ANTITERRORISM

COUNTERTERRORISM

INTELLIGENCE SUPPORT

CONSEQUENCE MANAGEMENT

TECHNICAL SUPPORT WORKING GROUP

2003

TSWG REVIEW

COMBATING TERRORISM

Preface

The unrelenting pace of terrorist attacks during 2003 served as a sobering reminder that the dangers of international terrorism, fully revealed to the American public on September 11, 2001, must never be forgotten. The locations and methods of attacks seen during 2003 underscore the world-wide scope and evolving technical sophistication of terrorist organizations intent on the destruction of political systems through the murder of political leaders, military and security forces, and innocent civilians around the world.

In his remarks to The Elliott School of International Affairs (The George Washington University, Washington, DC September 5, 2003), Secretary of State Colin L. Powell emphasized the importance of international cooperation in the Global War on Terrorism:

> "...the President set us on the task not just to get the killers of 9/11, but to instead lead a global campaign against all terrorism, against all terrorists. He did this because he understood that terrorism is not just America's problem; it is everyone's problem, it is a problem for the civilized world, and the civilized world had to come together under his leadership to deal with it."

Developing technical countermeasures to thwart or to respond to terrorist attacks has always been part of the arsenal of tools available to the U.S. These tools also include (inter alia) diplomacy, military intervention, intelligence collection, enhanced security, financial controls, law enforcement, and legislative initiatives. In light of the expanding variety of terrorist capabilities and methods, sophisticated technical approaches to counter terrorism are increasingly important to protect targets in government, military, and civilian settings and to take the Global War on Terrorism (GWOT) offensively to the terrorists. Whether person-borne suicide bomb attacks in Russia, Morocco, and Israel, or vehicle-borne improvised explosive attacks in

"The war on terror is not a war that we asked for. But it is a war that we must fight and we must win."

Donald H. Rumsfeld

Colombia, Saudi Arabia, Iraq, Turkey, India and Indonesia, the merciless application of deadly violence to pursue terrorist agendas underscores the essential need to develop more effective technical countermeasures and for cooperative counterterrorism efforts on a global scale.

In addition to the well-recognized threat from conventional and improvised explosive devices, there are consistent indications that terrorists are pursuing new and more deadly ways of attacking targets around the world. The U.S. intelligence community has warned that several mujahedin groups associated with Al-Qaida have attempted to carry out poison plot attacks in Europe with relatively easily produced chemicals and toxins. The Community further notes that Al-Qaida has expressed interest in radiological dispersal devices, and there are indications that the group possesses the knowledge and wherewithal to produce several crude chemical and biological agents. Deputy Secretary of State Richard L. Armitage, in his remarks at the Asia Society Forum (Sydney, Australia, August 13, 2003) captured the worldwide concern with indiscriminate and increasingly lethal use of all forms of terrorist violence:

> "After all, the terrorists espouse an ideology of destruction, and they aren't particular about just whom they kill. It's not just Americans and Australians who have been slaughtered by Al-Qaida and its affiliates, but hundreds of Filipinos, Kenyans, Moroccans, Saudis, and Tanzanians. Citizens of more than 90 nations died in the World Trade Center alone."

Since 1986, the Technical Support Working Group (TSWG) has pursued combating terrorism technologies in the broad context of national security by providing a cohesive interagency forum to define user-based technical requirements spanning the Federal interagency community. By harnessing the creative spirit of U.S. and foreign industry, academic institutions, government, and private laboratories, the TSWG ensures a robust forum for technical solutions to the most pressing counterterrorism requirements. Participants in the nine functional subgroup areas of the TSWG can come to a single table to articulate specific threats and user-defined technical requirements. This guarantees a consensus-based approach to the rapid prototyping and development of combating terrorism devices, training tools, reference materials, software, and other equipment.

The importance of engaging both the user communities and the scientific community in a coordinated, focused, and concerted effort to support the GWOT was underscored by President George W. Bush in his remarks on the Bioterrorism Initiative (National Institutes of Health, Bethesda, Maryland, February 3, 2003):

> "America's war on terror has tested this nation, has tested our resolve, our will, our determination, and I'm confident that we can call upon our resources and strengths to prevail. There is no doubt in my mind, the men and women of our scientific community are among this country's greatest strengths."

In furtherance of the President's charge and our national goals, the TSWG is continuing to focus its program development efforts to balance investments across the four pillars of combating terrorism: antiterrorism; counterterrorism; intelligence support; and consequence management. The challenge is to provide a coherent and consistent context for technology development based upon innovation, real operator needs, and proven procedures and tactics.

In this report you will read about some new capabilities developed by the TSWG in FY 2003, as well as some capabilities still under development. There are other projects that, because of sensitivity, cannot be described in an unclassified report. Together they comprise the TSWG's evolving program to develop technology and capability to support the U.S. and its allies in the GWOT.

"...we will fight back with all the tools at our disposal and we will be successful."

Colin L. Powell

Table of Contents

The Technical Support Working Group

Organization and Structure..... 1
Program Funding..... 3

The Technical Support Working Group Subgroups

Chemical, Biological, Radiological
and Nuclear Countermeasures..... 5
Explosives Detection..... 11
Improvised Device Defeat..... 15
Infrastructure Protection..... 19
Investigative Support and Forensics..... 23
Personnel Protection..... 27
Physical Security..... 31
Surveillance, Collection and Operations Support..... 35
Tactical Operations Support..... 37

Appendices

BAA Information Delivery System..... 41
TSWG Membership..... 43
TSWG Subgroup Membership..... 47
TSWG Performers..... 53
Glossary of Acronyms..... 59

TSWG Organization

In April 1982, National Security Decision Directive (NSDD) 30 assigned responsibility for the development of overall U.S. policy on terrorism to the Interdepartmental Working Group on Terrorism (IG/T), chaired by the Department of State (DOS). The 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 George H. W. Bush cited the TSWG as assuring “the development of appropriate counterterrorism technological efforts.”

Today, the TSWG still performs that counterterrorism technology development function as a stand-alone interagency working group. TSWG's mission is to conduct the national interagency research and development (R&D) program for combating terrorism requirements. It also has commenced efforts to conduct and influence the focus of longer-term R&D initiatives and, reflecting the shift to a more offensive strategy, balance its technology and capability development efforts among the four pillars of combating terrorism: intelligence support; counterterrorism; antiterrorism; and consequence management.

Structure

The TSWG operates under the policy oversight of the DOS’s Coordinator for Counterterrorism and the management and technical oversight of the Department of Defense (DoD) Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD (SO/LIC)). Participation is open to Federal departments and agencies. While the TSWG's core funds are derived principally from DoD's Combating Terrorism Technology Support (CTTS) Program and the DOS, other departments and agencies contribute additional funds. Other departments and agencies also provide personnel to act as project managers and technical advisors.

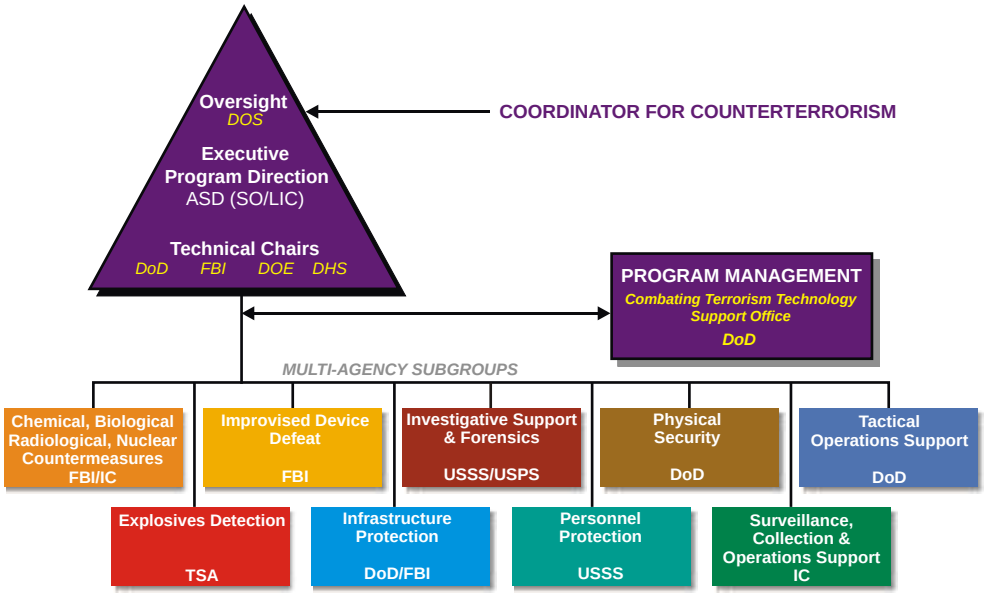
As a result of Congressional direction for the TSWG to engage in joint counterterrorism R&D efforts with selected NATO and major non-NATO allies, the TSWG assumed an international dimension in FY 1993. TSWG conducts cooperative R&D with Canada, Israel, and the United Kingdom through separate bilateral agreements. Cooperative technology development with selected foreign partners supports not only the GWOT, but increasingly addresses the specific needs of Coalition warfighters in Iraq and Afghanistan. During FY 2003, the TSWG expanded international cooperative activities with its current international partners. Continued discussions with two other nations are likely to lead to expansion of TSWG international activities in FY 2004.

The TSWG has successfully transitioned capabilities to the Departments of Agriculture, Defense, Justice, State, and Treasury; the Intelligence Community; the Transportation Security Administration; the Public Health Service; and other departments and agencies.

TSWG membership includes representatives from over eighty organizations across the Federal Government. These departments and agencies work together by

participating in one or more subgroups. A comprehensive listing of member organizations by subgroup is provided in the appendix.

The nine subgroups are: Chemical, Biological, Radiological and Nuclear Countermeasures; Explosives Detection; Improvised Device Defeat; Infrastructure Protection; Investigative Support and Forensics; Personnel Protection; Physical Security; Surveillance, Collection and Operations Support; and Tactical Operations Support.



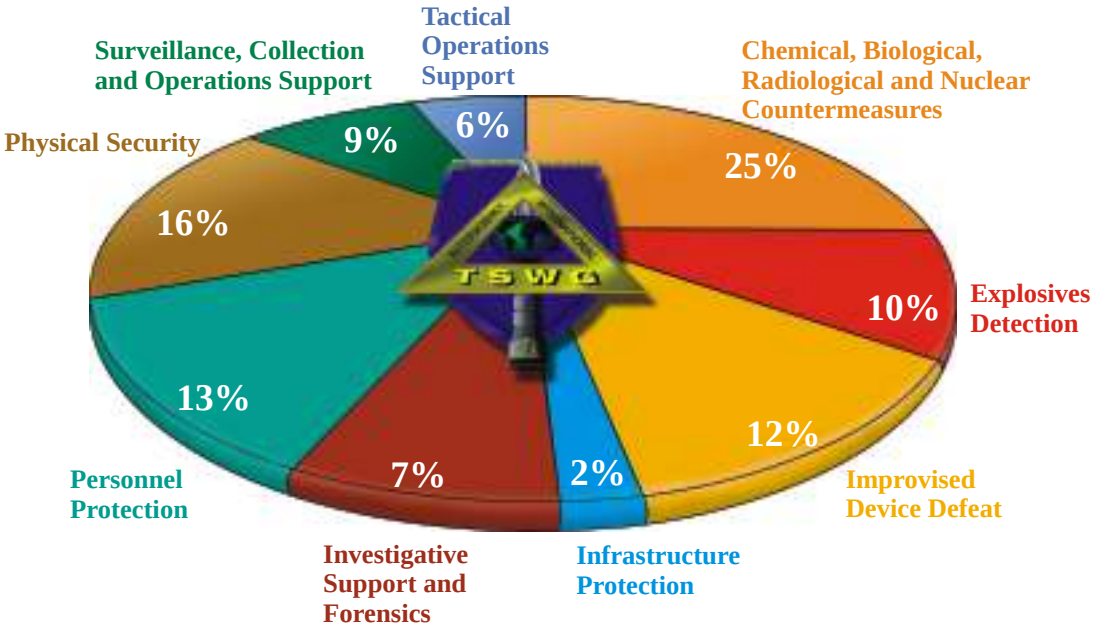
TSWG Organization

Each Subgroup is chaired by a senior representative from a Federal agency with special expertise in that functional area. Chairmanship of three Subgroups is shared as indicated in the organizational chart above.

The recently created Department of Homeland Security (DHS) was added to the TSWG Executive Committee this year as a technical co-chair. The DHS constituent agencies remain TSWG members as they were before the creation of DHS.

TSWG Program Funding

Funding for the TSWG program has increased from $8 million in FY 1992 to approximately $180 million in FY 2003. This increase reflects the heightened concern over terrorist activity and the recognized need to accelerate the development of technology to effectively address the threat. The Department of Defense provides the bulk of funding for TSWG activities. The Department of State contributes annually to TSWG core funding, while other departments and agencies share the costs of selected projects.



TSWG FY 2003 Program Funding *($ 180 Million)*

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 interagency user requirements for countering the terrorist employment of CBRN materials. The CBRNC Subgroup identifies, validates, and prioritizes multi-agency requirements and competitively seeks technology solutions. Through its participation in the Interagency Board (IAB) for Equipment Standardization and Interoperability and in coordination with DHS, NIJ, and EPA, the CBRNC Subgroup integrates technology requirements from the fire, hazardous materials, law enforcement, and emergency medical services communities into its process. The Subgroup is co-chaired by senior representatives from the FBI and the Intelligence Community.

