and U.S. standard non-guided ammunition. The EMTS has an integrated fire

Tactical Operations Support

control system, which, once provided target coordinates, automatically lays the mortar tube within 20 seconds and will provide accuracy with a standard mortar within one percent of range.

Contact Information

tossubgroup@tswg.gov

A comprehensive listing of member organizations by subgroup is provided in the appendix.

DoD photo by Master Sgt. Kevin J. Gruenwald, U.S. Air Force

Training Technology Development

Training Technology Development

Mission

Identify, prioritize, and execute projects that satisfy interagency requirements for the development and delivery of combating terrorism related education, training, and mission performance support products and technologies.

The Training Technology Development (TTD) Subgroup delivers training and training technologies to increase mission readiness and enhance operational capabilities in the combating terrorism community. The strategy behind the mission is to analyze, design, develop, integrate, evaluate, and leverage distributed learning technologies to deliver high-quality training and education in the medium best suited to the users' needs and requirements. A representative from the U.S. Marine Corps chairs the subgroup.

Focus Areas

The TTD Subgroup focus areas reflect the prioritized requirements of the military and civilian combating terrorism communities. During FY 2010, these focus areas were:

Models, Simulations, and Games

Develop interactive models, simulations, and games (MS&G), including, but not limited to: tabletop simulations, field exercise simulations, immersive virtual-learning environments, hands-on virtual reality, simulation models, and PC-based three-dimensional and isometric simulations and games. Develop crowd models, adversarial behavior models, network-based simulations, and mini-simulations on specific combating terrorism related tasks. Incorporate beneficial game characteristics through the full range of game genres (i.e., strategy, first person tactical, massively multiplayer online game, role-playing, etc.). Develop tools, technologies, and techniques for improving MS&G design, development, and validation.

Advanced Training and Education

Develop programs of instruction, training packages, and computer- and classroom-based terrorism training courses. Develop the advanced tools, techniques, and guidelines required to analyze needs, develop solutions, and evaluate results. Analyze performance needs to identify applicable solutions. Integrate delivery technologies with combating terrorism training materials to increase the quality, effectiveness, and accessibility of training.

Training and Information Aids and Devices

Develop job aids, performance improvement solutions, and training devices to support mission performance and increase mission readiness. Support new areas in the combating terrorism domain. Provide training simulants as aids in training exercises.

Training Technology Development

Delivery Architectures

Develop new, advance emerging, and enhance existing training to combating terrorism personnel. Emphasize ubiquitous and distributed computing to provide the basis for information and training technology interoperability and the standards needed to provide distributed, on demand, and customized training consistent with future computing infrastructure. Emphasize proven methods of effective and individualized instruction and electronic performance support.

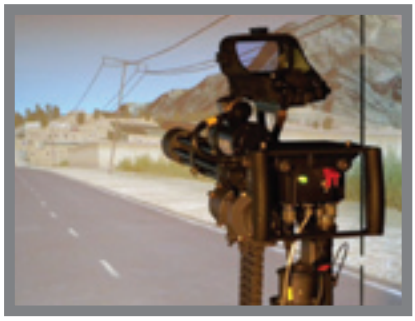
Selected Completed Projects

Special Operations Advanced Sniper Simulator

Training snipers to conduct missions on a long, known distance range is essential to develop and maintain critical marksmanship skills. Due to land use constraints, a limited number of adequate ranges available for training and testing sniper skills in sniper and counter-sniper missions exist. In response, Advanced Interactive Systems, Inc. developed a virtual-live fire sniper simulator that can handle up to a 50-caliber round and that can duplicate the conditions of a known distance range in a complex urban environment. Within these modular containers, sensors accurately record the strike of each live round and provide detailed scenario feedback on the probability of a kill given a hit. Requests for additional information should be sent to ttdsubgroup@tswg.gov.

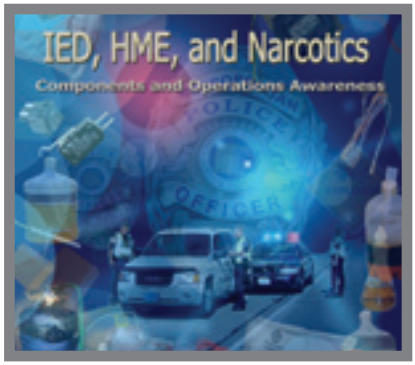
M134 Minigun Simulator

The M134 Minigun's high rate of fire (more than 3,000 rounds per minute) makes it a valuable weapon system downrange. However, using live rounds to train and qualify operators on the Minigun is extremely expensive, often prohibiting advanced training and limiting trainee throughput. As part of a joint effort sponsored by the Department of Defense and the Department of Energy, Cubic Defense Applications developed a high fidelity simulator that provides comparable and compatible training on the M134 Minigun at a fraction of the cost. The simulated weapon provides the look and feel of the Minigun while allowing the warfighter to engage targets on a virtual screen. Requests for additional information should be sent to ttdsubgroup@tswg.gov.



Improvised Explosive Device, Homemade Explosive, and Narcotics Component and Operations Awareness Web-Based Course

The threat of terrorism through the use of improvised explosive devices and homemade explosives against civilian and military law enforcement personnel has increased significantly. To address this threat, A-T Solutions designed and developed an Improvised Explosive Device, Homemade Explosive, and Narcotics Component and Operations Awareness Web-based course. By using text, imagery, videos, and interactive learning



Training Technology Development

activities, the course trains law enforcement personnel to differentiate between and respond appropriately to improvised explosives, homemade explosives, and narcotics-related incidents. The course is hosted on the Department of Homeland Security's Technical Resource for Incident Prevention (TRIPwire) Web site. Requests for additional information should be sent to ttdsubgroup@tswg.gov.

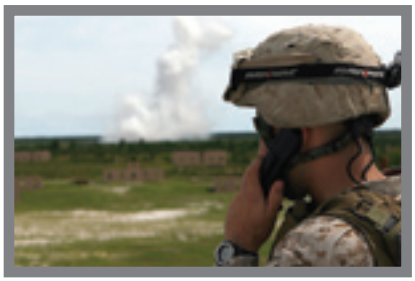
Post Blast Investigation Training for EOD Technicians

Following an improvised explosive device (IED) incident, the post-blast scene contains information that can be used to prevent and deter future IED incidents. However, it is critical that this information is gathered in a proper and timely manner by Explosive Ordnance Disposal (EOD) personnel who are trained in accurate and detailed tactical exploitations. The Post-Blast Investigation (PBI) Training for Military EOD Technicians developed by A-T Solutions, in cooperation with the U.S. Air Force and FBI, emphasizes proper evidence collection and preservation techniques by EOD technicians on the battlefield. The course focuses on the appropriate tactical approach, lexicon use, and attention to detail in report writing. The course is hosted on the U.S. Army's Joint Knowledge Online Web-based training portal. PBI field guides are available through the Government Printing Office at http://bookstore.gpo.gov.

PBI Field Guide Stock Number: 008-001-00207-6

Selected Current Projects

Incidental Fire Support Training for Observers



In the absence of a Forward Air Controller, Joint Terminal Attack Controller, Joint Fires Observer, or Forward Observer, the squad leader and squad may be required to act as observers in order to employ both air and surface delivered fires. In cooperation with the U.S. Marine Corps, the Penro Group is developing a training package that includes lessons on types of terminal attack control, self and target location, call for fire, close air support, talk-on techniques, and battle damage assessment. The training package contains instructor presentations and notes, student materials, video demonstrations, student evaluations, guidebooks, and reference cards. In addition to the new training content, the package incorporates practical exercises and sustainment training utilizing the current Marine Corps Deployable Virtual Training Environment laptop simulation system. The training package will be available through the Marine Corps' Training and Education Command in the spring of 2011.

Tactical Driving Simulator

When providing transportation and movement protection to high-profile government officials (i.e., VIPs) within the United States and abroad, protective detail personnel must be prepared to effectively and efficiently respond to threats upon the VIP. In collaboration with the Pentagon Force Protection Agency, U.S. Secret Service, and the U.S. Department of State,

Training Technology Development

Quantum Signal is developing a PC-based Tactical Driving Simulator that will help train and evaluate—within a virtual environment—the skills necessary for transporting VIPs and responding to threats. The simulation will provide a range of programmable scenarios that require situational awareness, decision making, and action, including principles of route planning and analysis, evasive driving skills, force-on-force counter ambush tactics, vehicle dynamics during crash avoidance, and defensive driving techniques when in hostile situations. The Tactical Driving Simulator project will be completed in the summer of 2011.

Culture and Irregular Conflict Courses

Trends in the global operational environment demand new skills for assessing the motivations leading to violent confrontation. Soldiers and civilians possessing an understanding of cultural variations can influence operational outcomes through the selective implementation of irregular tactics, techniques, and procedures. In cooperation with JFK Special Warfare Center and School (JFKSWCS), Norwich University Applied Research Institutes are developing computer-based undergraduate and graduate level courses to help the warfighter meet the challenges of persistent irregular conflict. The Culture and Irregular Conflict courses will be informed by anthropology and sociology as well as Department of Defense doctrine. The goal is to enable the warfighter to understand ethnic, religious and cultural rivalries resulting in the ability to predict, influence, and moderate the evolutionary path in which violent conflicts develop. Verifiable improvements in cross-cultural competence of students are anticipated in areas including cultural factors, socio-cultural awareness, social capital, social networks, values, decision-making styles, interpersonal skills, and personality factors. The courses will meet American Council on Education standards and be integrated into the JFKSWCS curriculum in the fall of 2011.

Assessment of Mobile Learning Trends for Use by the Military

The use of mobile technologies and Internet-based capabilities for training and educational purposes are the fastest growing and most useful developments in the training world today. The Center for Innovative Technology (CIT) conducted two assessments—one on mobile learning trends and challenges and the other on Internet-based capabilities—with the ultimate goal of shaping and developing new learning technologies and best practices within the Department of Defense. The assessments identified viable training alternatives, current and emerging mobile learning and Internet-based technologies, solutions, capabilities, best practices, and lessons learned for use within the military. Based on those assessments, CIT is working with the United States Marine Corps' Training and Education Command and the Army's Training and Doctrine Command on an implementation plan for how to implement a mobile learning program in each environment. This plan outlines the technical architecture, identifies the mobile learning content relevant to end users,

Training Technology Development

and lists the operational support requirements necessary to sustain a long-term program. CIT is also working with the U.S. Joint Forces Command on a plan to further integrate Internet-based capabilities into today's military training communities by detailing how information can be accessed across services. Results of the mobile learning and Internet-based capability assessments will be available to military, federal, state, and local government users through the TTD Subgroup at ttdsubgroup@tswg.gov.

Contact Information

ttdsubgroup@tswg.gov

A comprehensive listing of member organizations by subgroup is provided in the appendix.

U.S. Army photo by Spc. Theodore Schmidt

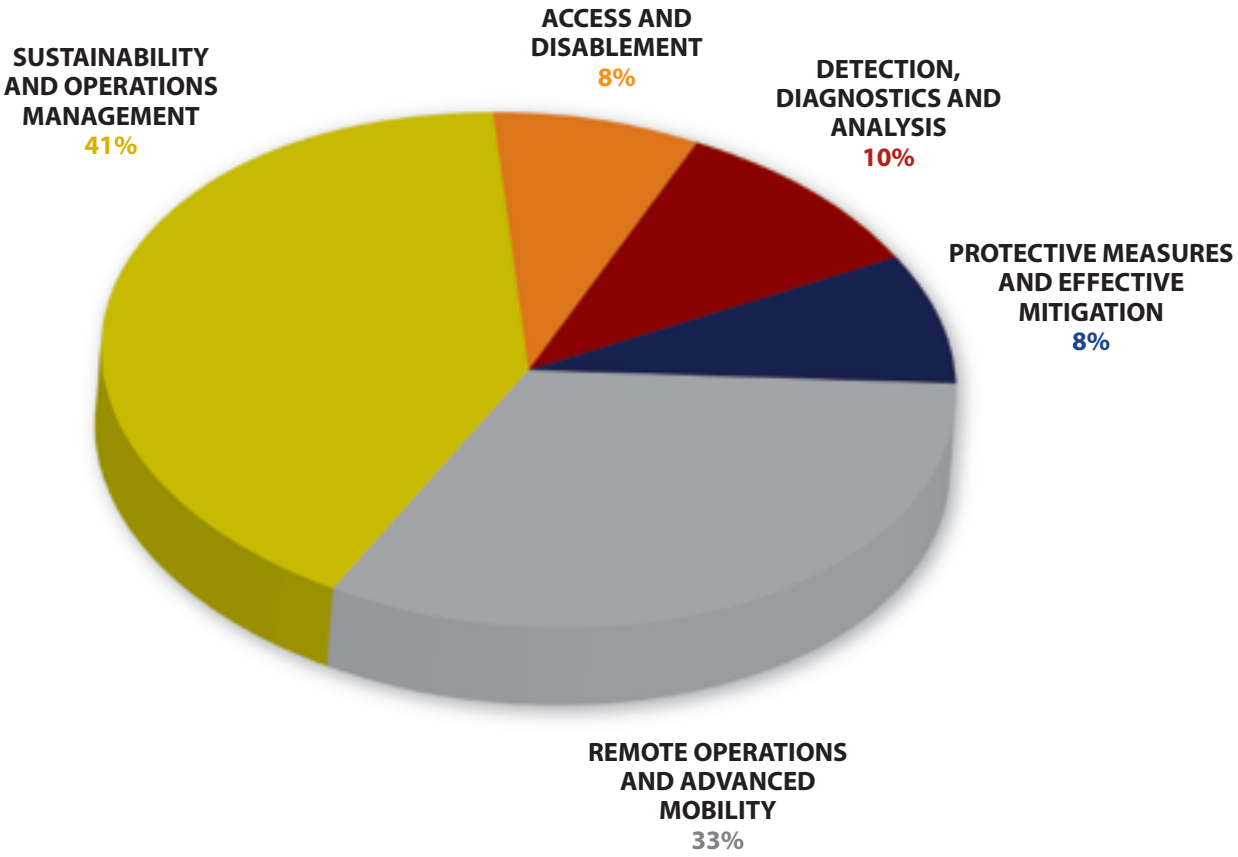
Explosive Ordnance Disposal/ Low-Intensity Conflict