Focus Areas
The Subgroup covers the full range of CBRN incident prevention and response to improvised CBRN devices and training. During FY 2003, these focus areas were:

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

Protection
Enhance the operating performance and reduce the costs of personal and building protection CB equipment. Personal Protective Equipment (PPE) includes respiratory protection systems and suits. Building protection includes design tools for engineers in addition to advanced filter materials.

Decontamination
Improve technologies and protocols for personnel, facilities and equipment decontamination. Systems will be low-cost, environmentally benign, and safe. They will also be effective for decontaminating biological and chemical warfare agents, and persistent toxic industrial chemicals. The technologies may also be used for mitigation after a release of radioactive materials.

Training
Develop hardware and software for military and civilian CBRN Consequence Management

Membership

ENVIRONMENTAL PROTECTION AGENCY
GENERAL SERVICES ADMINISTRATION
  Mail Policy
INTELLIGENCE COMMUNITY
INTERAGENCY BOARD
U.S. CAPITOL POLICE
U.S. DEPARTMENT OF AGRICULTURE
  APHIS
U.S. DEPARTMENT OF COMMERCE
  NIST
U.S. DEPARTMENT OF DEFENSE
  DIA, DTRA, JCS, NSA, DATSD/CBD, PFPA, SOCOM, USA (52nd Ord, USAMRIID, CMLS, ECBC, FORSCOM, MANSCEN, NGIC, SBCCOM, TEU), USAF (ACC, ESC, FPBL, SG), USMC (CBIRF), USN (NAVCENT, NAWC, NSWC)
U.S. DEPARTMENT OF ENERGY
  OS
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
  FDA
U.S. DEPARTMENT OF HOMELAND SECURITY
  FEMA, S&T, TSA, USCG, USSS
U.S. DEPARTMENT OF JUSTICE
  FBI (BDC, HMRU, WMDOU), NIJ, USMS
U.S. DEPARTMENT OF STATE
  DS, OBO, S/CT
U.S. DEPARTMENT OF TRANSPORTATION
  I&S
U.S. POSTAL SERVICE
  USPIS
WHITE HOUSE
  OSTP

training. Training materials will use Advanced Distance Learning media, including web-based, interactive CD-ROM, and virtual reality via the Internet. Training materials are also developed as part of this focus area.

Information Resources
Develop shared information management tools to provide a common "picture of the scene" and facilitate the efficient integration of diverse emergency and consequence management elements from Federal, State, and local agencies.

Selected Completed Projects

CB Building Improvement Design Protocol
Modifications to office buildings can reduce the vulnerability of occupants to terrorist attack with chemical or biological agents. To cost-effectively counter that threat, architects and engineers require computer models to predict how changes in building design and building HVAC system operating parameters improve the protection of the occupants. Using an array of databases, test protocols, analysis tools, and optimization methods, Lagus Applied Technology, Inc. developed a Windows-based design protocol to determine how design and operating changes improve the protection of building occupants. This tool also estimates the installation and operating costs for making the modifications to the building. The system is undergoing operational evaluation. Requests for additional information from government agencies should be sent to *cbrncsubgroup@tswg.gov*.

Escape Hood Testing

In the event of a chemical or biological attack on a workplace, escape hoods can provide personnel the additional protection they need to survive during evacuation to a safe area. The escape hoods provide at least 15 minutes of respiratory and ocular protection against a variety of chemical and biological threat agents. In their sealed containers, the hoods can easily fit in a desk drawer or briefcase. The hoods, which can be donned in less than 30 seconds, are designed to provide protection for the general population of adults, even those wearing eyeglasses or having beards. In addition to the two models that have already passed the testing, two designs that minimize claustrophobia, training, and breathing stress are under evaluation. More than 200,000 of these escape hoods have been sold. The Quick2000™ (*www.quickmask.com)* and the MSA Response™ Escape Hood (*www.msanet.com*) have successfully completed the testing The ILC Dover SCape Hood (*www.ilcdover.com)* has completed testing except for final human factors evaluation. The National Institute for Occupational Safety and Health (NIOSH) published its CBRN Escape Respirator Standard in October 2003.

Expedient Chemical/Biological Release Mitigation

A chemical or biological release when evacuation of personnel is not possible, such as in an aircraft in flight, poses a special challenge for those responsible for safety of the passengers. Trained HAZMAT response personnel typically will not be available during the early stages of such an attack. The expedient mitigation kit was designed for use by trained a crew member to minimize

the release of the chemical or biological agent. The kit includes effective, low-cost, and light-weight equipment to protect the hands, face, and respiratory system. Following protocols and response procedures in a laminated booklet, the trained crew member can secure the improvised chemical or biological device in an impermeable overpack bag and cover the contaminated area with sorbent and plastic sheeting to minimize the spread. To order the kits, send requests to *cbrncsubgroup@tswg.gov*.

Mass Personnel Decontamination Protocols

Decontaminating civilian victims of a terrorist chemical or biological (CB) attack presents unique challenges. Subject matter experts from the U.S. and TSWG's Canadian and United Kingdom partners have prepared evidence and consensus-based guidelines and best practices for decontaminating civilians of all ages and abilities in the event of a CB incident. The technical validity and operational desirability of each step of the existing procedures were evaluated. Members of the IAB provided direct user inputs during the process. The guidelines can be purchased in laminated flip book and CD formats through the Chemical and Biological Defense Information Analysis Center (CBIAC). To order visit the products catalog at *www.cbiac.apgea.army.mil*.

Portable Modular Filtration Unit

In the event of a terrorist attack with chemical or biological agents, other threats may preclude personnel at critical overseas facilities from immediately evacuating the building. Installed in a designated safe haven, the portable modular filtration unit will remove chemical and biological agents from the air to protect the occupants of the room. The prototype filtration system is designed for integration into office buildings. Providing protection comparable to military systems, the design and new sound dampening technology can provide safe rooms at critical facilities with the best available protection without detracting from the room's normal function. Information is available by sending an e-mail to *info@germfree.com.*

Self-Indicating Radiation Dosimeter

The self-indicating radiation dosimeter badge puts affordable radiation exposure data in the hands of public safety personnel responding to a radiological dispersion device or “dirty bomb.” This casualty radiation dosimeter uses a material that changes color on exposure to radiation. The instantaneous read-out of personal exposures permits incident managers and medical personnel to identify response personnel requiring immediate medical attention during a radiological or nuclear incident. Over 6000 dosimeters have been deployed during the user evaluation. A self-reading badge that provides direct numeric output in place of the color matching used now is being developed. Additional information is available at *www.jplabs.com*.

WMD Panic Response Operations (WMD-PRO) Course

The WMD-PRO course trains terrorism response personnel to recognize, minimize, and manage the severe panic and mass hysteria associated with weapons of mass destruction (WMD) incidents. The course addresses the potential for panic associated with emergency situations, specifically WMD incidents; the relationship between panic

and fear; and the tools needed to prevent fear from escalating into panic. The course also provides guidance on how to identify the non-verbal cues signaling the possibility of panic before, during, and following a WMD incident; how to observe behavior to understand what the victim is feeling; and how to help the victim manage his or her feelings long enough to prevent panic. The WMD-PRO course was developed by the St. Joseph's University Early Responders Distance Learning Center (*erdlc.sju.edu/education-course.php)* and is available in paper, CD-ROM, and web-based delivery formats.

Selected Current Projects

Drink System for Powered Air Purifying Respirator (PAPR) and Self-Contained Breathing Apparatus (SCBA)

One of the lessons learned during recovery operations following the terrorist attacks of 2001 was the importance of ensuring response personnel maintain hydration while wearing PPE. Battelle Memorial Institute has developed a hands-free hydration system that reduces the risk of heat stroke by permitting proper hydration. Integrating this universal drinking system into PAPRs and SCBAs used by public safety personnel will extend the time that response personnel can operate in the hot zone without having to decontaminate and exit the contaminated area to get a drink. Manufacturers are currently integrating the drink system into their design and submitting them to NIOSH for approval, after which the system will be commercially available.

Biodosimetry Assessment Tool (BAT) Integration

Emergency response and health care providers need information resources and tools to help identify and manage radiation casualties in the aftermath of a nuclear detonation, reactor accident, or large radiological dispersion device attack. The Armed Forces Radiobiology Research Institute (AFRRI) BAT provides reference, response, and management tools to meet that need. This project expands the availability of BAT by making it compatible with a wide array of commercially available emergency response software applications enhancing the ability to respond and save lives. The current stand-alone version of BAT is available from *www.afrri.usuhs.mil/www/outreach/batpage.htm.*

Building Disinfection Byproducts Database

Decontaminating buildings and property after a terrorist release of anthrax requires the use of gas or liquid chemical agents that react with organic material. The extent of such reactions and the byproducts formed are currently unknown. It is essential to understand these processes to ensure environmental health and safety and to protect property of national and historical importance. This project addresses both the composition and persistence of chemical byproducts formed when the three most widely accepted decontamination

agents are used to treat common building and office items as well as more sensitive materials. A software application will provide on-scene commanders with the planning information they need for safe and efficient building decontamination operations.

Food Protection and Security Training for Critical and Overseas Facilities

A ten-module curriculum to train food management and terrorism response personnel to recognize, minimize, and manage the threat of terrorist activities is being developed. The courses will focus on critical issues involving food safety and security, global food supply chain management and security, managing traceability from farm to fork, identifying and handling potential threats, rapid diagnostic capabilities at the point of entry, defending against threats before the point of consumption, procurement and distribution management, establishing procedures for recovery, risk communication for leaders, and leadership in times of crisis.

Irradiation of Suspect Luggage

Destroying bioterrorism agents before they ever enter the country can prevent widespread human suffering, death, and significant financial loss to major sectors of our economy. Smuggling of agricultural pathogens from countries where they are endemic in carry-on or checked luggage is of particular concern. This task has developed guidelines for the treatment of high-risk passenger luggage with a radiation dose high enough to kill common bioterrorism agents without damaging most contents. The treatment would cause only a moderate delay in the movement of personnel and cargo through ports of entry. Currently this project is developing guidelines to help agencies assess the cost-benefit ratio for installation of luggage irradiation systems.

Personal Heat Stress Calculator

When wearing PPE in emergency situations, heat stroke can quickly kill or disable the wearer. The personal heat stress calculator will provide a work-rest cycle specifically tailored to the protective equipment being worn, the individual's health and fitness, the current environmental conditions, and the work to be performed. The application will run on a handheld computer and will have an easy-to-use interface.

Electrostatic Decontamination System

The proliferation of CB weapons makes it imperative to develop new technologies to provide effective, safe, and efficient decontamination systems to facilitate the timely restoration of operations after their use. The portable Electrostatic Decontamination System uses a patent-pending decontamination solution, activated by ultraviolet light, to rapidly and effectively neutralize CB agents with a minimum of environmental impact and logistical burden. The system is currently undergoing field evaluation.

Contact Information

cbrncsubgroup@tswg.gov

Explosives Detection

Mission
Identify, prioritize, and execute research and development projects that satisfy interagency requirements for existing and emerging technologies for explosives detection and diagnostics. Emphasis is on a long-term, sustained approach leading to technology for detection of improvised explosive devices and large vehicle bombs.

The Explosives Detection (ED) Subgroup identifies and develops technologies for detection and subsequent characterization of concealed explosive devices. These improvements are intended to enhance the operational capability for both military and civilian entry-point screening applications. The current chair of the ED Subgroup is a representative from the Transportation Security Administration (TSA).

Focus Areas
The ED Subgroup focus areas reflect the prioritized requirements of a broad range of interagency customers, including those responsible for physical security and forensic analysis. During FY 2003, the Subgroup focused on the following areas:

Stand-Off Detection
Explore technologies to address the Defense Technology Objective (DTO) for a stand-off detection capability of nitrogen-based explosives. This effort entails investigating unique physical and chemical phenomena indicative of the presence of explosives, exploring the limits of the sensor technologies responding to these phenomena, and identifying necessary technology enhancements. Current stand-off techniques are generally limited with respect to both stand-off distance and type of explosives that can be detected.

Short-Range Detection and Diagnostics
Improve current explosives detection and characterization capabilities. Emphasis is on equipment development to enhance personnel, baggage and vehicle entry point screening and diagnostic analysis of improvised explosive devices. Areas of concern include single event detection rate, traffic throughput, operational safety, and overall accuracy in identification of explosives.

Marking Agents
Improve the manufacture, incorporation and detection of marking agents currently required by law to be used in plastic explosives. The marking agent, 2,3-dimethyl-2,3-dinitrobutane (DMNB), is one of several high vapor pressure compounds that when added to a plastic explosive will significantly increase the detection probability of that explosive.

Canines
Explore training tools, protocols, and technologies that support and/or enhance canine detection of explosives. Emphasis is on methods to optimize canine/handler capabilities.

Membership

INTELLIGENCE COMMUNITY
U.S. DEPARTMENT OF DEFENSE
USA (TEU), USAF (ACC, AFRL, FPBL, FPSPO), USN (NAVEODTECHDIV, NCIS)
U.S. DEPARTMENT OF ENERGY
OS
U.S. DEPARTMENT OF HOMELAND SECURITY
TSA, USCG, USSS
U.S. DEPARTMENT OF JUSTICE
ATF, NIJ
U.S. DEPARTMENT OF STATE
DS
U.S. POSTAL SERVICE
USPIS

Cargo Screening
Develop enabling technologies and advanced prototype systems to provide an enhanced capability to detect explosives concealed in cargo. Areas of concern include detection rate, variability of cargo contents, operational safety, and impact on the stream of commerce.

Suicide Bomber Detection
Develop systems that detect the presence of improvised explosive devices concealed by persons engaged in suicide attacks against domestic and international Government installations and public facilities.

Selected Completed Projects

Canine Selection and Rearing

This project established a scientific basis on which to maximize canine operational effectiveness for purpose-bred dogs. Results from this study provided insights into both behavioral and predicative metrics that may be used for selecting future bomb detection dogs. Findings from this study demonstrated that early regimented interaction with humans, commonly referred to as puppy walking, positively impacted canine performance. The degree of human-canine interaction during rearing and the canine ability to manage stress were observed to be discriminating factors for performance, whereas puppy testing was not. Of the 32 canines used in this effort, 19 are currently deployed, three in the United States and 16 internationally. Information from this study is being incorporated into ongoing canine training programs to improve the success rate of the selection and training process. Requests for the study from Government agencies should be sent to the *edsubgroup@tswg.gov.*

Low Cost Production of Dimethyl Dinitrobutane

International treaty and U.S. Law require all plastic demolition explosives be manufactured with high vapor pressure marking agents. In response to this requirement, a manufacturing capability to produce the marking agent DMNB has been developed. This project specifically addressed the issues of quality, affordability and availability of DMNB manufacturing capability. The process will be shared with nations that produce plastic explosives, and are signatories to the Convention on the Marking of Explosives for the Purpose of Identification covered by the International Civil Aviation Organization (ICAO).

Trace Portal Assessment
An EntryScan III portal was deployed for an operational assessment at an overseas military installation. The feedback from this assessment resulted in improvements to the 68 trace portals deployed worldwide. The TSA recently acquired several additional EntryScan III portals for incorporation into their integrated technology testing program, supported by TSWG. TSA will complete these test trials in the summer of FY 2004. Additional information on the EntryScan III is available at *www.geindustrial.com/ge-interlogix/iontrack/prod_entryscan.html.*

Selected Current Projects

Millimeter Wave Imaging System
A stand-off detection capability for suicide attackers is being developed based on millimeter wave technology. The goal is to develop an imaging capability to resolve concealed threat objects at a stand-off distance of at least 10 meters. Prototype delivery and initial testing is planned for late FY2004.

Neutron Resonance Radiography (NRR)
NRR technology is being investigated as a possible alternative to currently deployed Computed Tomographic X-ray (CTX) systems. NRR is a detection approach that affords improved detection of explosives with reduced false alarm rates. Currently feasibility and design studies for the NRR technique are being conducted.

Quadrupole Resonance (QR) Personnel Screening Portal

A prototype QR portal has been developed for the detection of explosive devices concealed on personnel and is scheduled for an operational assessment in FY 2004. QR technology improves the detectability of bulk explosives, which are traditionally identified by trace detection methods. This non-trace explosive detection system for personnel screening at security checkpoints may be used where trace detection is not viable, e.g., in environments with high background levels of dirt or chemicals.

Contact Information
edsubgroup@tswg.gov

Improvised Device Defeat

Mission
Identify, prioritize, and execute research and development projects that satisfy interagency requirements to more safely and effectively render terrorist devices safe. Particular emphasis is placed on technologies to access, safely diagnose, and safely defeat terrorist improvised explosive devices (IEDs), improvised chemical and radiological devices, and vehicle-borne improvised explosive devices (VBIEDs).

The Improvised Device Defeat (IDD) Subgroup delivers advanced technologies, tools, and information to increase the operational capabilities of the United States military Explosive Ordnance Disposal (EOD) community; Federal, State and local bomb squads; and law enforcement tactical units to defeat and mitigate IEDs and VBIEDs. In collaboration with Federal, State and local agencies, the IDD subgroup identifies, validates, and prioritizes multi-agency user requirements through an ongoing requirements generation and prioritization process. IDD is currently chaired by a representative from the Federal Bureau of Investigation's (FBI) Bomb Data Center.

Focus Areas
The IDD Subgroup focus areas reflect the joint priorities of military and civilian responders. During FY 2003, the Subgroup focused on the following areas:

Access & Diagnostics
Develop advanced technologies that address the current Defense Technology Objectives for diagnostic analysis of improvised explosive devices in the areas of improved tools and equipment for access and diagnosis of terrorist devices.

Defeat
Develop advanced technologies to defeat IEDs, VBIEDs, and chemical and biological improvised devices. Emphasis is placed on developing low-cost solutions that are readily available to the bomb squad community. This focus area includes projects that are designed to increase stand-off capabilities, reduce collateral damage, and provide precision disruption and disablement capabilities and techniques.

Tactical Tools
Develop improved tools and equipment to increase the safety and effectiveness of Close Quarter Battle (CQB)/Special Weapons and Tactics (SWAT), EOD, and Bomb Squad Technicians during tactical response events. Projects in this field provide enhanced situational and environmental awareness; improved communications systems; tools to counter emergent threats; and software systems capable of finding, retrieving, and exchanging near real-time intelligence information across numerous networks and systems.

Membership

INTELLIGENCE COMMUNITY
STATE AND LOCAL
- COLUMBUS FIRE DEPARTMENT, BOMB SQUAD
- D.C. METROPOLITAN POLICE DEPARTMENT, BOMB SQUAD
- FAIRFAX COUNTY POLICE DEPARTMENT, BOMB SQUAD
- MARICOPA COUNTY SHERIFF'S OFFICE, BOMB SQUAD
- NATIONAL BOMB SQUAD COMMANDERS ADVISORY BOARD
- PRINCE GEORGE'S COUNTY FIRE DEPARTMENT, BOMB SQUAD

U.S. CAPITOL POLICE
U.S. DEPARTMENT OF DEFENSE
- DIA, NSA, USA, USAF (ACC, AFRL), USMC, USN (NAVEODTECHDIV, NCIS)

U.S. DEPARTMENT OF HOMELAND SECURITY
- TSA, USSS

U.S. DEPARTMENT OF JUSTICE
- ATF, FBI (BDC), NIJ

Remote Controlled Vehicles and Tools
Develop technologies that will improve the performance and reliability of robotic systems for the bomb squad technician. These technologies include advanced robotic platforms with improved manipulation capabilities, control systems, navigation technologies, payloads, and communications. The foundation of these systems is the TSWG's Common Architecture, which will for the first time enable all robotic components, regardless of the developer, to be plug-and-play. With the increasing diversity and complexity of the terrorist threat, it is becoming more vital that the bomb technician conduct as much of the mission as possible by remote means.

Emergent Threats
Characterize improvised explosive mixtures used by terrorist organizations and develop effective response procedures, tools, and equipment to counter the threat.

Information Resources
Develop information resources and delivery systems to enhance response capability. This area provides equipment performance results; reference database resources; operational response technology information; and automated information systems to improve tactical and operational response capabilities.

Selected Completed Projects

Critical Incident Response Technology Seminars (CIRTS)

Programs centered on bringing various subject matter experts directly to the bomb squads and EOD units have been held at regional seminars in the United States. These seminars included briefings on critical incident response technology and hands-on use of new tools in practical exercises or demonstrations. They have provided the Government with direct feedback from the EOD/bomb squad user. In FY 2004, seminars will concentrate on the military EOD community.

EOD Expeditionary Backpack

This project provided EOD technicians with the ability to safely carry explosives, detonators, disruptors, cartridges, and support tools necessary for EOD missions. Packs are currently deployed worldwide with Special Operations Forces, the Intelligence Community, and EOD units worldwide. They are commercially available through London Bridge Trading Company, Ltd. at *www.londonbridgetrading.com*.

Precision Micro Disruptor

This effort developed, fabricated, and tested the .357 caliber micro disruptor for precision render safe applications. This disruptor is a light-weight, small, and application-adaptable system that allows flexibility for the bomb technician where size limitations and collateral damage are considerations. The kit is commercially available from Ideal Products, Inc., Lexington, KY, (859) 255-7738.

Low-Cost Law Enforcement Robot Evaluation

EOD Performance, Inc.'s Vanguard robot was evaluated to see if it met the needs of the current user community. Vanguard was compared to other commercially available platforms identified in a NIJ study for Low-Cost Bomb Squad Robots. Vanguard MK I is currently being modified and upgraded. MK II will incorporate all improvements outlined in the most recent evaluation. The new system will exceed user requirements. The system is commercially available from EOD Performance, Inc. Information is available at *www.eodperformance.com*

Urban Explosive Storage Magazine

Bomb squads are required to store explosives in isolated, remote locations because of the explosive hazard they pose to the public. To decrease response time, a new type of explosive storage magazine was developed. This magazine enables bomb squads to store a full explosive kit safely and securely within city limits. The transportable magazine is capable of withstanding an internal detonation equal to 50 pounds of Net Explosive Weight (NEW) TNT equivalent with no external hazard. The magazine is being type-certified by the Bureau of Alcohol, Tobacco, Firearms and Explosives. This item is currently undergoing transition for full production and may be purchased from EQE International, Inc. at *www.absconsulting.com.*

Selected Current Projects

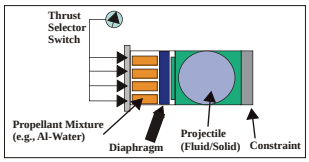
Suicide Bomber Standard Operating Procedure (SOP) Development

This project addresses an urgent request by the FBI and DHS/ODP to provide consensus-based response protocols to Federal, State and local bomb squads and first responders. The content will primarily be based on knowledge and expertise of international counterparts confronted on a daily basis by the threat of suicide bombers. It will include the minimum essential information, knowledge, procedures, tools, and references needed to prepare for, respond to, and mitigate consequences of suicide bombs and bombers in the U.S. The SOP will be distributed as a CD-ROM reference database (which can be updated) and distributed to Federal, State and local law enforcement agencies.

First Responder Automated Data Tool (FRAT)

The First Responder Automated Data Tool is an interactive database that a bomb technician can use to access tools and equipment when confronted with disabling vehicle IEDs or Large Vehicle Bombs (LVBs). These modules will include selected vehicle facts and graphical information to support decisions for assessment, access, removal, and disruption of IEDs. The database will also include modules regarding specific tools and information about their use, radiographic images of IED components, and blast and fragmentation hazard predictions. This tool can be used on any PDA, laptop, or desktop computer.

Variable Velocity Disruptor



This program will develop a low-recoil controlled disruption device capable of providing variable projectile velocities to more safely and effectively defeat IEDs. As robotic platforms have decreased in size to meet mission and deployment requirements of the bomb squad community, current disruptor systems routinely cause collateral damage to the robotic manipulator system because of the high recoil force of the disruptor. This variable-velocity disruptor cartridge will reduce the damage to robotic manipulators.

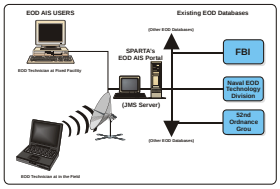
Remote Controlled Vehicles (RCVs) and Tools

A Next-Generation Explosive Ordnance Disposal Remote Controlled Vehicle (NGEODRCV), using TSWG's Common Architecture as the foundation, has been demonstrated. Each component is modular/scalable in design and is plug-and-play regardless of the developer. Cutting-edge technologies being developed include semi-autonomous mobility and manipulator behaviors; automatic pay-in-out tensionless fiber-optic systems having over 1 km range; and wireless communications with the capability of two-way audio and video transmission and an automatic recovery protocol in the event of loss of signal. Using an intelligent payload management approach, the payload shifts as necessary to execute difficult maneuvers.

Stand-off Connectivity and Control Unit

The Bomb Squad and EOD community requires increased remote capability without costly robotic modifications. The Stand-off Connectivity Control Unit (SCCU) is being developed to provide backward compatibility of existing sensor technology with legacy analog robotic systems. Existing digital equipment, such as the RTR-4 X-ray imaging system and an ADM-300 radiological monitor will be adaptable to the analog platform.

EOD Automated Information System (AIS)



The Automated Information System software will enable EOD operators and bomb technicians to search, retrieve, and exchange information across numerous networks and systems. The web-based AIS will speed the ability to assess, render safe, and dispose of IEDs and will be accessible from a fixed facility or from a laptop in the field.

Contact Information

iddsubgroup@tswg.gov

Infrastructure Protection

Mission
Identify, prioritize, and execute research and development projects that satisfy interagency requirements for the protection and assurance of critical Government, public, and private infrastructure systems required to maintain the national and economic security of the United States.

The Infrastructure Protection (IP) Subgroup provides capabilities to ensure the uninterrupted service of the infrastructure systems that are vital to maintaining the national and economic security of the United States. These critical systems include control systems for electric power, natural gas, petroleum products, and water; telephone, radio, and television; ground, rail, and air transportation facilities; and cyber communications networks. IP research and development reflects the multivariate threat to complex and interdependent systems, subsystems, and components of the nation's infrastructure. Solutions include conventional security measures plus those offered by emerging technologies. Representatives from the Department of Defense and the Federal Bureau of Investigation co-chair the IP Subgroup.