Explosive Ordnance Disposal/ Low-Intensity Conflict

Mission and Organization

The Explosive Ordnance Disposal/Low-Intensity Conflict (EOD/LIC) program provides Joint Service EOD technicians and Special Operations Forces (SOF) operators with the advanced technologies and mission-focused solutions required to address current and emerging threats presented by unconventional and asymmetric warfare. These communities annually submit prioritized requirements, which are then reviewed and approved by the Office of the Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict and Interdependent Capabilities.

EOD/LIC FY 2010 Funding by Focus Area ($7 Million)



Explosive Ordnance Disposal/ Low-Intensity Conflict

Focus Areas

Remote Operations and Advanced Mobility

Develop capabilities to remotely approach, enter, and conduct reconnaissance operations in hazard areas and danger zones. Enhance mobility-related technologies and equipment to facilitate safely approaching, operating in, and withdrawing from hazardous environments. Develop systems and technologies to gather and store operational information for transmission to operational personnel and unit commanders. Improve technologies for the relocation of unexploded ordnance, hazardous materials, and improvised devices.

Access and Disablement

Develop tools to quickly and efficiently breach or gain access to structures, barriers, vehicles, and containers. Develop chemical, mechanical, electrical, and explosively actuated systems for the neutralization and disruption of unexploded ordnance and improvised devices. Improve technologies for rendering fuzing and firing systems inoperable.

Detection, Diagnostics, and Analysis

Develop tools to locate and verify the presence of improvised devices, unexploded ordnance, booby traps, and other threats. Develop technologies to determine the specific type, condition, and characteristics of unexploded ordnance and improvised device components and the specific hazards associated with each. Improve methods to analyze and evaluate improvised device construction.

Protective Measures and Effects Mitigation

Advance the development of personnel protection systems for operations in enhanced environments. Develop novel and improved solutions to protect personnel and property from blast, fragmentation, and ballistic hazards.

Sustainability and Operations Management

Develop tools and equipment to enhance situational awareness and operational capability during incident response or direct action operations. Develop human performance improvement tools that foster the advancement of knowledge related to unexploded ordnance, improvised devices, and enhanced hazard environments. Develop tools and training for conducting novel and advanced missions related to improvised devices and hazardous environments.

Selected Completed Projects

Vehicle-Borne Assisted Detection System

While performing vehicular route reconnaissance, a significant number of military personnel have been injured and killed by the detonation of

Explosive Ordnance Disposal/ Low-Intensity Conflict

anti-tank mines and pressure-plate improvised explosive devices (IEDs). Vehicles performing reconnaissance missions require a real-time mobile capability to detect these threats buried in the ground. The Marine Corps Special Operations Command (MARSOC) developed a Vehicle-Borne Assisted Detection System (VBADS) based on a modified Geonics EM-61 Ground Penetrating Radar. The detection coils mount to the front of the vehicle, and the system is easily stowed when the vehicle is not in use. MARSOC deployed eight systems to Operation Enduring Freedom in 2009 for initial operational evaluation. Improved generation two systems were deployed in 2010 for further evaluation. This effort was jointly funded by CTTSO, the Joint Improvised Explosive Device Defeat Organization, and the United States Special Operations Command. Requests for additional information should be sent to eodlic@eodlic.cttso.gov.

Jamming Effectiveness Tester

Both vehicular convoys and dismounted troops utilize portable electronic countermeasures (ECM) systems, or jammers, to protect them from threats like radio-controlled IEDs. Military forces require assurance that they are safely within the defensive envelope of their ECM systems. The Jamming Effectiveness Tester (JET), a U.S.–Israel bilateral effort, assesses ECM effectiveness and performs spectral analysis. The JET also indicates whether the operator's location is within the protective area covered by a nearby jamming system. It will also perform an over-the-air functional test to verify that a specified local jamming system is performing within its operational specifications. The JET is a handheld, stand-alone device capable of analyzing signals within the range of common military jammers. It has a straightforward user interface, a logging capability, and a feature to wipe sensitive data. Requests for additional information should be sent to eodlic@eodlic.cttso.gov.

Selected Current Projects

EOD Homemade Explosives Kit

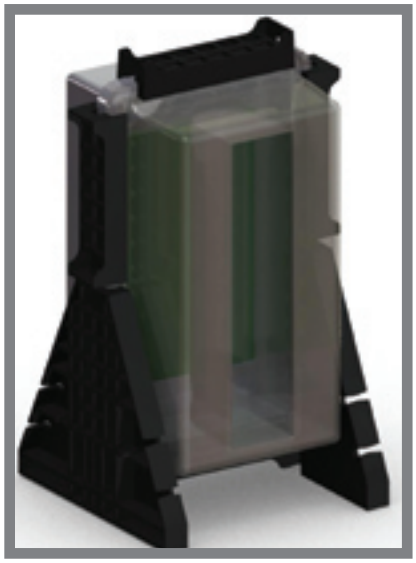
Homemade Explosives (HMEs) use by enemy forces has increased to the point that HMEs now pose a significant threat to military forces worldwide. As such, EOD technicians have a critical requirement for a field expedient capability to detect and identify HMEs. The EOD/LIC program investigated commercially available individual systems that could be packaged as a kit and meet the needs of EOD operators. Phase I of the EOD HME kit is comprised of the Thermo Scientific (formerly Ahura Scientific) FirstDefender handheld chemical identifier, the Smiths Detection HazMatID solid and liquid chemical identifier, and the American Innovations xD2i wet chemistry kit. The Naval EOD Technology Division developed a system-of-systems training course and manual that allows the operator to select the device best suited for the suspected threat. Nineteen kits were provided to EOD units deployed in various theatres of operation. Phase II of the effort looks at systems that provide the capability in a smaller form factor. The Phase II kit is comprised of the

Explosive Ordnance Disposal/ Low-Intensity Conflict

Thermo Scientific FirstDefender and TruDefender and the ChemSpectra Mini XD2. Ten kits and associated training will be provided to various EOD units for operational test and evaluation. The EOD HME kit's collection of systems has transitioned to a program of record through PMS-EOD under the Weapons of Mass Destruction Kit.

Concealed Device Disruption (Stingray)

EOD technicians require the capability to unearth buried or concealed IEDs to further exploit and render safe these devices. Sandia National Laboratories designed the Stingray, a shaped water charge that is an advanced, two function tool. The Stingray produces a high velocity, thin, coherent water blade from the front face and a directed wall of water from the back face. It was designed using advanced computer models to maximize the water velocity and optimize the blade shape. The Stingray's simple design and the decision to use injection molding technology have resulted in a low-cost manufacturing process. The EOD/LIC program funded a low rate initial production of the Stingray to support trials in current theatres of operation. Feedback from the evaluation by deployed forces will allow for the development of more effective employment procedures against buried or concealed IEDs.



Contact Information

eodlic@eodlic.cttso.gov

DoD photo by Lance Cpl. Jeremy Harris, U.S. Marine Corps

Human Social Culture Behavior Modeling Program

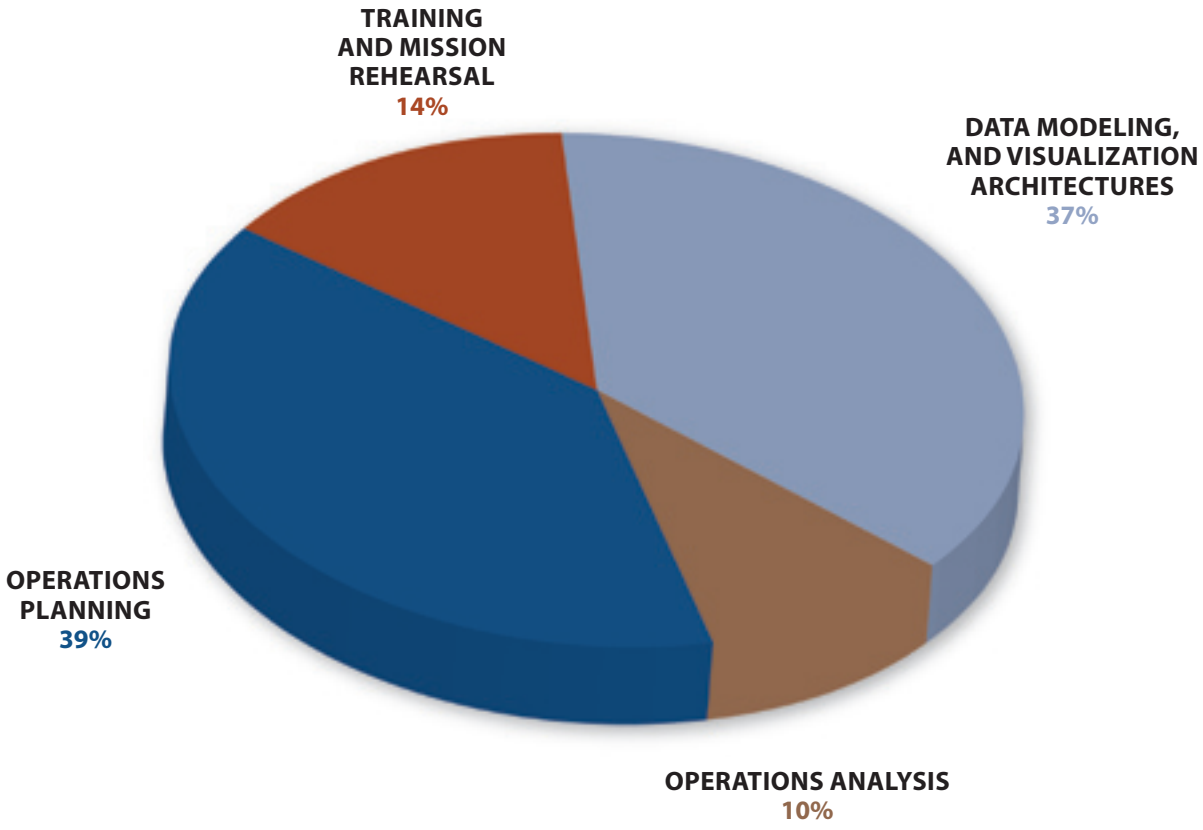
Human Social Culture Behavior Modeling Program

Mission

Develop tools and capabilities that facilitate sociocultural understanding, human terrain forecasting, and the application of human, social, cultural, and behavioral factors in mission planning and operations in diverse geographic regions.

Today's military is involved in a growing number of complex missions from Irregular Warfare to Stability, Security, Transition, and Reconstruction (SSTR) operations. These missions are best served by a force equipped to understand and appreciate the individual, tribal, cultural, ethnic, religious, social, and economic elements of the human terrain and able to apply this understanding to improve mission effectiveness. The CTTSO Human Social Cultural Behavior (HSCB) Modeling Program is working in conjunction with the military and multiple federal agencies. Funding is derived from the Office of the Secretary of Defense.

HSCB FY 2010 Funding by Focus Area ($16 Million)



Human Social Culture Behavior Modeling Program

Focus Areas

The HSCB Modeling Program focus areas reflect the prioritized requirements of the military and civilian combating-terrorism communities. During FY 2010, these focus areas were:

Operations Planning

Develop capabilities for military planners to enhance the understanding of complex operational problems related to the social and cultural terrain within their areas of responsibility. Design effective approaches that link potential effects of tactical actions to strategic aims. Develop tools that provide greater insight into how strategic, operational, and tactical operations may be impacted by, or may affect, the sociocultural dynamics and groups within the mission space.