Focus Areas
The IP Subgroup focus areas reflect the prioritized requirements generated with respect to the critical aspects of the nation's infrastructure. During FY 2003, these focus areas were:

Physical Protection
Standardize methodologies and decision aids for vulnerability analysis and enhanced protection of critical elements to secure the nation's infrastructure. These include power generation and transmission, water supplies, and health services. By understanding the dynamics of complex critical infrastructures, secure operating methodologies and strategies can be developed to prevent and mitigate widespread failures caused by cascading and interactive network effects. The linkages and infrastructure dependencies are complex. This research will evaluate dynamic behavior models of cascading effects, develop common standards and practices in and between critical infrastructures, and investigate system vulnerabilities to various threats.

Cyber Security
Provide detection, prevention, response, and alert capabilities to counter cyber attacks and harden computer systems. Our society increasingly relies upon new information technologies and the Internet to conduct business, manage industrial activities, engage in personal communications, and perform scientific research. The complexity and sophistication of information technologies and their widespread integration increase the likelihood of unforeseen vulnerabilities. Unprecedented opportunities are created for criminals, terrorists, and hostile foreign nation-states to steal money or proprietary data, invade private records, conduct industrial espionage, or cause vital infrastructure elements to cease operations. The prevention and mitigation of threats to computer networks is vital to homeland security.

Membership

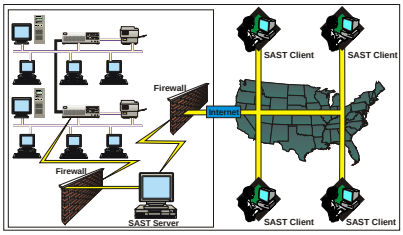
ENVIRONMENTAL PROTECTION AGENCY
NUCLEAR REGULATORY COMMISSION
PORT AUTHORITY OF NEW YORK/NEW JERSEY
U.S. DEPARTMENT OF AGRICULTURE
  FS
U.S. DEPARTMENT OF COMMERCE
  NIST
U.S. DEPARTMENT OF DEFENSE
  CID, DTRA, JPO-STC, USA (CE), USAF (OSI)
  USMC (CIP), USN (NCIS, NSWC)
U.S. DEPARTMENT OF ENERGY
  OEA, OS
U.S. DEPARTMENT OF HOMELAND SECURITY
  FEMA, FPS, NIPC, ODP, PSD, S&T, TSA, USSS
U.S. DEPARTMENT OF JUSTICE
  FBI
U.S. DEPARTMENT OF TRANSPORTATION
  FAA, Volpe

Selected Completed Projects

Communications Firewall

The Communications Firewall provides communication security by actively monitoring all telecommunications traffic entering and leaving a Sensitive Compartmented Information Facility (SCIF). The system is currently configured for a Nortel CTS switch and provides a capability for any anomaly to be reported via secure connection to a control center responsible for facility security. The Communications Firewall monitors alarm circuits, analog and digital phones, trunk lines (fiber and metallic), STU-III, fax (secure and non-secure), and modems and allows for remote programming, remote software upgrades, and monitoring of active circuits. This system is available from Applied Signal Technology, Inc., at *www.appsig.com.*

Systems Administrator Simulation Trainer (SAST)



The Systems Administrator Simulation Trainer (SAST) is the equivalent of a flight simulator for systems administrators. SAST provides an experience-based, distance-learning environment for a broad range of host and network-based computer security tools and techniques. SAST tests the ability of trainees to defend against a diverse cyber threat environment by applying a variety of cyber offensive tools. SAST provides system administrators with real-world experience in resisting, responding to, and recovering from cyber attacks. This item is currently being transitioned by the Pacific Northwest National Laboratory (PNNL). Additional information is available at *www.pnl.gov.*

Alert Trend Change Detection Tool (ATrCT)

The Alert Trend Change Tool (ATrCT) improves analysts' understanding of hostile alerts and indications of scanning attacks detected on computer networks. ATrCT uses an algorithm to analyze data collected by both freeware and custom software sensors to help protect a network against malicious autonomous agents. ATrCT provides analysts with warning indicators when sensors detect increased scanning activity against a particular service or an increase in the frequency of a particular alert. The second Code Red outbreak in August 2001, for example, was characterized by a near doubling of the number of attacking machines each hour in the early hours of the outbreak. ATrCT detects and reports this type of behavior to analysts, who in turn can then react quickly to prevent infection or repair infected machines. This item is being licensed through the Massachusetts Institute of Technology/Lincoln Laboratory (MIT/LL). Additional information is available at *www.ll.mit.edu.*

Selected Current Projects

Supervisory Control and Data Acquisition Protection II (SCADA)

A prototype cryptographic module will meet the needs of Supervisory Control and Data Acquisition (SCADA) users. The cryptographic module's ability to safeguard transmissions between master and remote terminal units and to deny unauthorized data transmissions or intrusions will be tested and evaluated. The software/hardware configuration is designed to

be acceptable to both users and manufacturers, economically feasible, and suitable for installation in existing systems.

Incident Command Information Tool (ICIT)
The Incident Command Information Tool (ICIT) is based on the current U.S. Geological Survey Hydrographic Database that allows an incident commander to analyze and react quickly to chemical and/or biological contaminants that are introduced into natural and engineered water sources. The models will simulate the propagation of the constituents and will assist incident commanders in minimizing contamination, deploying resources, and notifying local authorities and citizens to the potential dangers.

Virus Propagation Analysis Tool (VPAT)
The Virus Propagation Analysis Tool (VPAT) will assist system administrators in planning and protecting their communication networks from the harmful effects of malicious code by providing a better understanding of how viruses propagate across the Internet. The tool will analyze the severity of infection, identify weak points in a network's defense, and suggest strategies for recovery.

Insider Threat Countermeasures Toolkit (ITCT)
The Insider Threat Countermeasures Toolkit (ITCT) is a suite of tools that will non-intrusively monitor secure computing resources in order to mitigate the threat of insider compromise of sensitive information. The system will, for example, monitor, log, and control access to information resources and deny access to unauthorized users.

Contact Information

ipsubgroup@tswg.gov

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 (IS&F) Subgroup supports research and development projects to 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. Representatives from the U.S. Secret Service (USSS) and the U.S. Postal Service (USPS) co-chair the subgroup.

Focus Areas
The IS&F Subgroup focus areas reflect the prioritized requirements of the military and civilian law enforcement communities. During FY 2003, these focus areas were:

Digital Evidence Examination
Develop computer forensic hardware, software, decryption tools, and digital methods to investigate cyber-terrorism. New projects in this field are also developing advanced methods to extract and enhance audio recordings and video images from surveillance sources. This area includes identifying terrorists' use of computer systems and media and obtaining the maximum amount of evidence from them.

Energetic and Hazardous Materials Examination
Improve methods for the examination of energetic and hazardous materials used in assessing the size, construction, and composition of explosive devices or other energetic hazardous materials at post-blast scenes. This focus area emphasizes the identification and analysis of explosive residue and other trace evidence present at blast scenes, especially those requiring rapid protection and processing, to preserve the evidentiary value.

Forensic Biology and Molecular Biochemistry
Develop advanced analytical methods used on biological evidence found at terrorist scenes to make identifications and extract information such as origin or age. The use of DNA to identify or profile persons receives special interest because of its highly discriminative and sensitive properties for individualization and comparison. This focus area also looks at locating the geographic origin of organic material based on molecular stable isotope ratios.

Friction Ridge Analysis
Improve friction ridge analysis capabilities, especially latent print techniques, used in terrorism cases. Areas of special emphasis are processes involving automation of multiple techniques that

Membership

ENVIRONMENTAL PROTECTION AGENCY
FEDERAL RESERVE BOARD
INTELLIGENCE COMMUNITY
U.S. DEPARTMENT OF COMMERCE
  NIST (OLES)
U.S. DEPARTMENT OF DEFENSE
  AFIP, CCI, DTRA, NSA, PI, USA (CID), USMC (CBIRF), USN (NCIS)
U.S. DEPARTMENT OF ENERGY
  OS
U.S. DEPARTMENT OF HOMELAND SECURITY
  FEMA, TSA, USSS
U.S. DEPARTMENT OF JUSTICE
  ATF, DEA, FBI, NIJ (NCFS, NFSTC), NSA, USMS
U.S. DEPARTMENT OF TRANSPORTATION
  FAA

are tedious, cumbersome, toxic, expensive, perishable, and non-portable. This encompasses efforts to create better and more sensitive ways to visualize and develop latent prints with lasers or more versatile and affordable reagents. The better comprehension of latent prints, their specific features, and chemical content, as well as the scientific validation of fingerprint examinations are also of interest.

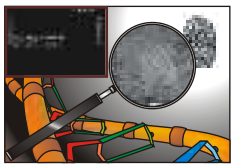
Questioned Document Examination
Improve questioned document examination capabilities through the development of more sensitive and discriminating techniques of document and handwriting analysis, standardized identification criteria, and establishing a legal scientific basis for these examinations. Questioned document examinations include forgeries, tracings, disguised handwritings, and writing or typing in different languages and sets of characters. The development of software for identifying counterfeit and genuine documents and matching documents by handwriting analysis and pattern recognition algorithms also fall in this focus area.

Surveillance Technology
Produce new and advanced surveillance devices for use by law enforcement or intelligence operations to support later prosecution. These technologies may be categorized by the nature of the technology (infrared, X-ray, visual, audio/speech), the type of data derived (visual, aural, digital), or the awareness of the target being surveilled. This focus area includes projects to improve polygraphy or to develop new methods and equipment for the detection of deception, such as thermal facial imaging and laser Doppler vibrometry.

Trace Evidence Analysis
Develop and enhance trace evidence analysis capabilities to include methods for the recovery, comparison, analysis, and interpretation of small, often microscopic, fragments of materials that transfer among and persist on people, places, and objects. Trace evidence is a wide-ranging field that also encompasses fibers, paint, glass, hair, soil, metal fragments, and chemical residues.

Selected Completed Projects

DNA Recovery from Processed Fingerprints



Forensic researchers have developed improved techniques for extracting and identifying DNA from partial, chemically developed prints. To obtain sufficient visualization, partial prints currently must be subjected to severe chemical conditions often resulting in minimally testable amounts of DNA. This project has optimized protocols for short tandem repeat (STR) DNA, mitochondrial DNA, and Alul DNA conforming to guidelines required for search and identification within the national DNA identification database. This DNA protocol is available through the Bode Technology Group at *www.bodetech.com*.

Morphological Reconstruction of Shredded Documents and Media

Engineers developed a method to reassemble shredded paper recovered from a crosscut shredder in order to reconstruct the original documents. After scanning the shredded pieces, an automated process reconfigures them to their original orientation. This capability has already successfully reconstructed documents for law enforcement agencies. This system is available from Pacific Northwest National Laboratory at *www.pnl.gov.*

Magnetic Nanoflake Fingerprint Powder

This project produced a superior magnetic fingerprint powder by making smaller and better-shaped particles. The flatter particles with sizes in the nanometer range adhere much more readily to latent prints because of their flake shape and better surface area-to-weight ratio. The flakes come in various colors, including fluorescent, for use on all types and colors of substrates. Additionally, an electro-magnetic application wand has been produced that has multiple "brush" sizes to improve the dusting process. Federal law enforcement agencies, who field tested the system, provided very positive feedback. The University of Texas at Austin is commercializing the product. For additional information, visit *www.utexas.edu/research/cemd/html/latent_fingerprint_detection.htm.*

Glass Evidence Data Reference

Researchers created a comprehensive glass evidence reference that allows forensic scientists to analyze and compare known and unknown samples. The automated reference provides trace element profiles of float, container, and headlamp glass, permitting a possible determination of origin. The project established new highly discriminative analytical techniques through the use of inductively coupled plasma and isotope dilution mass spectrometry. The reference expands the ability to positively match and eliminate glass evidence. The data reference is available for use by government agencies. Requests should be sent to *isfsubgroup@tswg.gov* for coordination with the International Forensic Science Institute at Florida International University.

Computer Forensics Processing Suite

This task produced a "next generation" computer forensics software examination tool for multiple platforms. It included new capabilities beyond present day commercial technology such as RAID pattern analysis tools and emulation drivers. The tool catalogs and summarizes the entire contents of the hard drive, beyond what is done by the computer's own operating system. This tool is available for law enforcement agencies from Veridian Information Systems at *www.veridian.com.*

Fingerprint Optimization Development of Paper

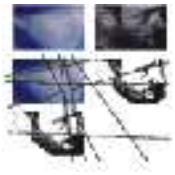
Forensic experts produced a set of new optimal latent print development procedures. They examined the interaction between paper, deposited latent fingerprints, environmental conditions, and numerous developing reagents to produce advanced techniques that made previously unusable latent prints identifiable. The researchers at The Hebrew University of Jerusalem (*sites.huji.ac.il/applsci/ac/facult.htm*) published their results in the *Journal of Forensic Science* (Azoury, M. et al. ESDA Processing and Latent Fingerprint Development: The Humidity Effect. J Forensic Sci, May 2003, Vol. 48, No. 3). These advanced development processes have been successfully applied in sensitive cases.