Operations Analysis

Develop tools and capabilities, grounded in social science theory, that provide insight into affecting attitudes and behaviors of particular foreign audiences. Create tools that provide socioculturally relevant estimates of the likely outcomes of kinetic and nonkinetic courses of action with respect to potential effects on attitudes, beliefs, and actions. Specific emphasis is placed on forecasting the direct, second, third, and higher order of effects of a given course of action to minimize the adverse impacts and unintended consequences.

Training and Mission Rehearsal

Develop training, tools, technologies, and assessment metrics to provide warfighters with sociocultural understanding and skills to effectively conduct missions and shape events in unfamiliar cultural environments. Specific emphasis is placed on the integration of sociocultural models, based on robust theoretical foundations, into training systems for enhancing sociocultural and human behavior/cognition skills at both the operational and tactical levels. Create training capabilities that provide warfighters with the ability to quickly assess and identify societal norms, behaviors, and social structures in a specific social or cultural group. Develop nontraditional, field-capable technologies that enable the training and/or mission rehearsal of nontechnical, adaptive skills related to cultural understanding, interpersonal communication, and teamwork. Create flexible training systems to support ongoing operations by rapidly delivering understanding of complex new regions of interest and new mission areas (e.g., transition and reconstruction).

Data, Modeling, and Visualization Architectures

Develop operational frameworks for the model-based decision support systems to assist decision makers in understanding and operating within the social, cultural, and behavioral domains. These frameworks will allow the wide array of models being developed across the HSCB program to be readily interoperable with a variety of data sources

Human Social Culture Behavior Modeling Program

and supporting applications integrated into the systems used by the operational community. Develop automated data management, translation, and extraction tools to service HSCB models. Create tools, methods, and functional architectures for collection, storage, shared use, and dissemination of sociocultural data. Develop visualization tools and frameworks that integrate cultural information into a military operational environment to facilitate the appropriate interaction of key sociocultural elements.

Selected Completed Projects

Situated Cultural Training

Cultural sensemaking, the processes by which people come to understand and explain culturally different behaviors, is increasingly being recognized as a core cultural competency for U.S. warfighters. This competency rests on the ability to develop general cognitive and metacognitive skills that allow warfighters to obtain ad hoc the knowledge they need to act within specific cultural environments. In other words, it provides the warfighter with an analytical approach to culture that helps them ask the right questions, develop appropriate solutions to culturally challenging situations, and shape events across the spectrum of operations.

The Culture and Cognition Group of Applied Research Associates, Inc. developed a training guide, *What Happens After the 3rd Cup of Tea? A Sensemaking Guide to Afghanistan* that facilitates the development of cultural sensemaking and other critical thinking skills. The guide is organized around seven vignettes describing actual intercultural interactions that have taken place within operational contexts in Afghanistan and provides a typical American as well as a typical Afghan perspective on the situation (i.e., it describes the concerns and motivations driving thinking and decision making within the situation for both sides). Each vignette is based on actual events from Afghanistan as reported in interviews conducted with soldiers and Marines who had just returned from Afghanistan deployments. The Afghan perspective on the Afghan behavior in the vignettes is based on interviews and a quantitative survey with Afghans both in the United States and Afghanistan representing the four main ethnic groups in Afghanistan (Pashtun, Tajik, Hazara, and Uzbek). In addition to the stories, the guide provides commentary from U.S. warfighters and from Afghans about each vignette that show how U.S. warfighters and Afghans see a given situation differently. *What Happens After the 3rd Cup of Tea?* is available through the Government Printing Office Web site at http://bookstore.gpo.gov, Stock Number: 008-001-00206-8.

Plug and Play Cultural Avatars for Training and Mission Rehearsal

Training the U.S. military for today's missions requires human-to-human

Human Social Culture Behavior Modeling Program

interaction with realistic cognitive, social, and emotional behavior expressed through speech, gestures, facial expressions and posture—capabilities not found in current virtual training software. These perceptual cues allow the trainee to form estimates of the emotions, beliefs, desires, and intents of the simulated characters with which they interact, thereby guiding the trainees' decisions while building rapport, obtaining information, or influencing action. To support training for missions in regions of interest around the world, the cognitive/emotive and physical actions must reflect the cultural norms, expectations, and characteristic responses of persons of the targeted populations.

To meet these needs, Vcom3D and Soar Technology developed authoring tools and reusable, authentic culture-specific avatars for a wide range of mobile, Web-based, and multi-user interactive training simulations. The avatars are based on cognitive and physical (observable) behavior models. The cognitive modeling architecture provides the sensemaking, motivations, and desires for acting, and the physical modeling architecture provides the outward expression of those behaviors. Combining these two technologies created realistic, cross-cultural rapport-building and negotiation experiences. VCom3D and Soar Technology developed prototype coursework to demonstrate their plug-and-play capabilities—a module for building rapport in Iraq, and a module for the development of interpersonal and negotiation skills in Afghanistan. In the Afghan module the trainee needs to train and support a cadre of village workers, support the Afghan Army's manpower needs, establish a working partnership between the Afghan government and the village power broker, and provide prestige to the local Afghan people. The module incorporates multiple Afghan subcultures (e.g. Pashtun and Tajik). The prototype coursework and authoring tools will be delivered to the JFK Special Warfare Center and School.

Selected Current Projects

Modeling Information Propagation (MIMEO)

Military Information Support Operations (MISO) practitioners require the ability to understand how information moves through a population to a specific target audience, as well as the possible range of effects on their attitudes, beliefs, and actions. This mission, part of the doctrinally defined MISO process, requires operators to reason about the social dynamics and information flow relevant to their situation. Although computational models can be used to understand these sociocultural dynamics, most operators have little or no formal training in social science, and most computational models are too complicated to be used effectively by nonsocial or noncomputational scientists.

Charles River Analytics is developing a tool—MIMEO—intended to support MISO operator tasks related to planning, media analysis, and

Human Social Culture Behavior Modeling Program

media selection. MIMEO is being designed as an operationally friendly tool that enables operators to apply computational HSCB models embodying broadly applicable social science theories addressing social dynamics and information propagation to a representation of their own situation. These include important issues, groups, arguments, and media channels, to augment their own reasoning while addressing specific challenges within the MISO process. These models are made accessible within MIMEO through purpose-built visualizations that illustrate their underlying logic and their outcome in a manner suited to nonexpert users, allowing operators to establish an appropriate level of trust in their results. Elements of MIMEO's capabilities have already been introduced to the MISO community as part of the PSYOP Planning Suite, an accredited tool developed by Charles River Analytics in collaboration with PM-MISO, CTTSO, and other government sponsors that is currently in use by MISO practitioners. Prototypes of MIMEO are currently undergoing iterative assessment and refinement in anticipation of its full inclusion into the PSYOP Planning Suite in the future.

Ethnic Conflict, Repression, Insurgency, and Social Strife

U.S. engagement around the world involving ethnic conflict, genocide and other humanitarian challenges raises a number of key challenges for military and civilian planners and raises the following key questions: What are the drivers of conflict and social strife? Which actions can be used to mitigate problems? What are the immediate and second- and third-order effects U.S. actions may have in conflict situations? To address these questions, NSI is developing the Ethnic Conflict, Repression, Insurgency and Social Strife (ERIS) system, a multi-paradigm model of ethnic conflict at multiple levels of analysis and implementation. ERIS aims to model the complexity of micro- and macro-level interactions within a society and provide insight into the range of possible social outcomes given varying sets of initial conditions. Social science theories such as relative deprivation, social capital and electoral incentives, among others, inform the system design.

ERIS is built upon flexible theoretical drivers that draw together methods and ideas from empirical social science and computer science so that the project can scale, generalize and apply to a variety of contexts. ERIS will enable military planners to anticipate the emergence of ethnic conflict and its negative consequences, develop courses of action to defuse ethnic conflict, and control the second- and third-order effects of U.S. actions on ethnic conflict. NSI has successfully developed an initial proof of concept model of ethnic conflict integrating agent-based and system dynamics methodologies. NSI is currently refining and extending the existing ethnic conflict model with a focus toward the direct and indirect effects of information actions on multiple groups within a population.

Contact Information

hscb@hscb.cttso.gov

Photo courtesy of TF Lafayette, French Armed Forces supporting ISAF operations in Afghanistan, March 2010

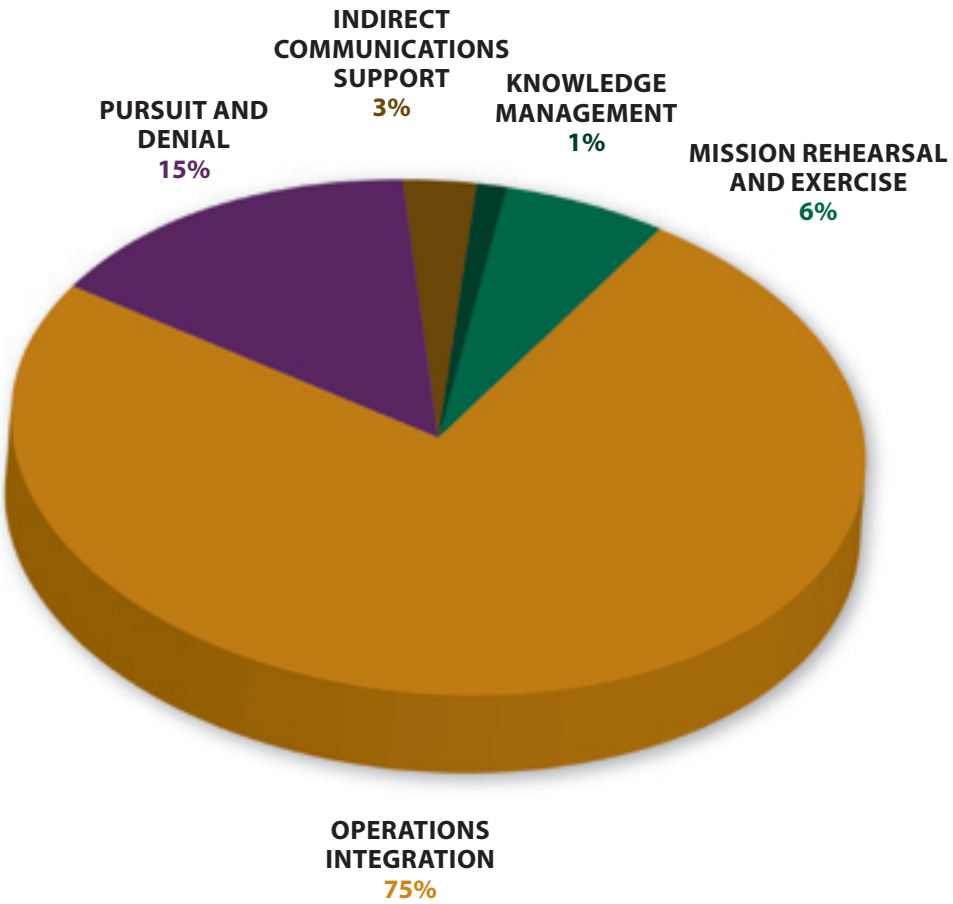
Irregular Warfare Support

Irregular Warfare Support

Mission

The Irregular Warfare Support (IWS) program develops adaptive and agile ways and means to support irregular warfare in current and evolving strategic environments. IWS supports joint, interagency, and international partners who conduct irregular warfare through indirect and asymmetric approaches with solutions to erode an adversary's power, influence, and will. IWS identifies material and nonmaterial solutions via operational analysis, concept development, field experimentation, and spiral delivery of capabilities to defeat the motivations, sanctuaries, and enterprises of targeted state and non-state actors.

IWS FY 2010 Funding by Focus Area ($16 Million)



Irregular Warfare Support

Focus Areas

IWS develops interagency capabilities and capacities for information age irregular warfare. During FY 2010, these focus areas were:

Building Partner Capacity

Conduct research, operational analysis, capability design, and implementation support in order to enable the Department of Defense to assist, train, advise, and influence foreign partners, foreign competitors, adversary leaders, military forces, and relevant populations by developing and presenting information and conducting shaping activities to affect their perceptions, will, behavior, and/or capabilities. This includes research and development that supports the conduct of communication, shaping missions, and activities, but does not include kinetic operations or maneuver of forces for the purpose of influence.

Photo courtesy of New Century Consulting

Pursuit and Denial

Conduct research, operational analysis, capability design, and implementation support to enable client organizations to better apply indirect and asymmetric force to identify, disrupt, deny, and destroy hostile organizations and their supporting enterprises.

Indirect Communications Support

Conduct research, operational analysis, capability design, and implementation support within the scope of traditional military information operations to enhance and improve client organization efforts to erode adversaries' power, influence, and will through proactive and responsive informational, psychological, and other irregular operations. IWS seeks to increase the efficacy of military information operations while decreasing the likelihood of direct action environments.

Photo courtesy of TF Lafayette (French Armed Forces Task Force in RC-E)

Mission Rehearsal and Exercise

Conduct research, operational analysis, capability design, and implementation support to increase U.S. proficiency in and capacity to wage irregular warfare on target states and non-state actors. IWS seeks to further the art and science of irregular warfare operations and their understanding in the appropriate agencies, forces, and bodies of government.

Knowledge Management

Conduct research, operational analysis, capability design, and spiral experimentation support to increase U.S. and appropriate partners' understanding of hostile forces, current and evolving tactical and operational environments, and opportunities for successful irregular warfare operations by client organizations.

Photo courtesy of the COIN Advisory & Assistance Team (CAAT), Project ARCHER

Irregular Warfare Support

Photo courtesy of LTC Albert Magon, FRA-A, CAAT Deputy Commander

Photo courtesy of John Tyman, Cultures in Context

Operations Integration

Conduct research, operational analysis, capability design, and implementation support to synchronize interagency irregular warfare efforts. IWS refines current capabilities and develops those capabilities necessary for friendly forces to prevent and prevail in future conflicts.

COIN Aviation Capability

Conduct research, operational analysis, capability design, and implementation support to provide low cost counterinsurgency (COIN) aviation mission requirements for small units engaged in distributed operations, and in austere and remote locations. This would be used by Special Operations Forces (SOF), General Purpose Forces (GPF), and their enablers to execute various missions to include building partner capacity, security force assistance, and irregular warfare.

Program Highlights

IWS programs are classified or sensitive. Program requirements, the success of programs, and specific program capabilities cannot be discussed in an unclassified document.

Contact Information

iws@iwsp.cttso.gov

DoD photo by Mass Communication Specialist 3rd Class Omar A. Dominquez, U.S. Navy/Released

Product Development and Delivery

Technology Transition

The TSWG charter identifies technology transition assistance throughout the development cycle as essential to supporting national combating terrorism objectives. CTTSO has formalized the technology transition process into every aspect of its R&D programs. CTTSO requires that every proposal received address technology transition as a principal task and that each new project include a technology transition plan. A dedicated technology transition manager works with CTTSO developers to prepare the plans and to address the issues associated with a successful transition to production, such as:

- Exploration of all applications and markets for the technology;
- Understanding and managing intellectual property (patents, trademarks, copyrights, trade secrets, and licensing; to include data and software rights and options);
- Market evaluations for military, federal, state, local, and commercial users;
- Environmental, safety, and health issues;
- Liability risk reduction and consideration of SAFETY Act Applications;
- Security and Export Control provisions;
- Regulatory restrictions to include electronic emissions, environmental, safety, health, transportation, and others;
- Test and evaluation planning and independent operational testing by users;
- Transition to production, including partnering, investment capital, licensing, and finding markets and distributors; and
- Operational suitability and operational support planning.

A number of technology transition tools and methodologies are used to assist the developer with resolving issues and reaching user markets, such as:

- Commercialization assessments and transition plan formats;
- Publication of handbooks and special primers;
- Non-disclosure agreements;
- Provisional patents versus full patents;
- Liability risk reduction techniques;
- Tailored license application forms and licensee/partner selection board assistance;
- Technical data and software package rights and management techniques;
- Federal Business Opportunity announcements;
- Licenses and Cooperative Research and Development Agreements (CRADAs);
- Implications of the Buy American Act on production;
- Export Control processing assistance;
- Technology briefs, articles, and outreach plans to reach large user groups;
- Interface with professional associations, user publications, and other media to provide product visibility; and
- Assistance with linkages to DHS Federal Grant funding for responder related technology.

Technology Transition

The keys to accelerating the complicated process of moving many prototypes to production includes having a disciplined process, available assistance, and teamwork among the project manager, technology transition manager, and developer. Additional information is available at the Technology Transition section of the CTTSO Web site, http://www.cttso.gov.

2010 Meetings and Conferences

January

Advanced Planning Briefing for Industry

On January 26, the Advanced Planning Briefing for Industry (APBI), sponsored by CTTSO, provided representatives of industry, government, entrepreneurs, and associated developers with a preview of the requirements identified in the annual CTTSO Broad Agency Announcements. This year 570 registrants attended the APBI, which was held in the Ronald Reagan Building and International Trade Center in Washington, D.C. CTTSO and EOD/LIC program representatives presented 46 requirements published in March 2010.

February

U.S. Army photo by Spc. Eric Cabral/Released

Waterside Security Working Group

The Physical Security Subgroup hosted the third Waterside Security Working Group on February 2. Government and industry participants with expertise in the field of waterside and port security attended the meeting. CTTSO, the Joint Non-Lethal Weapons Directorate, the Naval Criminal Investigative Service, and the Naval Research Laboratory presented technologies and capabilities currently available or under development to address waterside and port security concerns. Companies presented their technologies and capabilities that may assist the government in enhancing the nation's waterside security capabilities. The main theme of the meeting was new technologies and underwater explosive threats.

Blast Community Forum

The Physical Security Subgroup hosted the Blast Community Forum on February 3 in Washington, D.C. The event was held to re-engage stakeholders across the U.S. government interested in blast testing and to provide a venue for the coordination of blast testing efforts being undertaken. The event was successful in raising the awareness of ongoing programs, thereby providing the crucial benefit of leveraging complimentary efforts, curtailing redundancies, and collaborating on future requirements.

March

Homemade Explosives Working Group

The Physical Security Subgroup hosted a Homemade Explosives (HME) Working Group meeting on March 10 in McLean, Virginia. More than 90 participants, including Defense Research and Development Canada and Natural Resources Canada, attended. The meeting focused on the various HME training courses provided by, and available to, military EOD, general purpose forces, and state/local bomb squads. Government agencies and commercial vendors presented training overview briefings. The meeting

2010 Meetings and Conferences

concluded with a panel discussion about training standardization, requirements, gaps, and policy.

Counter-Tunnel Operations Working Group

The Physical Security Subgroup hosted the Counter-Tunnel Operations Working Group on March 24-25. More than 40 attendees participated, representing approximately 18 U.S. government agencies and organizations. The event accomplished four primary functions: (1) to convene a forum of stakeholders from across the U.S. government interested in subterranean operations; (2) to update the operational/threat picture as it exists on the ground; (3) to update programmatic events aimed at assisting the operators; and (4) to capture new or emerging requirements. The event succeeded in promoting interagency collaboration and ensured the most up-to-date operational and programmatic developments were understood by all. Several operational requirements were identified from the Special Response Team, which is Immigration and Customs Enforcement's special weapons and tactics equivalent.

May

Evaluating LEGACY Conference

The Irregular Warfare Support Program sponsored a one-day conference and workshop on May 19 on a unique police and military intelligence capacity building program, known as LEGACY. More than 60 participants from throughout the U.S. government and academia attended. The purpose of the day was to consider the results of two unique pilot programs that sought to demonstrate police-based intelligence capacity development in counterinsurgency (COIN) operations. Participants and researchers from the Rand Corporation considered LEGACY's applicability in other COIN environments; its applicability against other armed groups (terrorists, narcotics, and organized crime); obstacles and issues to success; and the metrics and measures used to evaluate the program's effectiveness.

Homemade Explosives International Workshop

The Physical Security Subgroup hosted the Homemade Explosives (HME) International Workshop, which was attended by more than 150 participants, on May 25-27. The meeting opened with recent events and threat perspectives from the intelligence community and operators from the U.S., the United Kingdom, Canada, Israel, Australia, and Singapore. Following discussions included ongoing projects and current scientific research conducted to support the understanding of HME and aide in the development of necessary tools to defeat the threat. The meeting concluded with three break-out sessions on explosive equivalence, illicit laboratory detection and HME training needs. Overall interest in HME is significant, and working group membership consists of almost

2010 Meetings and Conferences

400 individuals from six countries and includes federal, state, and local bomb technicians and ordnance disposal, national laboratories, and U.S. federal departments including the Department of Homeland Security, the Department of Justice, and the Department of Transportation.

August

Counter-Tunnel Operations Working Group

The Physical Security Subgroup hosted the Counter-Tunnel Operations Working Group October 6-7 in San Diego, California. The meeting also included a trip to the U.S.-Mexico border to see the operational environment firsthand.

Tunnel/Border Technology Objective Demonstration

The Physical Security Subgroup hosted the Tunnel/Border Technology Objective Demonstration (TOD) on August 10-12 in Socorro, New Mexico. The purpose of the TOD event was to demonstrate technologies of interest to the counter-tunnel/border user community. This event included demonstrations of robotic platforms; perimeter intrusion detection and surveillance capabilities; and subsurface mapping, tracking, voice communication, and video capabilities.

Waterside Security Working Group

The Physical Security Subgroup hosted the Waterside Security Working Group on August 31 in Washington, D.C. The main theme of this meeting, attended by government and industry participants with expertise in the field of waterside and port security, was lethal and non-lethal interdiction of divers and swimmers.

September

Crime Wars: Gangs, Cartels, and U.S. National Security

On September 30 the Center for a New American Security held an event to launch "Crime Wars: Gangs, Cartels, and U.S. National Security," a report that surveyed organized crime throughout the Western Hemisphere, analyzed the challenges it poses for the region, and made recommendations for how the United States could better confront the interrelated challenges of drug trafficking and violence ranging from the Andean Ridge to American streets. The Irregular Warfare Support Program sponsored both the report and the event, which convened a diverse panel of experts who discussed this multi-layered national security challenge and answered questions from the community of interest about the report's findings and recommendations.

2010 Meetings and Conferences

October

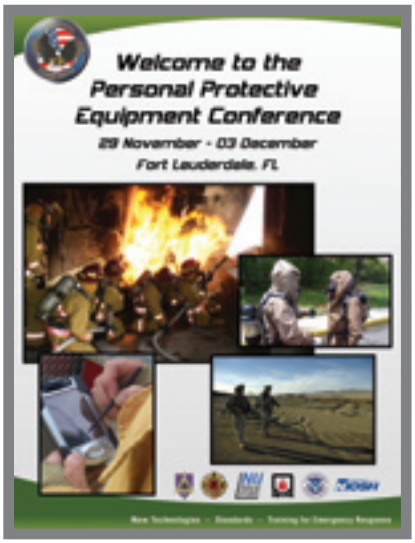
Vehicle Barrier International Working Group

The Physical Security Subgroup hosted the Vehicle Barrier International Working Group meeting on October 14 in Washington, D.C. The purpose of the working group meeting was to convene U.S. government stakeholders and their international counterparts from the United Kingdom and Canada to discuss ongoing research programs, best practices, and a path forward for future collaboration.

Homemade Explosives Working Group

The Physical Security Subgroup hosted a Homemade Explosives Working Group meeting on October 27 in Washington, D.C. The meeting focused on explosive equivalency solutions to better understand the HME threat on various types of U.S. targets.

November



Personal Protective Equipment Conference

The CBRNC Subgroup hosted its second Personal Protective Equipment (PPE) Conference, PPE 2010, in November/December. PPE 2010 was co-sponsored by the Department of Homeland Security, the National Institute of Occupational Safety and Health, the National Institute of Justice, the National Fire Protection Association, and the International Association of Fire Fighters. PPE 2010 provided TSWG and its partners with a forum to highlight emerging technologies in the area of PPE. The conference included briefings of new technologies and an exhibition of new and emerging equipment from PPE vendors. Allies present included Australia, Canada, the Czech Republic, Israel, Japan, the Netherlands, the United Kingdom, Singapore, and others. Deliverables from the event included the identification of gaps to drive future research directions.

December 2010

Bio-Threat Conference

The CBRNC Subgroup co-sponsored the 4th National Bio-Threat Conference with the Department of Defense's Joint Program Executive Office for Chemical and Biological Defense, Chemical Biological Medical Systems, Joint Project Manager Guardian; the Department of Homeland Security; and the Environmental Protection Agency in December. This conference provided TSWG and its partners with a forum for dialogue between government, industry, academia, and first responders to address critical issues in environmental sampling and bio-detection as well as

2010 Meetings and Conferences

special focus on biosurveillance and microbial forensics. The conference included presentations, discussions, and exhibits of new technologies, protocols, and procedures from federal, state, and local agencies, vendors, and commercial entities. The sessions and networking opportunities informed key personnel of the state of sampling and detection and will drive future research and development activities.

BAA Information Delivery System (BIDS)

The Broad Agency Announcement (BAA) Information Delivery System, better known as BIDS, works to support the CTTSO mission through the electronic publication of its annual BAAs. BAAs are the solicitation method of choice to bring the most urgent combating terrorism requirements forward for publication. CTTSO staff monitors BAA package instruction in light of submitter responses and feedback, and CTTSO implements improvements as needed each year to clarify the submission process.