Selected Current Projects

Gunshot Residue (GSR) Analysis of Novel Ammunition

This project focuses on generating a scientific reference to correlate new ammunition, chemical gunpowder mixtures, and post-firing residue to link a shooter with a particular weapon and ammunition. As ammunition manufacturers are rapidly changing production methods to make environmentally friendly and novel (frangible, limited penetration, and other) ammunition with new chemical components, traditional GSR testing is becoming less useful. Research also will determine if commercially available GSR collection kits can be used to identify these new components and elements, such as tungsten and tin.

Computer-Aided Forensic Facial Recognition



Forensic scientists are developing enhanced methods for photogrammetric matching of faces to confirm or rule out a person's identity by facial measurements. These methods will aid criminal investigations and prosecutions and will improve security systems by rapidly comparing facial images taken in a real environment to images of known and suspected terrorists.

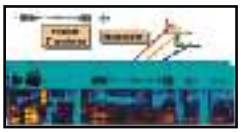
Improved Audio Tape Enhancement

Counterterrorism investigations require better techniques of audiotape enhancement that produce final processed audiotape of evidentiary quality, either for court presentation or intelligible interpretation. This task will improve extremely poor quality audiotapes by performing speaker separation, reducing or eliminating random noise, and suppressing pulsed noise.

Improved Video Tape Enhancement

This task will design and develop new videotape enhancement algorithms and processes that produce final processed videotapes of evidentiary quality. The final result will be advanced techniques for correcting the effects of motion blurring, out-of-focus lenses, and overused tapes.

Reliable Audio Voice Identification



This task will develop an advanced voice identification system and reference capable of comparing a new/unknown voice sample to a collection of known voice samples. Phone-based speaker recognition technology is one component of this new system.

Range Evaluated Improvised Explosives

Scientists are validating the detonation properties and post-blast forensic signatures of specified improvised explosives used by terrorist groups or made from open sources. This project will create a forensic compendium of studied formulation properties that will extend the ability to analyze what occurred at explosion scenes.

Contact Information

isfsubgroup@tswg.gov

Personnel Protection

Mission
To identify, prioritize, and execute research and development projects that satisfy interagency requirements for equipment and systems that alert and prevent attacks on VIP protectees. This includes hardware and tools that provide security to both the VIPs and their protectors. Inherent in this development is additional emphasis on life safety and emergency response equipment. The Personnel Protection Subgroup is chaired by a representative from the United States Secret Service (USSS).

The Personnel Protection (PP) Subgroup focuses on the development of prototype hardware, systems, personnel protection equipment, and diagnostic and reference tools and standards that will support greater security for VIPs who are highly visible in public environments and thus subject to terrorist attempts on their lives. In order to be effective, personnel who are charged with the safety of these VIPs must also have protective equipment that will prevent injury and tools that will improve their effectiveness. These developments benefit Federal, State, military, and local law enforcement personnel who are charged with the protection of VIPs. These technologies and tools also have application for the protection of law enforcement and military personnel who work in high-threat environments.

Focus Areas
The PP Subgroup focus areas reflect the prioritized requirements of the VIP protection community. During FY 2003, the Subgroup focused on the following areas:

Vehicle Protection and Performance
Improve the safety of armored passenger vehicles and effectiveness of the protection of passengers. This includes the development of vehicle system upgrades that will enhance the performance and reliability of the vehicles in a broad range of operational environments. It also supports the validation of the designs of existing countermeasures.

Transparent Armor Development
Develop and validate tools that will predict the performance of transparent armor and support the assessment of advanced designs. This includes evaluations of armors and designs that will protect against a broad range of threat projectiles. Because of the significant weight penalty of transparent armor, this area also focuses on the development of advanced lightweight transparent armor that will provide substantial reductions in the weight and thickness necessary to obtain the required protection.

Individual Protection Systems
Individual protection systems include personal body armor and methods for the defense of personnel assigned to protection details. Many of the developments will also support the protection of law enforcement officers. This focus area emphasizes improving the performance of body armor, understanding its limitations, and providing associated systems that will improve the comfort of and effectiveness for the wearer. It also includes technologies that identify situations where

Membership

U.S. DEPARTMENT OF COMMERCE
NIST (OLES)
U.S. DEPARTMENT OF DEFENSE
USA (Natick RD&E Center, TACOM), USN (SWC)
U.S. DEPARTMENT OF ENERGY
OS
U.S. DEPARTMENT OF HOMELAND SECURITY
USSS (SSD, TSD)
U.S. DEPARTMENT OF JUSTICE
NIJ
U.S. DEPARTMENT OF STATE
DS
U.S. CAPITOL POLICE

protection personnel and the VIPs under their protection are in need of support or assistance.

Emerging Threats
Develop systems that identify indications of and protect against a potential sniper attack. The technologies will provide locating information and appropriate countermeasures. This area will also address emerging threats to VIPs and will provide methods to address those threats.

VIP Installation Protection
Develop technologies that support the indications and warnings of potential threats directed against critical installations that are occupied by senior government officials. Included in this area are appropriate countermeasures that will enhance the safety of the installations from terrorist actions.

Selected Completed Projects

Portable Transparent Shield for Ballistic Protection

Portable, transparent shields are used to protect high-profile personnel from attack by firearms and small explosive devices. The shortcomings of the previous shield system includes the use of transparent armor glass that loses transparency over time, difficulty and safety issues associated with erecting the shield, and a reluctance to deploy the shield because of its unpleasant appearance. To overcome these deficiencies, a safer design has been developed that uses gas springs to help support the weight of the upper part of the shield, allowing safer set up. Seven shields have been delivered for operational use. The shield was developed and manufactured by Applied Research Associates, San Antonio, TX. Information is available at *www.ara.com.*

Body Armor Cooling

An under-armor cooling system was developed and found to be effective in maintaining the wearer's body temperature at safe levels when wearing body armor or other protective clothing. The system consists of a shirt worn against the skin with embedded cooling channels and a heat exchanger that allows circulation of cooling water. A cooling bladder, worn in a CamelBak™ pack, houses the batteries, thermostatic control valve, and heat exchanger. When the ice used for cooling melts, it can also be used for drinking water. The system is lightweight and provides comfort to wearers for several hours without having to replace the cooling media. The system is available from Technical Products, Inc., Waltham, MA. For additional information, send requests to *ppsubgroup@tswg.gov.*

Selected Current Projects

Armored Passenger Vehicle Standards
This task is conducting a thorough evaluation and development of standards for armored passenger vehicles, addressing protection, and criteria for ballistic, blast, transparent armor, performance, and quality control. As these areas are developed, they will be integrated into a standard that can be used to define protection levels for typical armored vehicles.

Body Armor Aging and Environmental Effects

Concerns for potential deterioration of body armor over time resulted in a thorough analysis of several factors that could affect the long-term protection of a variety of body armor types. The effect of high temperature was observed to significantly reduce the protection offered by several types of armor. Accelerated aging and specialized testing are being used to evaluate the performance and to identify proper care of body armor to reduce environmental effects. It is anticipated that this project may eventually lead to the development of criteria for removing potentially deteriorated armor from use prior to its scheduled warranty or planned retirement.

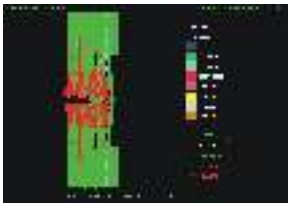
Instantaneous Personnel Protection System (IPPS)

The IPPS will stop a bullet before it hits the target by erecting a protective shield in the bullet's path. A proof-of-concept has been demonstrated. A robust system is being designed to protect against a broad range of threats. Critical enabling technologies needed for an operation system are being developed. This project includes the assessment of appropriate shield material, a shield deployment system that meets timing requirements, and a detection system that will have a very low or no false alarm rate. The integrated system will be an unobtrusive, automated bullet detection and countermeasure system.

Large Spinel Armor Development

Spinel transparent armor is a ceramic that has potential to provide equivalent ballistic protection with reduced weight and thickness for the same level of protection as standard glass armor. The development of the armor in practical sizes will be evaluated to determine how it compares to Aluminum-Oxynitride (ALON), another ceramic that also offers reduced transparent armor weight.

Transparent Armor Model Validation



In a joint U.S.-U.K. project, a design model for predicting the performance of transparent armor was developed. This model will be validated against actual performance results by conducting ballistics testing on specific types of targets to demonstrate the model's accuracy. The results of the validation testing will be incorporated into the model to upgrade its capability. A valid design model will offer a lower cost approach to designing transparent armor than is currently used.

Magshoe

The Magshoe project was developed in a joint U.S.-Israeli program to provide a system that could quickly screen the shoes of people going through checkpoints for the presence of unusual metal concentrations and provides an alert to the operator. This system will allow faster throughput of people at checkpoints and will identify individuals requiring more detailed screening.

Deployable Protective Armor

There are situations where temporary protective armor must be used to ensure the safety of VIPs. This project will develop a relatively lightweight system that can be easily deployed to support requirements of protective detail personnel. This deployable armor will be modular in nature to accommodate a variety of applications and will also be able to be used in other law enforcement applications. It will provide protection against typical rifle threats (NIJ Level IV) and can be adapted to protect against higher threats.

Contact Information

ppsubgroup@tswg.gov

Physical Security

Mission
To identify, prioritize and execute research and development projects that satisfy interagency requirements for physical security support to protect personnel, equipment, and facilities against terrorist attack.

The Physical Security (PS) Subgroup identifies and develops capabilities for the protection of miliary and civilian personnel, and property from terrorist attack. The subgroup develops prototype hardware, software, systems and protocols for technical and operational evaluation by Federal, State and local user agencies and foreign partners. A DoD representative of the United States Naval Forces Europe chairs this subgroup.

Focus Areas
The PS Subgroup focus areas reflect the prioritized requirements of the physical protection community. During FY 2003, the Subgroup focused on the following areas:

Blast Mitigation
Develop blast mitigation technology necessary to address blast debris hazards and prevent structural collapse, the primary sources of injury and death. This focus area seeks design and construction solutions for new buildings, as well as retrofit techniques for existing structures.

Entry Point Screening
Develop technologies, techniques and procedures to protect installations from terrorist threat devices and other contraband in vehicles, ships, cargo, mail, or carried on or in personnel entering protected facilities. The threats include explosives, weapons, toxic chemicals, radiological and nuclear materials, and other contraband. The solutions sought must be safe, increase throughput, improve detection rates while minimizing the incidence of false alarms and reduce the number of security force personnel required.

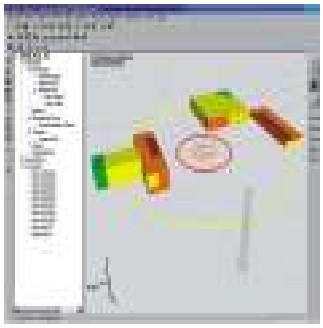
Intrusion Detection, Assessment & Delay
Develop improved intrusion detection systems, video alarm-assessment systems, specialized intrusion-delay barriers and subsequent armed response capabilities for protecting outer perimeters, building perimeters, key assets and personnel from terrorist attacks. This focus area emphasizes prototype security systems with fewer false alarms, improved reliability, higher probability of detection and assessment, and lower operation and maintenance costs. The overriding goal is to provide more effective response capabilities with higher probabilities of neutralizing the adversaries with reduced hazards for responding personnel.

Membership

FEDERAL RESERVE BOARD
INTELLIGENCE COMMUNITY
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
NUCLEAR REGULATORY COMMISSION
PORT AUTHORITY OF NEW YORK/NEW JERSEY
SUPREME COURT OF THE UNITED STATES
U.S. DEPARTMENT OF DEFENSE
CENTCOM, DTRA, EUCOM, JCS, JFCOM, NSA, OUSD (AT&L), USA, USAF, USMC, USN
U.S. DEPARTMENT OF ENERGY
NNSA, OS
U.S. DEPARTMENT OF HOMELAND SECURITY
BTSD, FLETC, TSA, USCG, USSS
U.S. DEPARTMENT OF JUSTICE
ATF, FBOP, NIJ
U.S. DEPARTMENT OF STATE
DS
U.S. DEPARTMENT OF TRANSPORTATION
OIS
U.S. POSTAL SERVICE
USPIS

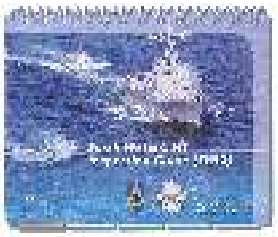
Selected Completed Projects

Blast Effects Estimation Model (BEEM)



BEEM integrates several sophisticated physics models that complement each other in assessing the blast damage to buildings and personnel for various explosive device scenarios. This project combines the best features of the existing Force Protection Tool and AT Planner into a single software application interoperable with the Site Profiler application of the Joint Vulnerability Assessment Toolkit Suite. The software design supports the incorporation of future improved physics models. The U.S. Army Corps of Engineers is managing the distribution of the current software release and further development. Visit the BEEM website at *beem.pecp1.nwo.usace.army.mil/* for more information, software downloads, and product support.