To ensure the widest possible distribution to potential submitters, BAAs can be downloaded at the BIDS Web site (http://www. Bids.tswg.gov) and are also advertised at the Federal Business Opportunities Web site (http://www. fedbizopps.gov). In addition to conventional government solicitation notices, the BIDS Web site provides a BIDS Advisory and Announcement area that posts BAA news, coming events, and partnering agency solicitations. In addition to the advisory, the RSS (really simple syndication) news feed allows interested users to receive real-time broadcast information at a local computer when connected to the Internet.

BIDS is a rich source of submitter information, providing small business outreach, online training, and guidance for offerers proposing the use of human subjects in research. Overall BAA statistics are posted once the BAA closes.

BIDS not only functions as a response collection system, but also provides for submission evaluation and submitter notification. Submitter data is fully protected in a 128-bit encrypted environment. Evaluators must comply with source selection data handling requirements and accept a nondisclosure agreement to access BIDS. In addition to the nondisclosure, evaluators must also certify that there is no conflict of interest before access is granted to any submissions. The evaluation process is monitored for timely notice to submitters with the typical response via an automated e-notice complete within 90 days.

BIDS continues to serve as a leading solicitation process model for other federal programs by providing a streamlined electronic solution to receive proposals, providing access for subject matter expert evaluation, processing submissions through the approving authority, notifying the submitter of status, and maintaining a record of solicitation results.

CTTSO Portal Web Site — *www.cttso.gov*

The CTTSO portal Web page (www.cttso.gov) works to centralize comprehensive program resources while maintaining the individual technical expertise of each sector.

Featured program elements to date include the Technical Support Working Group, Explosive Ordnance Disposal/Low-Intensity Conflict, and the Irregular Warfare Support program. Each program maintains its own Web site and is easily accessed through the portal. The TSWG site also includes a focus on the transition of products available to end users.

Portal visitors can freely navigate several information pages to learn about the CTTSO or review business opportunities for product commercialization. Helping small businesses and nontraditional defense contractors to find opportunities and do business with the government is one of several information focuses. A Technology Transition page is provided for CTTSO contract awardees to help in the transition to production or commercialization of products. Links to BIDS and other government sites such as NATO and the Terrorism Research Center are also available. The Contract Award page details information on current performers, recent contract awards, and BAA statistical data.

CTTSO Forums, an access-controlled site for data sharing among mission area participants, is linked from the portal.

Photo by U.S. Army Spc. William Hatton

Appendix

2010 Membership

Federal Agencies

U.S. Department of Agriculture

- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service
- Forest Service

U.S. Department of Commerce

- National Institute of Standards and Technology
- Office of Law Enforcement Standards

U.S. Department of Defense

- Armed Forces Institute of Pathology
- Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense; Acquisition, Technology and Logistics
- Counterintelligence Field Agency
- Defense Academy for Credibility Assessment
- Defense Advanced Research Projects Agency
- Defense Computer Forensics Laboratory
- Defense Criminal Investigative Service
- Defense Finance and Accounting Service
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Explosives Safety Board
- Joint Chiefs of Staff
- Joint Forces Staff College
- Joint Improvised Explosive Device Defeat Organization
- Joint Personnel Recovery Agency
- Joint Program Executive Office for Chemical and Biological Defense
- Joint Task Force North (NORTHCOM)
- Joint Warfare Analysis Center (JFCOM)
- National Geospatial-Intelligence Agency
- National Reconnaissance Office
- National Security Agency
- Office of the Provost Marshal General
- Offices of the Secretary of Defense
- Pentagon Force Protection Agency
- Physical Security Equipment Action Group
- Rapid Reaction Technology Office
- Special Operations Command
- Unified Combatant Commands

U.S. Air Force

- Air Combat Command
- Engineering and Services Center
- Office of Special Investigations
- Research Laboratory

2010 Membership

U.S. Army

- 20th Support Command – Chemical, Biological, Radiological, Nuclear and high-yield Explosives (CBRNE)
- 22nd Chemical Battalion
- 52nd Ordnance Group
- Armaments Research, Development and Engineering Center
- Asymmetric Warfare Group
- Chemical School
- Chemical School, Maneuver Support Center
- Communications-Electronics Research, Development and Engineering Center
- Corps of Engineers
- Criminal Investigation Command
- Criminal Investigation Laboratory
- Edgewood Chemical Biological Center
- Explosive Ordnance Disposal Detachment
- Intelligence and Security Command
- John F. Kennedy Special Warfare Center and School
- Medical Department
- Medical Research and Material Command
- Joint Trauma Analysis and Prevention of Injury in Combat
- National Ground Intelligence Center
- National Guard Bureau
- Office of the Provost Marshal General
- Product Manager-Force Protection Systems
- Product Manager-Guardian
- Program Executive Office Soldier Protective Equipment
- Rapid Equipping Force
- Research, Development and Engineering Command
- Research, Development and Engineering Command Simulation and Training Technology Center
- Research Laboratory
- Soldier Systems Center (Natick)
- Special Forces Command
- Special Operations Command
- Training and Doctrine Command
- War College

U.S. Marine Corps

- Central Command
- Chemical, Biological Incident Response Force
- Criminal Investigation Division
- Explosive Ordnance Disposal Detachment
- Special Operations Command
- Systems Command
- Training and Education Command
- U.S. Marine Corps Forces-Pacific
- Warfighting Laboratory

2010 Membership

U.S. Navy

- Bureau of Medicine
- Chief of Naval Operations
- Commander Navy Installations Command
- Criminal Investigative Service
- Expeditionary Combat Command
- Explosive Ordnance Disposal Detachment 63
- Explosive Ordnance Disposal Fleet Liaison Office
- Explosive Ordnance Disposal Technology Division
- Facilities Engineering Command
- Naval Air Systems Command
- Naval Air Warfare Center
- Naval Criminal Investigative Service
- Naval Forces Central Command
- Naval Research Laboratory
- Naval Sea Systems Command
- Naval Surface Warfare Center
- Office of Naval Research
- Program Executive Office, Ships
- Strategic Systems Program

U.S. Department of Energy

- Lawrence Livermore National Laboratory
- National Nuclear Security Administration
- Office of Health, Safety and Security

U.S. Department of Health and Human Services

- Centers for Disease Control and Prevention
- Food and Drug Administration
- National Institute for Occupational Safety and Health
- Office of Inspector General

U.S. Department of Homeland Security

- Border and Transportation Security Directorate
- Coast Guard
- Customs and Border Protection
- Federal Air Marshal Service
- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Federal Protective Service
- Forensic Document Laboratory
- Homeland Security Advanced Research Project Agency
- Immigration and Customs Enforcement
- Information Analysis and Infrastructure Protection Directorate
- Office for Domestic Preparedness
- Office of Bombing Prevention
- Science and Technology Directorate
- Secret Service

2010 Membership

- Transportation Security Administration
- Transportation Security Laboratory
- Urban Search and Rescue

U.S. Department of the Interior
- Bureau of Reclamation

U.S. Department of Justice
- Ballistic Research Facility
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Counterterrorism Office
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Federal Bureau of Investigation – Hostage Rescue Team
- Federal Bureau of Prisons
- Marshals Service
- National Center for Forensic Science
- National Forensic Science Technology Center
- National Institute of Justice

U.S. Department of State
- Bureau of Diplomatic Security
- Office of the Coordinator of Counterterrorism

U.S. Department of Transportation
- Federal Aviation Administration
- Research and Innovative Technology Administration (Volpe Center)

U.S. Department of the Treasury
- Internal Revenue Service
- Office of the Inspector General

U.S. Department of Veterans Affairs

U.S. Environmental Protection Agency
- National Enforcement Investigations Center

U.S. Postal Inspection Service

State and Local Agencies
- Arlington County (VA) Fire Department
- Bloomington Minnesota Police Department (Central Region)
- DC Metropolitan Police
- Fairfax County (VA) Fire and Rescue Department
- Fairfax County (VA) Police Department
- Fire Department, City of New York
- Georgia Bureau of Investigation (Southern Region)
- Houston Texas Police Department (Western Region)

2010 Membership

- Jacksonville Port Authority
- Long Beach (CA) Police Department
- Los Angeles County (CA) Sheriff's Department
- Lynchburg Sheriff's Office
- Maryland State Police
- Michigan State Police
- Morris County Sheriff's Office (Eastern Region)
- New York City Police Department
- NYC Office of Chief Medical Examiner
- Pentagon Force Protection Agency Bomb Squad (VA)
- Pinellas County Sheriff's Office
- Port Authority of New York & New Jersey
- Protective Services Police Department
- Seattle (WA) Fire Department
- State and local SWAT teams
- South Pasadena (CA) Police Department
- U.S. Capitol Police
- U.S. Supreme Court Police

Federal Reserve Board

Intelligence Community

InterAgency Board

National Aeronautics and Space Administration

National Bomb Squad Commanders Advisory Board

National Tactical Officers Association

National Transportation Safety Board

U.S. Senate Sergeant at Arms

White House

- Homeland Security Council
- Office of Science and Technology Policy

TSWG 2010 Membership by Subgroup

Chemical, Biological, Radiological, and Nuclear Countermeasures

Environmental Protection Agency
Federal Reserve Board
Intelligence Community
InterAgency Board
    State and Local Agencies:
    - Arlington County (VA) Fire Department
    - Fairfax County (VA) Fire and Rescue Department
    - Fire Department, City of New York
    - New York City Police Department
    - NYC Office of Chief Medical Examiner
    - Seattle (WA) Fire Department

U.S. Department of Agriculture
    - Animal and Plant Health Inspection Service
    - Food Safety and Inspection Service

U.S. Capitol Police
U.S. Department of Commerce
    - National Institute of Standards and Technology

U.S. Department of Defense
    - Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense; Acquisition, Technology and Logistics
    - Defense Intelligence Agency
    - Defense Threat Reduction Agency
    - Joint Chiefs of Staff
    - Joint Improvised Explosive Device Defeat Organization
    - Joint Program Executive Office for Chemical and Biological Defense
    - National Security Agency
    - Pentagon Force Protection Agency
    - Special Operations Command
    - U.S. Air Force Air Combat Command
    - U.S. Army 20th Support Command – Chemical, Biological, Radiological, Nuclear, and high yield Explosives (CBRNE)
    - U.S. Army 22nd Chemical Battalion
    - U.S. Army Chemical School, Maneuver Support Center
    - U.S. Army Medical Department
    - U.S. Army National Ground Intelligence Center
    - U.S. Army Research, Development, and Engineering Command – Edgewood Chemical Biological Center
    - U.S. Marine Corps Chemical, Biological Incident Response Force
    - U.S. Marine Corps Systems Command
    - U.S. Navy Bureau of Medicine
    - U.S. Navy Naval Air Warfare Center
    - U.S. Navy Naval Forces Central Command
    - U.S. Navy Naval Surface Warfare Center

U.S. Department of Energy
    - Office of Health, Safety and Security

TSWG 2010 Membership by Subgroup

- National Nuclear Security Administration

U.S. Department of Health and Human Services
- Centers for Disease Control and Prevention
- Food and Drug Administration
- National Institute for Occupational Safety and Health

U.S. Department of Homeland Security
- Federal Emergency Management Agency
- Federal Protective Service
- Science and Technology Directorate
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

U.S. Department of Justice
- Federal Bureau of Investigation
- National Institute of Justice
- U.S. Marshals

U.S. Department of State
- Bureau of Diplomatic Security
- Bureau of Overseas Buildings Operations
- Counterterrorism Office

U.S. Department of Transportation
- Research and Innovative Technology Administration (Volpe Center)

U.S. Senate Sergeant at Arms

White House
- Homeland Security Council
- Office of Science and Technology Policy

Explosives Detection

U.S. Department of Commerce
- National Institute of Standards and Technology

U.S. Department of Defense
- Defense Intelligence Agency
- Joint Improvised Explosive Device Defeat Organization
- Pentagon Force Protection Agency
- U.S. Air Force Engineering and Services Center
- U.S. Air Force Research Lab
- U.S. Army Edgewood Chemical Biological Center
- U.S. Marine Corps Explosive Ordnance Disposal
- U.S. Navy Naval Explosive Ordnance Disposal Technology Division
- U.S. Navy Naval Research Laboratory

U.S. Department of Homeland Security
- Science and Technology Directorate
- Transportation Security Administration
- Transportation Security Laboratory
- U.S. Coast Guard
- U.S. Secret Service

TSWG 2010 Membership by Subgroup

U.S. Department of Justice
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Federal Bureau of Investigation

U.S. Department of State
- Bureau of Diplomatic Security

Improvised Device Defeat

Intelligence Community
National Bomb Squad Commanders Advisory Board
State and Local Agencies:
- Fairfax County (VA) Police Department
- Pentagon Force Protection Agency Bomb Squad (VA)
- Maryland State Police
- Michigan State Police
- Bloomington, Minnesota Police Department (Central region)
- Houston, Texas Police Department (Western region)
- Morris County Sheriff's Office (Eastern region)
- Georgia Bureau of Investigation (Southern region)