Small Watercraft Inspection Guide (SWIG)



TSWG published a pocket-sized reference guide to assist U.S. security forces in screening small boats for improvised explosives and other contraband. TSWG developed the SWIG based on the success of the Vehicle Inspection Checklist (VIC), a similar guide for land-based entry point screening personnel with over 100,000 copies distributed thus far. The Government Printing Office currently distributes both the SWIG and the VIC. For further information about both publications, visit the TSWG website at *www.tswg.gov/tswg/prods_pubs/prods_pubs.htm.*

Glass Penetration Model

This product is a human injury prediction model that determines the potential severity of injuries based on window characteristics, blast parameters, and the location of a person relative to the window. The model approximates the effects of multiple hits with glass shards and has already proved to be a successful planning tool. The Bureau of Alcohol, Tobacco, Firearms and Explosives has constructed a glass wall at its new facility using the glass penetration model. Inquiries about the Glass Penetration Model should be directed to the Physical Security Subgroup at *pssubgroup@tswg.gov*.

Barrier Impact Response Model (BIRM 3D)

BIRM 3D software permits engineers and physical security managers to assess the effectiveness of existing and planned barrier designs in stopping terrorists trying to use cars and trucks to penetrate the protected facility perimeter. Finite element 3D software models of selected security barriers and threat vehicles (based on DYNA3D) are available in the database to make it easy to use. Actual crash test data was used to validate the results of the models. Inquiries about this tool may be sent to *pssubgroup@tswg.gov.*

Selected Current Projects

Stabilized Panoramic Intruder Detection and Recognition (SPIDER)

TSWG developed the SPIDER in conjunction with its partners in Israel. The project focused on developing an automatic long-range surveillance system to locate intruders using day and night video imaging. U.S. Central Command field-tested two prototype systems in 2003 in an operational military environment locating human and vehicular targets at extended ranges not achievable with other systems and under adverse conditions. Further field-testing of these prototypes is scheduled for 2004. Also in 2004, TSWG anticipates the delivery of a third prototype system with improved capabilities. The Department of Energy will field-test this new prototype in 2005. TSWG plans to retrofit the first two prototypes with these improved capabilities. For inquiries about the SPIDER system, please visit *www.controp.co.il*.

Ground Surveillance Radar for Perimeter Intrusion Detection

Major U.S. airports use existing airport surface detection equipment ground surveillance radar to track the movement of aircraft and vehicles. A prototype Airport Security Display Processor (ASDP), currently in development will display ground surveillance radar and existing perimeter intrusion detection systems data at one central security processing station. The ASDP's combined real-time data will provide airport security forces with improved capability for detecting perimeter intrusions. The ASDP is scheduled for field-testing at John F. Kennedy International Airport over the next year. Planned expansion upon this project includes the use of commercially available sensors and closed-circuit television, other perimeter intrusion detection subsystems, and enhanced communications subsystems in 2004. This will provide security forces with improved perimeter intrusion detection capability, situational awareness, and command and control.

Explosive Loading Laboratory Testing

The Explosive Loading Laboratory Testing program has two primary objectives. First, the University of California, San Diego (UCSD) will develop a laboratory-based explosive loading simulator to perform fully repeatable, controlled blast load simulations on critical structural elements (e.g., columns, beams, girders, walls, and floors) and on potentially lethal non-structural elements such as glass windows, masonry walls, and curtain walls. Second, UCSD will employ the simulator to generate quality data for computer model validations for verification in a parametric investigation of blast retrofit designs including the use of Fiber Reinforced Polymer (FRP) composites, and for optimization of hardening technologies. Comparisons with field explosive testing will validate the blast simulator data.

Advanced Vehicle Driver Identification System (AVIDS)

TSWG is developing and commercializing AVIDS to expedite the screening process at vehicle entry points by providing force protection personnel with near real-time access to control databases. Entry point screening personnel can check a vehicle and verify the occupants

against the database in less than three seconds over a secure wireless LAN. A currently fielded prototype network can cover eighteen square miles and up to eight vehicle entry points. AVIDS integrates weigh-in-motion, RF tags, and license plate reader modules for vehicle identification. Biometrics modules are used to verify driver and passenger identity against another database established using an enrollment process. The modular system allows users to select only those components needed at their particular facility. Additional modules to be added in the near future include an automated under-vehicle inspection system and an Arabic license plate reader. Two stand-alone systems are planned for installation at overseas U.S. military facilities.

Drive-By Backscatter Imaging Van

This effort will demonstrate the capabilities of a utility van equipped with a backscatter X-ray imaging system. While slowly driving past vehicles or objects of concern, the van will unobtrusively screen them for explosives and other contraband. Future refinements will include a remote operational capability and a radiological threat detection capability. The prototype has undergone initial testing with final delivery to DoD and other government agency users in Spring 2004.

Blast Mitigation Database Conversion and Optimization

This project will develop and deliver a concise, easy-to-use database which includes the current blast mitigation test reports in a convenient electronic format. The database, the first of its kind, will have both military and civilian applications in building planning, design, construction and renovation. New reports can be easily added as new blast test data becomes available in the future. All the blast effects models, algorithms and formulas used in the reports will be fully operational and available as part of the system.

Contact Information

pssubgroup@tswg.gov

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 (SC&OS) Subgroup identifies high-priority user requirements and special technology initiatives focused primarily on countering terrorism/offensive operations. The research and development projects supported by this subgroup include reducing the capabilities and support available to terrorists and enhancing U.S. capabilities to conduct retaliatory or preemptive operations. A representative from the Intelligence Community chairs the subgroup.

Focus Areas
The SC&OS Subgroup focus areas reflect the prioritized requirements of the Intelligence Community. During FY 2003, the Subgroup focused on the following areas:

Traditional Surveillance
Success in countering terrorism often depends on the quality of intelligence collection. These programs include improving capabilities for the collection and enhancement of video, imagery, and audio surveillance.

Analytic Surveillance
The purpose of programs in this focus area is to improve the means for detecting terrorists by developing automated tools for terrorist identification using biometrics, pattern recognition, voice and speaker recognition, and database technologies.

Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR)
The means to locate, identify, and track terrorists and terrorist activities is extremely critical. C4ISR programs focus on developing and improving that ability through programs and initiatives such as tagging, tracking and locating (TTL); special sensors; and covert communications.

Membership

INTELLIGENCE COMMUNITY
U.S. DEPARTMENT OF DEFENSE
DIA, NRO, NSA, SOCOM
U.S. DEPARTMENT OF HOMELAND SECURITY
USSS
U.S. DEPARTMENT OF JUSTICE
FBI

Information Operations Support (IOS)
IO programs exploit digital information age technology by developing and improving tools to degrade, disrupt, deny or destroy adversary information and information systems.

Program Highlights

SC&OS programs are classified or highly sensitive. Program requirements, the success of programs, and specific program capabilities cannot be discussed in an open document.

Contact Information
scossubgroup@tswg.gov

Tactical Operations Support

Mission
Identify, prioritize and execute research and development projects that satisfy DoD and interagency user requirements to develop equipment and systems to support specialized force offensive operations directed against terrorist activities and groups. The use of non-sensitive prototype hardware for state and local law enforcement agencies is considered for transition and commercialization.

The Tactical Operations Support (TOS) Subgroup supports counterterrorist tactical operations, particularly those performed by specialized tactical forces trained for assault operations. The subgroup supports technology development activities, which provide a foundation for subsequent advances, and the development of prototype special equipment designed to facilitate more effective execution of various tactical missions. The principal users of the technology developed by this subgroup are the Military Special Forces, the FBI-Hostage Rescue Team, DOE nuclear security teams, Department of State, and the U.S. Secret Service. A representative from the DoD chairs this subgroup.

Focus Areas
The TOS Subgroup focus areas reflect the prioritized requirements of offensive counterterrorism forces. During FY 2003, the Subgroup focused on the following areas:

Advanced Imaging Systems
Advanced imaging systems focuses on the development of systems to improve night and reduced visibility and imaging in all environments. The objective is to obtain the best images in reduced lighting conditions and provide systems that will enable tactical forces to operate more effectively.

Specialized Access Systems
This area emphasizes the development of technologies and systems that will assist tactical assault forces in accessing objectives, evaluating tactical options, and supporting efficiencies in operations, while providing added safety for personnel.

Membership

U.S. DEPARTMENT OF DEFENSE
SOCOM
U.S. DEPARTMENT OF ENERGY
OS
U.S. DEPARTMENT OF HOMELAND SECURITY
USSS
U.S. DEPARTMENT OF JUSTICE
FBI (HRT)
U.S. DEPARTMENT OF STATE
DS

Chemical and Radiation Detectors
The tactical chemical and radiation detectors area focuses on the development of chemical and radiological instruments that are specifically designed to support the tactical user in the field. As such there are specific features included that consider the need for reduced size, greater robustness and covertness needed by tactical users. This development is done in close coordination with the CBRNC subgroup.

Offensive Systems
The offensive systems focus area emphasizes development of technologies to address requirements for equipment and systems that will enhance the effectiveness of small offensive tactical teams in specialized operations.

Tactical Communications Systems
This area emphasizes providing greater communications flexibility to tactical forces. The major focus is on reducing the size of equipment and improving operator mobility and efficiencies.

Program Highlights

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

Contact Information
tossubgroup@tswg.gov

Appendices

BAA Information Delivery System (BIDS)

The TSWG seeks technology solutions that address operational and technological shortfalls identified by Government agency users at least once annually. User requirements are disclosed in a solicitation format called a Broad Agency Announcement or "BAA." The BAA enables the Government to solicit industry, academia and Government Laboratories for innovative research and development solutions to these requirements. The BAA is advertised in the Federal Business Opportunities at *www.fedbizopps.gov*. The FedBizOpps site directs interested bidders to the appropriate web address where additional information for submitting a proposal is posted. Each open BAA is always posted at the TSWG program website: *www.bids.tswg.gov*. The application at this website is called the BAA Information Delivery System or "BIDS." BIDS provides an electronic submission and record evaluation capability for receiving and evaluating responses to a BAA. BIDS is a secure 128-bit encryption that provides proposal response uploads for prospective bidders and ensures control of bidder proprietary data.

In addition, the TSWG has released BAAs for the Department of Homeland Security. Through this effort, the TSWG increases the return on the investment in counterterrorism technologies made by multiple Federal agencies by harnessing the technical capabilities of BIDS to support their initiatives. BIDS continues to serve as a model for other federal programs that seek to solicit technical proposals while eliminating the inconvenience of paper forms, the unnecessary waste in processing time, and excessive application mailing expenses.

TSWG Membership

U.S. Department of Defense

- Cyber Crime Institute
- Defense Computer Forensics Laboratory
- Defense Intelligence Agency
- Defense Logistics Agency
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- National Reconnaissance Office
- National Security Agency
- Office of the Assistant to the Secretary of Defense/Chemical and Biological Defense
- Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics
- Pentagon Force Protection Agency
- Polygraph Institute

U.S. Central Command

U.S. European Command

U.S. Joint Forces Command

U.S. Special Operations Command

U.S. Air Force

- Air Combat Command
- Air Force Research Lab
- Electronic Systems Command
- Force Protection Battle Lab
- Force Protection Systems Program Office
- Office of Special Investigations
- Surgeon General

U.S. Army

- 52nd Ordnance Group
- Chemical School
- Corps of Engineers
- Criminal Investigation Command
- Forces Command

- Maneuver Support Center
- Medical Research Institute of Infectious Diseases
- Natick Research, Development, and Engineering Center
- National Ground Intelligence Center
- Soldier and Biological Chemical Command
  - Edgewood Chemical Biological Center
- Tank-Automotive and Armaments Command
- Technical Escort Unit

U.S. Marine Corps

- Chemical Biological Incident Response Force
- Critical Infrastructure Protection

U.S. Navy

- Joint Program Office, Special Technology Countermeasures
- Naval Air Warfare Center
- Naval Criminal Investigative Service
- Naval Explosive Ordnance Disposal Technology Division
- Naval Facilities Engineering Service Center
- Naval Forces Central Command
- Naval Surface Warfare Center
- Special Warfare Center

Environmental Protection Agency

Federal Reserve Board

General Services Administration

- Mail Policy

Intelligence Community

InterAgency Board

National Aeronautics and Space Administration

Nuclear Regulatory Commission

Supreme Court of the United States

U.S. Capitol Police

U.S. Department of Agriculture

- Animal and Plant Health Inspection Service
- Forest Service

U.S. Department of Commerce

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

U.S. Department of Energy

- National Nuclear Security Administration
- Office of Energy Assurance
- Office of Security

U.S. Department of Health and Human Services

- Food and Drug Administration

U.S. Department of Homeland Security

- Border and Transportation Security Directorate
- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Federal Protective Service
- National Infrastructure Protection Center
- Office for Domestic Preparedness
- Science and Technology
- Transportation Security Administration
  - Land and Maritime Security
- United States Coast Guard
- United States Secret Service
  - Protective Security Division
  - Special Services Division
  - Technical Security Division

U.S. Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
  - Bomb Data Center
  - Hazardous Materials Response Unit
  - Hostage Rescue Team
  - Weapons of Mass Destruction Operations Unit

- Federal Bureau of Prisons
- National Center for Forensic Science
- National Forensic Science Technology Center
- National Institute of Justice
- U.S. Marshals Service

U.S. Department of State

- Bureau of Diplomatic Security
- Office of the Coordinator for Counterterrorism
- Overseas Building Operations