U.S. Capitol Police
U.S. Department of Defense
- U.S. Air Force Air Combat Command
- U.S. Army 52nd Ordnance Group
- U.S. Army Explosive Ordnance Disposal Technical Detachment
- U.S. Marine Corps Chemical Biological Incident Response Force
- U.S. Marine Corps Explosive Ordnance Disposal Detachment
- U.S. Navy Explosive Ordnance Disposal Detachment 63
- U.S. Navy Explosive Ordnance Disposal Fleet Liaison Office
- U.S. Navy Explosive Ordnance Disposal Technology Division

U.S. Department of Homeland Security
- Border and Transportation Security Directorate
- Homeland Security Advanced Research Project Agency
- Information Analysis and Infrastructure Protection Directorate
- Office for Domestic Preparedness
- Science and Technology Directorate
- Secret Service
- Transportation Security Administration

U.S. Department of Justice
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Federal Bureau of Investigation
- Marshals Service
- National Institute of Justice

Investigative Support and Forensics

Environmental Protection Agency
- National Enforcement Investigations Center

National Aeronautics and Space Administration

TSWG 2010 Membership by Subgroup

Federal Reserve Board
Intelligence Community
National Transportation Safety Board
U.S. Capitol Police
U.S. Department of Commerce
- National Institute of Standards and Technology

U.S. Department of Defense
- Armed Forces Institute of Pathology
- Counterintelligence Field Activity
- Defense Academy for Credibility Assessment
- Defense Computer Forensics Laboratory
- Defense Criminal Investigative Service
- Defense Finance and Accounting Service
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- National Geospatial-Intelligence Agency
- Office of the Provost Marshal General
- Pentagon Force Protection Agency
- U.S. Air Force Office of Special Investigations
- U.S. Army Communications-Electronics Research, Development and Engineering Center
- U.S. Army Criminal Investigation Command
- U.S. Army Criminal Investigation Laboratory
- U.S. Army Intelligence and Security Command
- U.S. Marine Corps Criminal Investigation Division
- U.S. Marine Corps Forces-Pacific
- U.S. Navy Naval Criminal Investigative Service
- U.S. Special Operations Command

U.S. Department of Energy
- Office of Health, Safety, and Security

U.S. Department of Health and Human Services
- Office of Inspector General

U.S. Department of Homeland Security
- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Federal Protective Service
- Forensic Document Laboratory
- Immigration and Customs Enforcement
- Science and Technology Directorate
- Secret Service
- Transportation Security Administration
- Transportation Security Laboratory

U.S. Department of Justice
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Marshals Service
- National Center for Forensic Science
- National Forensic Science Technology Center

TSWG 2010 Membership by Subgroup

- National Institute of Justice

U.S. Department of State
- Office of the Coordinator for Counterterrorism

U.S. Department of Transportation
- Federal Aviation Administration

U.S. Department of the Treasury
- Internal Revenue Service
- Office of the Inspector General

U.S. Postal Inspection Service

U.S. Department of Veterans Affairs

State and Local Agencies
- Long Beach Police Department
- Los Angeles County Sheriff's Department
- Michigan State Police
- South Pasadena Police Department

Personnel Protection

Intelligence Community

U.S. Capitol Police

U.S. Department of Commerce
- National Institute of Standards and Technology
- Office of Law Enforcement Standards

U.S. Department of Defense
- Defense Threat Reduction Agency
- Joint Improvised Explosive Device Defeat Organization
- Joint Personnel Recovery Agency
- Pentagon Force Protection Agency
- Rapid Reaction Technology Office
- U.S. Air Force Office of Special Investigations
- U.S. Army
- U.S. Army Criminal Investigation Command
- U.S. Army Joint Trauma Analysis and Prevention of Injury in Combat
- U.S. Army Medical Research and Material Command
- U.S. Army Program Executive Office Soldier Protective Equipment
- U.S. Army Research, Development and Engineering Command
- U.S. Army Research Laboratory
- U.S. Army Soldier Systems Center (Natick)
- U.S. Army Special Operations Command
- U.S. Navy Naval Air Systems Command
- U.S. Navy Naval Criminal Investigative Service
- U.S. Navy Program Executive Office Ships

U.S. Department of Energy

U.S. Department of Homeland Security
- Federal Air Marshal Service
- Transportation Security Administration
- U.S. Secret Service, Special Services Division, Technical Security Division

U.S. Department of Justice

TSWG 2010 Membership by Subgroup

- Marshals Service
- National Institute of Justice

U.S. Department of State
U.S. Protective Services Police Department
U.S. Supreme Court Police

Physical Security

Environmental Protection Agency
Federal Reserve Board
Intelligence Community
State and Local Agencies

- DC Metropolitan Police
- Jacksonville Port Authority
- Lynchburg Sheriff's Office
- New York Police Department
- Pinellas County Sheriff's Office
- Port Authority of New York & New Jersey
- Protective Services Police Department
- U.S. Capitol Police

U.S. Department of Agriculture

- Forest Service

U.S. Department of Commerce

- National Institute of Standards and Technology

U.S. Department of Defense

- Defense Advanced Research Projects Agency
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Explosives Safety Board
- Joint Chiefs of Staff
- Joint Improvised Explosive Device Defeat Organization
- Joint Task Force North (NORTHCOM)
- Joint Warfare Analysis Center (JFCOM)
- National Reconnaissance Office
- Offices of the Secretary of Defense
- Physical Security Equipment Action Group
- Unified Combatant Commands
- U.S. Air Force Research Laboratory
- U.S. Army Armaments Research, Development and Engineering Center
- U.S. Army Asymmetric Warfare Group
- U.S. Army Chemical School
- U.S. Army Corps of Engineers
- U.S. Army Maneuver and Support Center
- U.S. Army Office of the Provost Marshal General
- U.S. Army Product Manager-Force Protection Systems
- U.S. Army Product Manager-Guardian
- U.S. Army Rapid Equipping Force
- U.S. Army Research, Development and Engineering Command
- U.S. Army Research Laboratory

TSWG 2010 Membership by Subgroup

- U.S. Army Special Forces Command
- U.S. Army Special Operations Command
- U.S. Army Training and Doctrine Command
- U.S. Marine Corps Central Command
- U.S. Marine Corps Special Operations Command
- U.S. Marine Corps Systems Command
- U.S. Marine Corps Warfighting Laboratory
- U.S. Navy Chief of Naval Operations
- U.S. Navy Commander Navy Installations Command
- U.S. Navy Criminal Investigative Service
- U.S. Navy Expeditionary Combat Command
- U.S. Navy Explosive Ordnance Disposal Technology Division
- U.S. Naval Facilities Engineering Command
- U.S. Naval Facilities Engineering Service Center
- U.S. Navy Office of Naval Research
- U.S. Navy Sea Systems Command
- U.S. Navy Strategic Systems Programs
- U.S. Navy Surface Warfare Center

U.S. Department of Energy

- Lawrence Livermore National Laboratory
- National Nuclear Security Administration
- Nuclear Regulatory Commission

U.S. Department of Homeland Security

- Coast Guard
- Customs and Border Protection
- Immigration and Customs Enforcement
- Science and Technology Directorate
- Secret Service
- Transportation Security Administration
- Transportation Security Laboratory

U.S. Department of the Interior

- Bureau of Reclamation

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Federal Bureau of Prisons

U.S. Department of State

- Bureau of Diplomatic Security

U.S. Department of Transportation

Tactical Operations Support

National Tactical Officers Association

State and Local SWAT Teams

U.S. Department of Defense

- Defense Threat Reduction Agency
- U.S. Army
- U.S. Marine Corps

TSWG 2010 Membership by Subgroup

- U.S. Navy
- U.S. Special Operations Command

U.S. Department of Energy
- National Nuclear Security Administration
- Office of Health, Safety and Security

U.S. Department of Homeland Security
- Urban Search and Rescue
- U.S. Border Patrol
- U.S. Coast Guard
- U.S. Immigration and Customs Enforcement
- U.S. Secret Service

U.S. Department of Justice
- Ballistic Research Facility
- Federal Bureau of Investigation
- Hostage Rescue Team

Training Technology Development

Intelligence Community
InterAgency Board
National Bomb Squad Commanders Advisory Board
National Tactical Officers Association

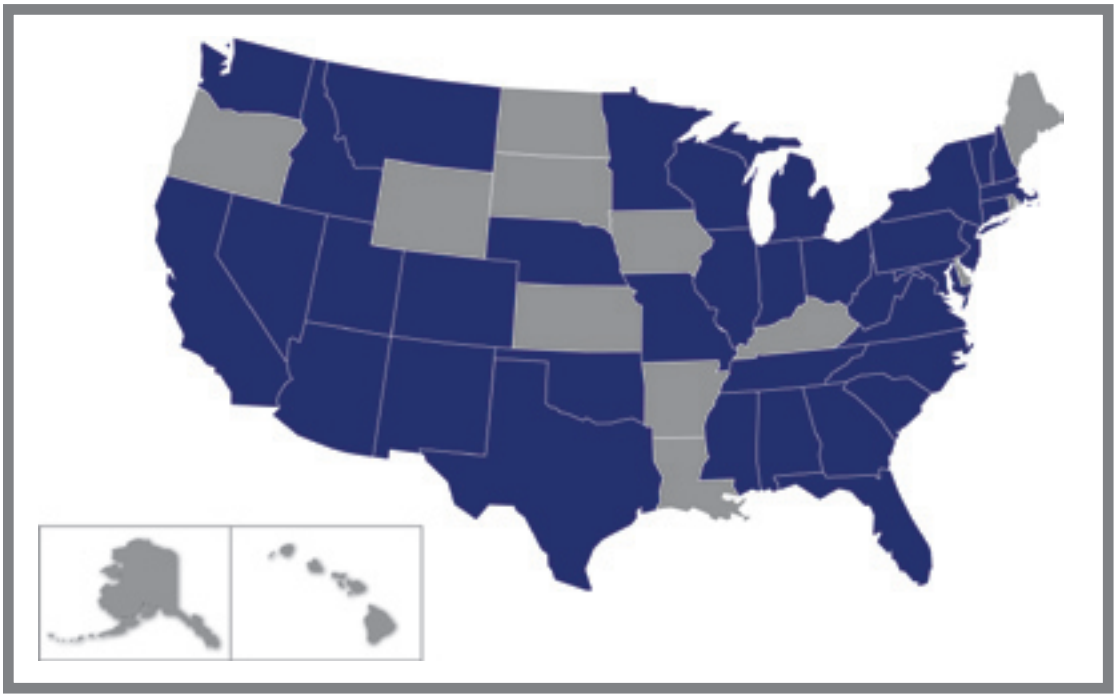
U.S. Department of Defense
- Joint Improvised Explosive Device Defeat Organization
- Office of the Undersecretary of Defense for Personnel and Readiness
- Pentagon Force Protection Agency
- U.S. Army John F. Kennedy Special Warfare Center and School
- U.S. Army National Guard Bureau
- U.S. Army Research, Development and Engineering Command Simulation and Training Technology Center
- U.S. Army Training and Doctrine Command
- U.S. Army War College
- U.S. Marine Corps
- U.S. Marine Training and Education Command
- U.S. Joint Forces Staff College
- U.S. Special Operations Command

U.S. Department of Energy
U.S. Department of Homeland Security
- Customs and Border Protection
- Office of Bombing Prevention
- Science and Technology Directorate
- Secret Service

U.S. Department of Justice
- National Institute of Justice

U.S. Department of State
- Bureau of Diplomatic Security

2010 Performers



Alabama

Auburn University, Auburn
Lewis Innovative Technologies, Inc., Moulton
U.S. Army AMRDEC, Redstone Arsenal

Arizona

Armorworks, Tempe
University of Arizona, Tucson

California

Cantimer, Inc., Menlo Park
GKN Aerospace Transparency, Garden Grove
Information Systems Laboratories, San Diego
Intelligent Optical Systems, Inc., Torrance
L-3 Communications, San Diego
Lawrence Berkeley National Laboratory, Berkeley
Lawrence Livermore National Laboratory, Livermore
Morpho Detection, San Diego
Naval Air Warfare Center, China Lake
Naval Facilities Engineering Service Center, Port Hueneme
Naval Health Research Center, San Diego
Pacific Science and Engineering Group, Inc., San Diego
Perlegen Sciences, Inc., Mountain View
QPC Fiber Optic, Inc., San Clemente
Rapiscan Security Products, Inc., Hawthorne

2010 Performers

Rapiscan Systems, Hawthorne
Rapiscan Systems Neutronics and Advanced Technologies, Sunnyvale
Raymat Materials, Inc., Fremont
SAIC, San Diego
Smiths Detection, Pasadena
Spectrum San Diego, San Diego
SRI International, Menlo Park
Tactical Survey Group, San Bernardino
Torrey Pines Logic, Inc., San Diego
University of California, San Diego
University of Southern California, Marina del Rey
U.S. Marine Corps Logistics Base, Barstow

Colorado

Alion Science and Technology, Boulder
APTEK, Inc., Colorado Springs
Applied Research Associates, Littleton
Rocky Mountain Scientific Laboratories, Highlands Ranch
SET Corporation, an SAIC Company, Greenwood Village
Stratom, Inc., Boulder
Summa Design, LLC, Montrose

Connecticut

Clovis Point Solutions, LLC, Stamford
Nextgen Fiber Optics, LLC, Dayville
United Technologies Research Center, Hartford

District of Columbia

Bureau of Alcohol, Tobacco, Firearms and Explosives
Defense Intelligence Agency
Department of Homeland Security
Government Printing Office
International Association of Fire Fighters
Naval Research Laboratory
Naval Sea Systems Command

Florida

AMP Research, Inc., Naples
CTC Tampa Bay, Largo
Cubic Corporation Simulation Systems Division, Orlando
Engineering and Computer Simulations, Inc., Orlando
Florida International University, Miami
Florida State University, Tallahassee
General Dynamics-Ordnance and Tactical Systems, Orlando
Knights Armament Company, Titusville
Lightmaker Group, Ltd., Orlando
Naval Surface Warfare Center, Panama City
Perception IR Manufacturing, LLC, Palm Harbor

2010 Performers

Quantum Technology Sciences, Inc., Cocoa Beach
Studio 14b, Safety Harbor
University of Florida, Gainesville
U.S. Air Force Civil Engineer Support Agency, Tyndall Air Force Base
U.S. Air Force Research Laboratory, Tyndall Air Force Base
U.S. Army Research, Development and Engineering Command, Simulation and Technology Training Center
Vcom3D, Inc., Orlando

Georgia

Georgia Tech Research Institute, Atlanta

Idaho

Idaho National Laboratory, Idaho Falls

Illinois

Argonne National Laboratory, Argonne
Illinois Fire Service Institute – University of Illinois, Champaign

Indiana

Conflict Kinetics, Merrillville
Indiana University-Purdue University Indianapolis, Indianapolis
Naval Surface Warfare Center, Crane Division, Crane
Raytheon Technical Services, Indianapolis
Vohne Liche Kennels Canine Security, LLC, Denver

Maryland

Army Aberdeen Test Center, Aberdeen Proving Ground
Army Medical Research and Material Command, Fort Detrick
Army Research Laboratory, Aberdeen Proving Ground
Edgewood Chemical Biological Center, Aberdeen Proving Ground
HazTrain, Waldorf
Impact Computing Corporation, Silver Spring
Naval Air Warfare Center Aircraft Division, Patuxent River
Naval Explosives Ordnance Disposal Technology Division, Indian Head
Naval Surface Warfare Center, Indian Head Division, Indian Head
Pitney Bowes Government Solutions, Inc., Latham
Regal Decisions Systems, Inc., Belcamp
SimQuest, Silver Spring
SURVICE Engineering, Belcamp
TRX Systems, Inc., Greenbelt
U.S. Army Public Health Command, Aberdeen
U.S. Army Test and Evaluation Center, Aberdeen
Vehicle Systems Integration, LLC, College Park
W.L. Gore & Associates, Elkton
Zephyr Technology Corporation, Annapolis

2010 Performers

Massachusetts
American Science and Engineering, Inc., Billerica
Artisent, Inc., Boston
BAE Systems, Burlington
Black I Robotics, Tyngsboro
Charles River Analytics, Cambridge
Excellims Corporation, Maynard
Foster-Miller, Inc., Waltham
Noble Peak, Wakefield
QinetiQ – North America, Inc., Waltham
Raytheon BBN, Cambridge
Reveal Imaging Technologies, Bedford
Safran, Wilmington
Technical Products, Inc., Sterling
ThermoFisher Scientific, Wilmington
U.S. Department of Transportation Volpe Center, Cambridge

Michigan
Avon Protection Systems, Inc., Cadillac
Baker Enterprises, Alpena
Michigan State University, East Lansing
Quantum Signal, LLC, Ann Arbor
Soar Technology, Inc., Ann Arbor
Wayne State University, Detroit

Minnesota
Agile Defense, LLC, Hopkins
University of Minnesota, Minneapolis

Mississippi
U.S. Army Engineer Research and Development Center, Vicksburg

Missouri
Clean Earth Technologies, LLC, Earth City
Essex PB&R Corporation, St. Louis
Midwest Research Institute, Kansas City
Washington University in St. Louis, St. Louis

Montana
Veridical Research and Design Corporation, Bozeman

Nebraska
U.S. Army Corps of Engineers Protective Design Center, Omaha

Nevada
Global Specialized Medicine, Reno
HBM Associates, LLC, Las Vegas
ID Scientific, Las Vegas

2010 Performers

National Nuclear Security Administration, Las Vegas
Protype, Las Vegas
Remote Sensing Laboratory, Las Vegas

New Hampshire
Elbit Systems of America, Merrimack
Globe Manufacturing Company, LLC, Pittsfield
Integral Design and Development, Brentwood
U.S. Army Cold Regions Research and Engineering Lab, Hanover
Warwick Mills, New Ipswich

New Jersey
Armament, Research, Development and Engineering Center, Picatinny Arsenal
Lockheed Martin Advanced Technology Laboratories, Cherry Hill
Sarnoff Corporation, Princeton
Structured Materials Industries, Piscataway

New Mexico
Applied Research Associates, Albuquerque
Energetic Materials Research and Testing Center, Socorro
Least Squares Software, Inc., Albuquerque
Los Alamos National Laboratory, Los Alamos
MesoSystems Technology, Inc., Albuquerque
National Assessment Group, Kirtland Air Force Base
Sandia National Laboratories, Albuquerque
Stolar Research Corporation, Raton
White Sands Missile Range, White Sands

New York
CUBRC, Inc., Buffalo
GE Global Research, Niskayuna
Kitware, Inc., Clifton Park
Material Intelligence, LLC, New York
Persistent Systems, LLC, New York
Plug Power, Inc., Latham
Skidmore College, Saratoga Springs

North Carolina
Appealing Products, Inc., Raleigh
Archangel Armor, Fayetteville
BGP, Inc., Raleigh
Duke University, Durham
General Dynamics Armament & Technical Products, Inc., Charlotte
North Carolina State University, Textile Protection and Comfort Center, Raleigh
XinRay Systems, Research Triangle Park

Ohio
Applied Research Associates, Inc. (Klein Associates Division), Fairborn

2010 Performers

Battelle Memorial Institute, Columbus
Honeywell, Dayton
Lion Apparel, Dayton

Oklahoma
ICx Nomadics, Inc., Stillwater
Southwest Research Institute, Midwest City
Tactical Electronics, LLC, Broken Arrow

Pennsylvania
Carnegie Mellon University, Pittsburgh
Drexel University Data Fusion Laboratory, Philadelphia
DRS Laurel Technologies, Johnstown
Dynamic Defense Materials, LLC, Boothwyn
EyeSee360, Inc., Pittsburgh
L-3 Services Group, Command and Control Systems and Software Division, Horsham
National Institute for Occupational Safety and Health – The National Personal Protective Technology Laboratory, Pittsburgh
Nuvision Engineering, Pittsburgh
Ordnance Holdings, Inc., Drexel Hill
Pennsylvania State University, University Park
RE2, Inc., Pittsburgh
Saint Joseph's University, Early Responders Distance Learning Center, Philadelphia
University of Pennsylvania, Philadelphia

South Carolina
Advanced Mission Systems, Fort Mill
Time Cuffs, LLC, North Charleston

Tennessee
Northrop Grumman-Remotec, Clinton
Oak Ridge National Laboratory, Oak Ridge
Universal Strategy Group, Inc., Mt. Pleasant

Texas
21st Century Technologies, Austin
Accuracy 1st, Inc., Arthur City
Applied Research Associates, Inc., San Antonio
International Personnel Protection, Inc., Austin
OI Analytical, College Station
Protection Engineering Consultants, Spring Branch
Southwest Foundation for Biomedical Research, San Antonio
Southwest Research Institute, San Antonio
University of Houston, Houston
U.S. Army Institute of Surgical Research, Fort Sam Houston

Utah
AccessData Corporation, Lindon

2010 Performers

Vermont
Norwich University Applied Research Institutes, Northfield

Virginia
Analytic Services, Inc. (ANSER), Arlington
Ashlar International, LLC, Ashburn
A-T Solutions, Fredericksburg
Avir, LLC, Charlottesville
Battelle Memorial Institute, Arlington
Blackbird Technologies, Herndon
Center for Innovative Technology, Herndon
Courage Services, Inc., McLean
Defense Threat Reduction Agency
Federal Bureau of Investigation, Quantico
Gatekeeper Security, Inc., Reston
George Mason University, Fairfax
Goetz Printing, Springfield
Hazard Management Solutions, Inc., Arlington
Institute for Applied Science, Reston
Lockheed Martin Information Systems and Global Services, Chantilly
Logos Technologies, Inc., Arlington
McQ, Inc., Fredericksburg
Naval Surface Warfare Center, Dahlgren
NSI, Inc., Fairfax
Ocean Marine Industries, Inc., Chesapeake
Patriot3, Inc., Fredericksburg
Platinum Solutions, Inc., Reston
S4 Tech, Inc., Reston
Science Applications International Corporation (SAIC), Sterling
SPADAC, McLean
Sparta, Inc., Arlington
System Planning Corporation, Arlington
The Penro Group, Alexandria
Trident Systems, Inc., Fairfax
University of Virginia, Charlottesville
White Canvas Group, Arlington

Washington
Advanced Interactive Systems, Seattle
Boeing, Seattle
Cascade Designs, Inc., Seattle
Isotron Corporation, Seattle
MesoSystems Technology, Inc., Kennewick
Pacific Northwest National Laboratory, Richland

West Virginia
STS International, Berkeley Springs

2010 Performers

West Virginia High Technology Consortium Foundation, Fairmont

Wisconsin
Quantumspex, Inc., Madison

International

Australia
Appen Pty Ltd., Chatswood, New South Wales
Australian Customs and Border Protection Service
Australian Federal Police, Canberra
Bond University, Gold Coast, Queensland
Defence Science and Technology Organisation, Fishermans Bend, Victoria
Defence Science and Technology Organisation, Melbourne
Department of the Prime Minister and Cabinet, Canberra
Emergency Management Australia, Canberra
Flinders University of South Australia, Adelaide
Griffith University, Brisbane
Queensland Fire and Rescue, Brisbane
Queensland University of Technology, Brisbane
University of Adelaide, Adelaide
University of Western Australia, Sydney

Canada
Allen-Vanguard Protective Technologies, Ltd., Ottawa, Ontario
Ballard Power Systems, Burnaby, British Columbia
Canadian Border Service Agency, Ottawa, Ontario
Canadian Commercial Corporation, Ottawa, Ontario
Defence Research and Development Canada, Suffield
Defence Research and Development Canada, Valcartier, Quebec
Oculus, Toronto, Ontario
Optosecurity, Inc., Quebec City, Quebec
Royal Canadian Mounted Police, Ottawa, Ontario

France
University of Rennes, Brittany

Germany
Siemens Medical Solutions, Vacuum Technology, Erlangen

Israel
Adaptive Imaging Technologies, Yokneam Illit
Controp Precision Technologies, Hod Hasharon
DEA Research and Development, Ltd., Jerusalem
Elbit Systems, Haifa
Electro-Optics Industries, Ltd., Rehovat

2010 Performers

Elop, Rehovat
Israel Defense Forces, Combat Engineering Corps
Israel Defense Forces, Home Front Command
Israel Institute for Biological Research, Tel Aviv
Israel Ministry of Defense, Tel Aviv
Israel National Police, Jerusalem
Israel Police National Headquarters, Jerusalem
Israeli Security Agency
Negev Nuclear Research Center, Negev
Rafael Armament Development Authority Ltd., Haifa
ROTEM Industries, Ltd., Tel Aviv
Soltam Systems, Ltd., Yokneam
Soreq, Tel Aviv
Tamar Explosives, Inc.
The Hebrew University of Jerusalem, Jerusalem

Netherlands

TNO Defence, Security and Safety, Soesterberg

Singapore

Defence Science and Technology Agency
Ministry of Defense
Ministry of Home Affairs
Nanyang Technological University
Naval Surface Warfare Centre
Republic of Singapore Navy
Singapore Armed Forces
Singapore Technologies Electronics Ltd.
Specialized Craft Group, Fleet