U.S. Department of Transportation

- Federal Aviation Administration
- Intelligence and Security
- Office of Information Services
- Volpe National Transportation Systems Center

U.S. Postal Service

- U.S. Postal Inspection Service

White House

- Office of Science and Technology Policy

State and Local Agencies

- Columbus Fire Department, Bomb Squad
- D.C. Metropolitan Police Department, Bomb Squad
- Fairfax County Police Department, Bomb Squad
- Maricopa County Sheriffs Office, Bomb Squad
- National Bomb Squad Commanders Advisory Board
- Port Authority of New York/New Jersey
- Prince George's County Fire Department, Bomb Squad

TSWG Subgroup Membership

Chemical, Biological, Radiological and Nuclear Countermeasures

Environmental Protection Agency

General Services Administration
- Mail Policy

Intelligence Community

InterAgency Board

U.S. Capitol Police

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

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

U.S. Department of Defense
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- National Security Agency
- Office of the Assistant to the Secretary of Defense/Chemical and Biological Defense
- Pentagon Force Protection Agencye
- U.S. Air Force
  - Air Combat Command
  - Electronic Systems Command
  - Force Protection Battle Lab
  - Surgeon General
- U.S. Army
  - 52nd Ordnance Group
  - Chemical School
  - Forces Command
  - Maneuver Support Center
  - Medical Research Institute of Infectious Diseases
  - National Ground Intelligence Center
  - Soldier and Biological Chemical Command
    - Edgewood Chemical Biological Center
  - Technical Escort Unit
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
- U.S. Navy
  - Naval Air Warfare Center
  - Naval Forces Central Command
  - Naval Surface Warfare Center

U.S. Department of Energy
- Office of Security

U.S. Department of Health and Human Services
- Food and Drug Administration

U.S. Department of Homeland Security
- Federal Emergency Management Agency
- Science and Technology
- U.S. Coast Guard
- United States Secret Service
  - Technical Security Division
- Transportation Security Administration

U.S. Department of Justice
- Federal Bureau of Investigation
  - Bomb Data Center
  - Hazardous Materials Response Unit
  - Weapons of Mass Destruction Operations Unit
- National Institute of Justice
- U.S. Marshals Service

U.S. Department of State
- Bureau of Diplomatic Security
- Office of the Coordinator for Counterterrorism
- Overseas Building Operations

U.S. Department of Transportation
- Intelligence and Security

U.S. Postal Service
- U.S. Postal Inspection Service

White House
- Office of Science and Technology Policy

Explosives Detection

Intelligence Community

U.S. Department of Defense
- National Security Agency
- U.S. Air Force
  - Air Combat Command
  - Air Force Research Lab
  - Force Protection Battle Lab
  - Force Protection Systems Program Office
- U.S. Army
  - Technical Escort Unit
- U.S. Navy
  - Naval Criminal Investigative Service
  - Naval Explosive Ordnance Disposal Technology Division

U.S. Department of Energy
- Office of Security

U.S. Department of Homeland Security
- Transportation Security Administration
- United States Coast Guard
- United States Secret Service

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

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

U.S. Postal Service
- U.S. Postal Inspection Service

Improvised Device Defeat

Intelligence Community Columbus

State and Local
- Fire Department, Bomb Squad
- D.C. Metropolitan Police Department, Bomb Squad
- Fairfax County Police Department, Bomb Squad
- Maricopa County Sheriffs Office, Bomb Squad
- National Bomb Squad Commanders Advisory Board
- Prince George's County Fire Department, Bomb Squad

U.S. Capitol Police

U.S. Department of Defense
- Defense Intelligence Agency
- National Security Agency
- U.S. Army
- U.S. Air Force
  - Air Combat Command
  - Air Force Research Lab
- U.S. Marine Corps
- U.S. Navy
  - Naval Criminal Investigative Service
  - Naval Explosive Ordnance Disposal Technology Division

U.S. Department of Homeland Security
- Transportation Security Administration
- United States Secret Service

U.S. Department of Justice
- Bureau of Alcohol, Tobacco, and Firearms
- Federal Bureau of Investigation
  - Bomb Data Center
- National Institute of Justice

Infrastructure Protection

Environmental Protection Agency

Nuclear Regulatory Commission

Port Authority of New York/New Jersey

U.S. Department of Agriculture
- Forest Service

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

U.S. Department of Defense
- U.S Army
  - Criminal Investigation Division
- Defense Threat Reduction Agency
- Defense Logistics Agency
- Joint Program Office, Special Technology Countermeasures
- U.S. Air Force
  - Office of Special Investigations
- U.S. Army
  - Corps of Engineers
- U.S. Marine Corps
  - Critical Infrastructure Protection
- U.S. Navy
  - Naval Criminal Investigative Service
  - Naval Surface Warfare Center

U.S. Department of Energy
- Office of Energy Assurance
- Office of Security

U.S. Department of Homeland Security
- Federal Emergency Management Agency
- Federal Protective Service
- National Infrastructure Protection Center
- Office for Domestic Preparedness
- Science and Technology
- Transportation Security Administration
- United States Secret Service
  - Protective Security Division

U.S. Department of Justice
- Federal Bureau of Investigation

U.S. Department of Transportation
- Federal Aviation Administration
- Volpe National Transportation Systems Center

Investigative Support and Forensics

Environmental Protection Agency

Intelligence Community

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

U.S. Department of Defense
- Cyber Crime Institute
- Defense Computer Forensics Laboratory
- Polygraph Institute
- U.S. Army
  - Criminal Investigation Command
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
- U.S. Navy
  - Naval Criminal Investigative Service

U.S. Department of Energy
- Office of Security

U.S. Department of Homeland Security
- Federal Emergency Management Agency

- Transportation Security Administration
- United States Secret Service

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

U.S. Department of Transportation
- Federal Aviation Administration

U.S. Postal Service
- U.S. Postal Inspection Service

Personnel Protection

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

U.S. Department of Defense
- U.S. Army
  - Natick Research, Development, and Engineering Center
  - Tank-Automotive and Armaments Command
- U.S. Navy
  - Special Warfare Center

U.S. Department of Energy
- Office of Security

U.S. Department of Homeland Security
- United States Secret Service
  - Special Services Division
  - Technical Security Division

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

Physical Security

Federal Reserve Board

Intelligence Community

National Aeronautics and Space Administration

Nuclear Regulatory Commission

Supreme Court of the United States

U.S. Department of Defense
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- National Security Agency
- Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics
- U.S. Air Force
- U.S. Army
- U.S. Central Command
- U.S. European Command
- U.S. Joint Forces Command
- U.S. Marine Corps
- U.S. Navy

U.S. Department of Energy
- National Nuclear Security Administration
- Office of Security

U.S. Department of Homeland Security
- Border and Transportation Security Directorate
- Federal Law Enforcement Training Center
- Transportation Security Administration
  - Land and Maritime Security
- U.S. Coast Guard
- U.S. Secret Service

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

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

U.S. Department of Transportation
- Office of Information Services

U.S. Postal Service
- U.S. Postal Inspection Service

Surveillance, Collection and Operations Support

Intelligence Community

U.S. Department of Defense
- Defense Intelligence Agency
- National Reconnaissance Office
- National Security Agency
- U.S. Special Operations Command

U.S. Department of Homeland Security
- U.S. Secret Service

U.S. Department of Justice
- Federal Bureau of Investigation

Tactical Operations Support

U.S. Department of Defense
- U.S. Special Operations Command

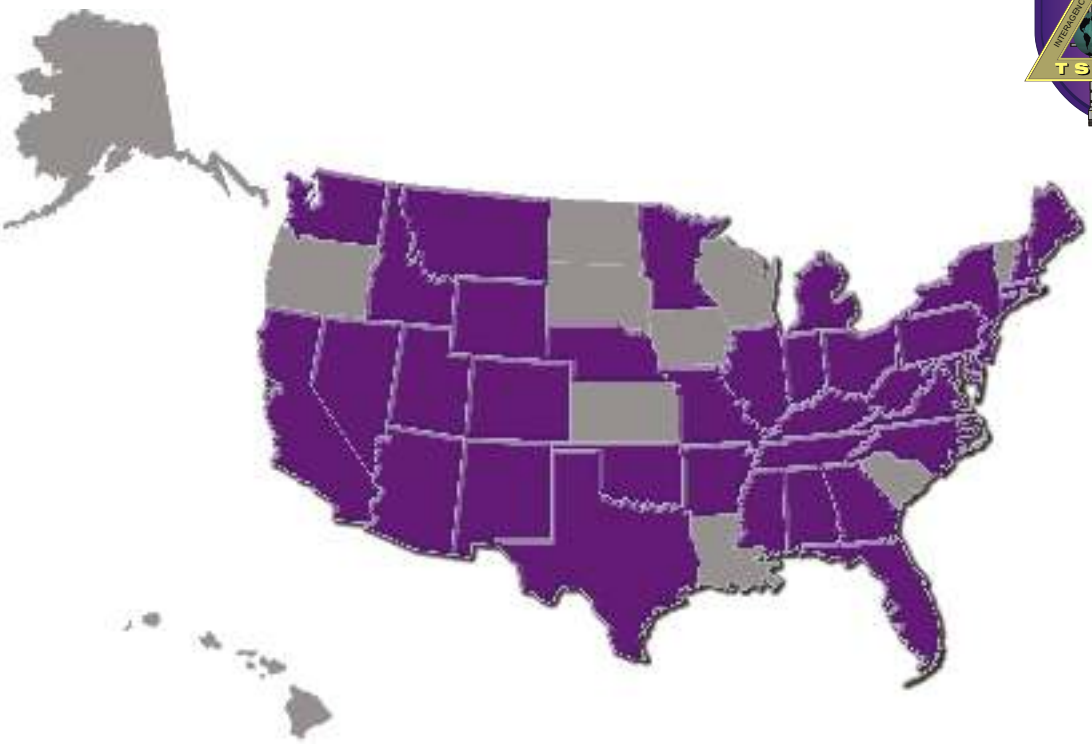
U.S. Department of Energy
- Office of Security

U.S. Department of Homeland Security
- United States Secret Service

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

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

TSWG Performers



Alabama
Auburn University, Auburn
Auburn University, The Canine & Detection Research Institute, Auburn
Missile and Space Intelligence Center, Huntsville
Sparta, Inc., Huntsville

Arizona
Armorworks, Tempe
Army Electronic Proving Ground, Fort Huachuca
Authenti-Corporation, Gilbert
Litton Electro-Optical Systems, Phoenix

Arkansas
The Tekne Group, Inc., Hot Springs
University of Arkansas, Fayetteville

California
3rd Ring, Mammoth Lakes
Advanced Countermeasures Systems, Rancho Cordova
American Technology Corporation, San Diego
Applied Signal Technology, Inc., Sunnyvale
Comglobal Systems, Inc., San Diego
Dynamics Technology, Inc., Torrance
High Technologies Solutions, Inc., San Diego
Intelligent Optical Systems, Inc., Torrance
Jet Propulsion Laboratory, Pasadena
Karagozian & Case, Glendale
Lawrence Berkeley National Laboratory, Berkeley
Lawrence Livermore National Laboratory, Livermore
MAXIM Systems, Inc., San Diego
Mission Research Corporation, Santa Barbara
Quantum Magnetics, Inc., San Diego
Rapiscan Security Products, Inc., Hawthorne
Raytheon Company NCS, El Segundo
Raytheon Company, Electronic Systems, Buena Vista

San Jose State University, San Jose
Sandia National Laboratory, Livermore
Science Applications International Corporation, San Diego
Space and Naval Warfare Systems Center, San Diego
Special Technologies Laboratory, Santa Barbara
Technology Services Corporation, Los Angeles
University of California, Davis
University of California, San Diego
Virage, Inc., San Mateo

Colorado
Applied Research Associates, Inc., Littleton

Connecticut
Interspiro, Inc., Branford
Nextgen Fiber Optics, LLC, Dayville
Pulmatrix, Inc., Ridgefield
United Technologies Research Corporation, Hartford

Delaware
DuPont, Wilmington

District of Columbia
International Association of Firefighters
Naval Research Laboratory
Perrault Structural Products, Inc.
Psynapse

Florida
Air Force Research Laboratory, Tyndall AFB
ANRO Engineering, Inc., Sarasota
Civil Engineering Support Agency, Tyndall AFB
Engineering Technology, Inc., Orlando
Florida International University, Miami
Harris Government Communications Systems Division, Melbourne
Knights Armament Company, Vero Beach
National Center for Forensic Science, Orlando
National Terrorism Preparedness Institute, St. Petersburg College, St. Petersburg
Purified MicroEnvironments, Ormond Beach
University of Florida, Gainesville

Georgia
Georgia Tech Research Institute, Atlanta

Idaho
Idaho National Engineering and Environmental Laboratory, Idaho Falls

Illinois
Argonne National Laboratory, Argonne
Gas Technology Institute, Des Plaines
Nanosphere, Inc., Northbrook
Underwriters Laboratory, Chicago

Indiana
Creative Building Products, Fort Wayne
Naval Surface Warfare Center, Crane