United Kingdom

Centre for the Protection of National Infrastructure, London
Chelsea Technologies Group, West Molesey
Cognitive Consultants International, Ltd., Southhampton
Counter Terrorism Science and Technology Centre, Porton Down
Defence Science and Technology Laboratory, Fort Halstead, Kent
Defence Science and Technology Laboratory, Porton Down
Hazard Management Solutions, Inc. Farington, Oxfordshire
Home Office Scientific Development Branch, London
MBDA, Bristol
Ministry of Defence, London
Ministry of Defence Counter Terrorism Science and Technology Center, Salisbury
QinetiQ, Farnborough
UK Metropolitan Police, London

Glossary of Acronyms

A

ACC	Air Combat Command
AFESC	Air Force Engineering and Services Center
AFIP	Armed Forces Institute of Pathology
AFRL	Air Force Research Lab
AFS	Advanced Small-Room Chemical and Biological Filtration System
AGMMN	Air/Ground Mobile Mesh Network
AMEDD	Army Medical Department
ANSS	Airborne Network Security Simulator
ARA	Applied Research Associates, Inc.
ARDEC	Armaments Research, Development and Engineering Center
ARL	Army Research Laboratory
ASD	Assistant Secretary of Defense
ASD (SO/LIC & IC)	Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict and Interdependent Capabilities
ATD	Anthropomorphic Test Device
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AWE	Assured Wireless Ethernet

B

BAA	Broad Agency Announcement
BIDS	BAA Information Delivery System

C

CB	Chemical and/or Biological
CBA	Canine Body Armor
CBP	Customs and Border Protection
CBIRF	Chemical Biological Incident Response Force
CBR	Chemical, Biological, and Radiological
CBRN	Chemical, Biological, Radiological, and Nuclear
CBRNC	Chemical, Biological, Radiological, and Nuclear Countermeasures
CBRNE	Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives
CbT	Combating Terrorism
CDC	Centers for Disease Control and Prevention
CENTCOM	U.S. Central Command
CID	Criminal Investigation Command (U.S. Army)
CIRTS	Critical Incident Response Technology Seminars
CIT	Center for Innovative Technology
CML Bn(TE)	Chemical Battalion (Tech Escort)
CMLS	Chemical School
COIN	Counterinsurgency
COTS	Commercial Off-the-Shelf
CTTSO	Combating Terrorism Technical Support Office

Glossary of Acronyms

D

DACA	Defense Academy for Credibility Assessment
DARPA	Defense Advanced Research Projects Agency
DATSD (CBD)	Office of the Deputy Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense
DCFL	Defense Computer Forensics Laboratory
DEA	Drug Enforcement Administration
DFL	Drexel University Data Fusion Laboratory
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DOE	Department of Energy
DOG	Digital Observation Guard
DOJ	Department of Justice
DORA	Detection of Rocket Attacks
DOS	Department of State
DS	Bureau of Diplomatic Security
DTRA	Defense Threat Reduction Agency

E

ECBC	Edgewood Chemical Biological Center
ECM	Electronic Countermeasures
ED	Explosives Detection
EMTS	Enhanced Mortar Targeting System
EOD	Explosive Ordnance Disposal
EOD/LIC	Explosive Ordnance Disposal/Low-Intensity Conflict
EPA	Environmental Protection Agency
ERIS	Ethnic Conflict, Repression, Insurgency and Social Strife

F

FAA	Federal Aviation Administration
FAMS	Federal Air Marshal Service
FBI	Federal Bureau of Investigation
FBOP	Federal Bureau of Prisons
FDA	Food and Drug Administration
FDE	Forensic Document Examiners
FDL	Forensic Document Laboratory
FEMA	Federal Emergency Management Agency
FPS	Federal Protective Service
FSIS	Food Safety and Inspection Service
FY	Fiscal Year

Glossary of Acronyms

G

GPO	Government Printing Office
GPS	Global Positioning System

H

HAZMAT	Hazardous Material
HME	Homemade Explosives
HRP	High-Risk Personnel
HRT	Hostage Rescue Team
HSC	Homeland Security Council
HSCB	Human Social, Cultural, and Behavior Modeling
HSS	Office of Health, Safety and Security

I

IC	Intelligence Community
ICBA	Improved Concealable Body Armor
ICE	Immigration and Customs Enforcement
IDD	Improvised Device Defeat
IED	Improvised Explosive Device
INSCOM	Intelligence and Security Command
IR	Infrared
IRCC	Integrated Ruggedized Checkpoint Container
IRS	Internal Revenue Service
ISF	Investigative Support and Forensics
IWS	Irregular Warfare Support

J

JANS	Joint Airborne Network Security
JCS	Joint Chiefs of Staff
JET	Jamming Effectiveness Tester
JIEDDO	Joint Improvised Explosive Device Defeat Organization
JWAC	Joint Warfare Analysis Center

M

MANSCEN	Maneuver Support Center
MARSOC	Marine Corps Special Operations Command
MGED	Multifunction GPS/Emergency Device
MIMEO	Modeling Information Propagation Through Memetic Evolution
MISO	Military Information Support Operations
MRMC	Medical Research and Material Command
MS&G	Models, Simulations, and Games

Glossary of Acronyms

N

NASA	National Aeronautics and Space Administration
NAVAIR	Naval Air Systems Command
NAVATA	Networked Advanced Vehicle Anti-Tamper and Alert System
NAVCENT	Naval Forces Central Command
NAVEODFLTLAU	Naval Explosive Ordnance Disposal Fleet Liaison Office
NAVEODTECHDIV	Naval Explosive Ordnance Disposal Technology Division
NAVFAC	Naval Facilities Engineering Command
NAVSEA	Naval Sea Systems Command
NAWC	Naval Air Warfare Center
NCFS	National Center for Forensic Science
NCIS	Naval Criminal Investigative Service
NEIC	National Enforcement Investigations Center
NFPA	National Fire Protection Association
NFSTC	National Forensic Science Technology Center
NGA	National Geospatial-Intelligence Agency
NGIC	National Ground Intelligence Center
NIJ	National Institute of Justice
NIOSH	National Institute for Occupational Safety and Health
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NRL	Naval Research Laboratory
NRO	National Reconnaissance Office
NSA	National Security Agency
NSWC	Naval Surface Warfare Center
NTOA	National Tactical Officers Association
NTSB	National Transportation Safety Board
NV	Night Vision

O

OIG	Office of the Inspector General
OLES	Office of Law Enforcement Standards
ONR	Office of Naval Research
OSI	Office of Special Investigations
OUSD (P&R)	Office of the Under Secretary of Defense for Personnel and Readiness

P

PAPR	Powered Air Purifying Respirator
PBI	Post-Blast Investigation
PBIED	Person-Borne Improvised Explosive Device
PD	Police Department
PEO-SEQ	Program Executive Office Soldier Equipment
PFPA	Pentagon Force Protection Agency
PM-FPS	Product Manager for Force Protection Systems

Glossary of Acronyms

PM-G	Product Manager for Guardian
PP	Personnel Protection
PPE	Personal Protective Equipment
PS	Physical Security
PSASK	Portable Seismic Acoustic Sensor Kit
PSD	Protective Service Details
PSDA	Personal Security Decision Aid
PSYOP	Psychological Operations

R

R&D	Research and Development
RAM	Random-Access Memory
RDD	Radiological Dispersion Device
RDECOM	Research, Development and Engineering Command
RMP	Remote Mobility Platform

S

S/CT	Department of State Office of the Coordinator for Counterterrorism
S&T	Science and Technology
SCBA	Self-Contained Breathing Apparatus
SCOS	Surveillance, Collection, and Operations Support
SOF	Special Operations Forces
SO/LIC & IC	Special Operations/Low-Intensity Conflict and Interdependent Capabilities
SOCOM U.S.	Special Operations Command
SOS	Security Observation Set
SSC	Soldier Systems Center (Natick)
SSTR	Stability, Security, Transition, and Reconstruction
STARRS	Special Timer Activated Restraint and Release System
SWAT	Special Weapons and Tactics

T

TD-STAMP	Triple Sensor/Designator-Stabilized Miniature Payload
TIC	Toxic Industrial Chemical
TOS	Tactical Operations Support
TRADOC	Training and Doctrine Command
TSA	Transportation Security Administration
TSL	Transportation Security Laboratory
TSWG	Technical Support Working Group
TTD	Training Technology Development

U

UAS	Unmanned Aerial Systems
UBT	Universal Biometric Translator

Glossary of Acronyms

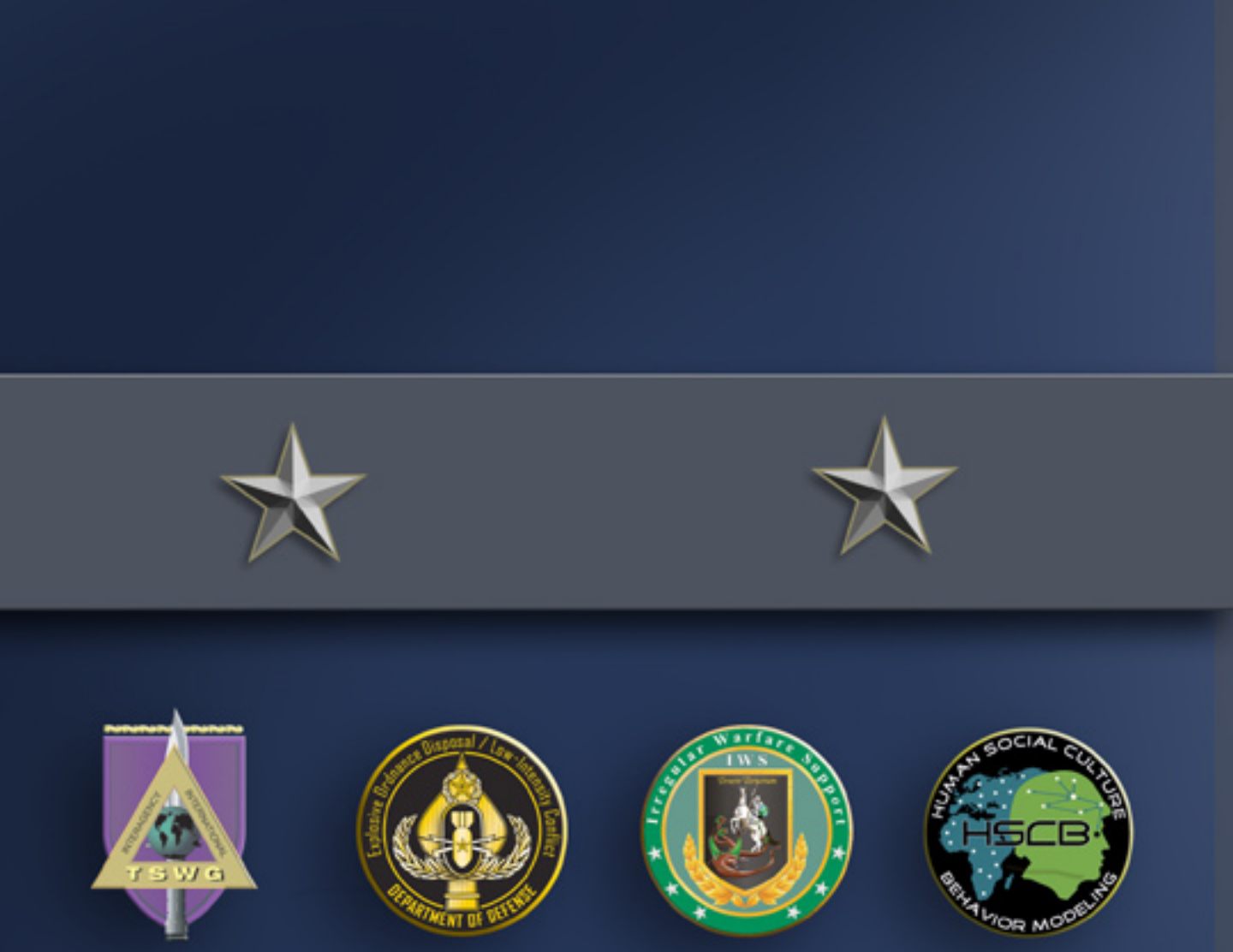
US&R	Urban Search and Rescue
USACE	United States Army Corps of Engineers
USAF	United States Air Force
USCD	University of California at San Diego
USCG	United States Coast Guard
USMC	United States Marine Corps
USMS	United States Marshals Service
USN	United States Navy
USSS	United States Secret Service

V

VBADS	Vehicle-Borne Assisted Detection System
VBIED	Vehicle-Borne Improvised Explosive Device
VIP	Very Important Person
VIPR	VIP Ruggedized Security Kit
VIPSKIT	VIP Security Kit

W

WAVELib	Wide Area Video Exploitation Library


TSWG
Explosive Ordnance Disposal / Low-Intensity Conflict
DEPARTMENT OF DEFENSE
Irregular Warfare Support
IWS
HSCB
HUMAN SOCIAL CULTURE
BEHAVIOR MODELING