Kentucky
Microsensor Systems, Inc., Bowling Green

Maine
Sensor Research and Development Corporation, Orono

Maryland
20/20 Gene Systems, Rockville
Advanced Engineering & Sciences, Abingdon
Armed Forces Radiobiology Research Institute, Bethesda
Eagan, McAllister Inc., Lexington Park
Edgewood Chemical Biological Center, Aberdeen Proving Ground
GEOMET Technologies, Inc., Germantown
Jackson and Tull, Baltimore
Johns Hopkins University, Applied Physics Laboratory, Laurel
Johns Hopkins University School of Medicine, Baltimore
Lagus Applied Technology, Olney
Loats Associates, Inc., Westminster
Multispectral Solutions, Inc., Germantown

National Institute of Standards and Technology, Gaithersburg
Naval Explosive Ordnance Disposal Technology Division, Indian Head
Naval Surface Warfare Center, Carderock
Naval Surface Warfare Center, Indian Head
Sytex, Inc., Ellicott City
Syntonics, Columbia
Techno Sciences, Inc., Lanham
Technology Assessment & Transfer, Inc., Annapolis
Technology Service Corporation, Silver Spring
Veritas, Inc., Rockville
Windermere Information Technology Systems, Annapolis

Massachusetts

American Science and Engineering, Billerica
BBN Technologies, Cambridge
Charles Stark Draper Lab, Cambridge
Curtiss Wright/Lau Defense Systems, Inc., Littleton
Foster-Miller, Inc., Waltham
GE Ion Track, Wilmington
Idolon Technologies, Melrose
Implant Sciences Corporation, Wakefield
iRobot, Somerville
Massachusetts Institute of Technology, Cambridge
Massachusetts Institute of Technology, Lincoln Laboratory, Lexington
Millivision, Inc., South Deerfield
Natick RD&E Center, Natick
SenTech, Inc., Stoneham
Surmet Corporation, Burlington
Technical Products Inc., Framingham
TIAX, LLC, Cambridge
Tufts University, Medford
University of Massachusetts, Amherst
Viisage Technology, Littleton
Volpe National Transportation Systems Center, Cambridge

Michigan

Michigan State University, East Lansing
Triad Services Group, Inc., Madison Heights
Wayne State University, Detroit

Minnesota

Honeywell Laboratories, Minneapolis
The Mayo Clinic, Rochester
University of Minnesota, Duluth

Mississippi

ProVision Technologies, Stennis Space Center
U.S. Army Corps of Engineers - Engineering Research and Development Center, Waterways Experiment Station, Vicksburg

Missouri

Clean Earth Technologies, LLC, Earth City
Hanford Nuclear Services, Inc., West Plains
Midwest Research Institute, Kansas City

Montana

Veridical Research and Design, Bozeman

Nebraska

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

Nevada

Remote Sensing Laboratory, Las Vegas
Sparta Inc., Las Vegas
University of Nevada, Las Vegas

New Hampshire

BAE Systems (IEWS), Nashua
Global Manufacturing Company, Pittsfield
Impact Science and Technology, Hollis

New Jersey

Communications and Electronics Command, Fort Monmouth
FibreGuide, Stirling
Hi Temp Technology, Inc., Flemmington

JeBen Photonics, Inc., Denville
JP Laboratories, Middlesex
New Jersey Institute of Technology, Newark
Rutgers University, Piscataway
Sarnoff Corporation, Princeton

New Mexico

Applied Research Associates, Inc., Albuquerque
Los Alamos National Laboratory, Los Alamos
MesoSystems Technology, Inc., Albuquerque
National Assessment Group, Albuquerque
New Mexico Institute of Mining and Technology, Energetic Materials Research and Testing Center, Socorro
Sandia National Laboratories, Albuquerque
Science & Engineering Associates, Inc., Albuquerque

New York

Amherst Systems, Buffalo
New York University, New York
Northrop Grumman Corporation, Buffalo
Northrop Grumman ISS, Bethpage
Portable Environments, LLC, Ithaca
Rensselaer Polytechnic Institute, Troy
Sensatex, Inc., New York
Weidlinger Associates, Inc., New York

North Carolina

Applied Marine Technology, Inc., Southern Pines
North Carolina State University, Textile Protection and Comfort Center, Raleigh
Research Triangle Institute, Research Triangle Park
Signalscape, Raleigh

Ohio

Air Force Institute of Technology, Dayton
Battelle Memorial Institute, Columbus
Komar Industries, Inc., Groveport
National Air Intelligence Center, Wright Patterson AFB, Dayton
Ohio University, Clippinger Laboratories, Athens
Total Fire Group/Morning Pride Manufacturing, Dayton
University of Dayton Research Institute, Dayton

Oklahoma

Nomadics, Inc., Stillwater

Pennsylvania

Carnegie Mellon University, Learning Systems Architecture Lab, Pittsburgh
CDG Technology, Bethlehem
Concurrent Technologies Corporation, Johnstown
Drexel University, Data Fusion Laboratory, Philadelphia
DRS Laurel Technologies, Johnstown
Franklin Applied Physics, Oaks
Optical Systems Technology, Inc., Freeport
St. Joseph's University, Early Responders Distance Learning Center, Philadelphia
University of Pittsburgh, Pittsburgh

Tennessee

Atmospheric Glow Technologies, Knoxville
BAE Systems, Ordnance Systems, Inc., Kingsport
BWXT Y-12, Oak Ridge
Northrop Grumman, REMOTEC, Oak Ridge
Oak Ridge National Laboratory, Oak Ridge
PIPS Technology, Knoxville
Turtle Mountain Communications, Maryville

Texas

Applied Research Associates, Inc., San Antonio
BAE Systems, Austin
International Personnel Protection, Inc., Austin
Litton Electro-Optical, Dallas
Lynntech, Inc., College Station
Northrop Grumman-Litton Electro Optical Systems, Dallas

Southwest Research Institute, San Antonio
University of Houston, Houston
University of Texas at Dallas, Richardson
University of Texas, Austin
Wilfred Baker Engineering, Inc., San Antonio

Utah
Battelle Memorial Institute, Dugway
Mission Research Corporation, Logan
U.S. Army, Dugway Proving Ground
Utah State University, Logan

Virginia
Applied Marine Technology, Inc., Virginia Beach
Battelle Memorial Institute, Arlington
Booz Allen Hamilton, Inc., McLean
DCS Corporation, Alexandria
DTI Associates Inc., Arlington
Flatter & Associates, Garrisonville
General Dynamics, Charlottesville
General Testing Laboratories, Colonial Beach
Homeland Water Security Technologies, Inc., Annandale
International Association of Firechiefs, Fairfax
K&M Environmental, Inc., Virginia Beach
Naval Surface Warfare Center, Dahlgren
ORION Scientific Systems, McLean
Qinetiq, Inc., Arlington
Science Applications International Corporation, McLean
Sparta Inc., Arlington
SRA International, Inc., Fairfax
The Bode Technology Group, Springfield
Night Vision and Electronic Sensors Directorate, Fort Belvoir
Veridian Information Systems, Inc., Arlington

Washington
Cascade Designs, Inc., Seattle
MesoSystems Technology, Inc., Kennewick
Pacific Northwest National Laboratory, Richland
Washington State University, Pullman

West Virginia
West Virginia University, Morgantown

Wyoming
Aristatek, Inc., Laramie

International

Canada
Defence Research Establishment, Medicine Hat, Suffield
Defence Research & Development Centre, Val Cartier, Quebec
EOD Performance, Inc., Ottawa
MREL, Ontario, Ottawa
National Research Council of Canada, Ottawa
Royal Canadian Mounted Police, Ottawa

Israel
Israel Institute for Biological Research, Ness Ziona
Israel Ministry of Defence, Tel Aviv
Rafael, Tel Aviv

United Kingdom
Defence Science and Technology Laboratories, Fort Halstead, Kent
Defence Science and Technology Laboratories, Porton Down, Wiltshire
Forensic Science Service, Birmingham
Home Office, Police Scientific Development Branch, Horsham, West Sussex
Home Office, Police Scientific Development Branch, Hertfordshire
Qinetiq, Farnborough, Hampshire
Qinetiq, Malvern
University of Sheffield, Department of Forensic Pathology, Sheffield

Glossary of Acronyms

A

ACC	Air Combat Command
AFIP	Armed Forces Institute of Pathology
AFRL	Air Force Research Lab
AFRRI	Armed Forces Radiobiology Research Institute
AIS	Automated Information System
ALON	Aluminum-Oxynitride
APHIS	Animal and Plant Health Inspection Service
ASDE	Airport Surface Detection Equipment
ASD (SO/LIC)	Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
ASDP	Airport Security Display Processor
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
ATrCT	Alert Trend Change Tool
AVIDS	Advanced Vehicle Driver Identification System

B

BAA	Broad Agency Announcement
BAT	Biodosimetry Assessment Tool
BDC	Bomb Data Center
BEEM	Blast Effects Estimation Model
BIDS	BAA Information Delivery System
BIRM	Barrier Impact Response Model
BTSD	Border and Transportation Security Directorate

C

C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CB	Chemical and/or Biological
CBIAC	Chemical and Biological Defense Information Analysis Center
CBIRF	Chemical Biological Incident Response Force
CBRN	Chemical, Biological, Radiological and Nuclear
CBRNC	Chemical, Biological, Radiological and Nuclear Countermeasures
CCI	Cyber Crime Institute
CD	Compact Disc
CD-ROM	Compact Disc-Read Only Memory
CE	U.S. Army Corps of Engineers
CENTCOM	U.S. Central Command
CID	Criminal Investigations Division
CIP	Critical Infrastructure Protection
CIRTS	Critical Incident Response Technology Seminar
CMLS	Chemical School
CODIS	Combined DNA Index System
COMUSNAVEUR	Commander, United States Naval Forces, Europe
CTTS	Combating Terrorism Technology Support

CTTSO	Combating Terrorism Technology Support Office
CTS	Call Through Simulator
CTX	Computed Tomographic X-ray
CQB	Close Quarter Battle

D

DATSD/CBD	Deputy Assistant to the Secretary of Defense for Counterproliferation/Chemical and Biological Defense
DEA	Drug Enforcement Administration
DHS	U.S. Department of Homeland Security
DIA	Defense Intelligence Agency
DLA	Defense Logistics Agency
DMNB	2,3-Dimethyl-2,3dinitrobutane
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DS	Bureau of Diplomatic Security
DTO	Defense Technology Objective
DTRA	Defense Threat Reduction Agency

E

ECBC	Edgewood Chemical Biological Center
ED	Explosives Detection
EOD	Explosive Ordnance Disposal
EPA	Environmental Protection Agency
ESC	Electronic Security Command
ESDA	Electrostatic Detection Apparatus
EUCOM	U.S. European Command

F

FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FBOP	Federal Bureau of Prisons
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Center
FORSCOM	U.S. Army Forces Command
FPBL	Force Protection Battle Laboratory
FPS	Federal Protective Service
FPSPO	Force Protection Systems Program Office
FRAT	First Responder Automated Data Tool
FRP	Fiber Reinforced Polymer
FS	Forest Service
FY	Fiscal Year

G

GSR	Gunshot Residue Analysis

GWOT	Government War on Terrorism

H

HAZMAT	Hazardous Materials
HMRU	Hazardous Materials Response Unit
HRT	Hostage Rescue Team
HVAC	Heating, Ventilation and Air Conditioning

I

IAB	InterAgency Board for Equipment Standardization and InterOperability
IC	Intelligence Community
ICAO	International Civil Aviation Organization
ICIT	Incident Command Information Tool
IDD	Improvised Device Defeat
IED	Improvised Explosive Device
IG/T	Interdepartmental Working Group on Terrorism
IO	Information Operations
IOS	Information Operations Support
IP	Infrastructure Protection
IPPS	Instantaneous Personnel Protection Systems
IS&F	Investigative Support and Forensics
ITCT	Insider Threat Countermeasures Toolkit
IWG/CT	Interagency Working Group on Counterterrorism

J

JCS	Joint Chiefs of Staff
JFCOM	U.S. Joint Forces Command
JPO-STC	Joint Program Office-Special Technology Countermeasures

L

LAN	Local Area Network
LL	Lincoln Laboratory
LVB	Large Vehicle Bomb
LVBCM	Large Vehicle Bomb Countermeasures

M

MANSCEN	Maneuver Support Center
MIT	Massachusetts Institute of Technology

N

NATO	North Atlantic Treaty Organization
NAVEODTECHDIV	Naval Explosive Ordnance Disposal Technology Division
NAVCENT	Naval Forces Central Command
NAWC	Naval Air Warfare Center
NCFS	National Center for Forensic Science
NCIS	Naval Criminal Investigative Service
NEW	Net Explosive Weight

NFSTC	National Forensics Science Technology Center
NGEODRCV	Next-Generation Explosive Ordnance Disposal Remote Controlled Vehicle
NGIC	National Ground Intelligence Center
NIJ	National Institute of Justice
NIOSH	National Institute for Occupational Safety and Health
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NRL	Naval Research Laboratory
NRO	National Reconnaissance Office
NRR	Neutron Resonance Radiography
NSA	National Security Agency
NSDD	National Security Decision Directive
NSWC	Naval Surface Warfare Center

O

OBO	Overseas Building Operations
ODP	Office for Domestic Preparedness
OEA	Office of Energy Assurance
OIS	Office of Information Services
OLES	Office of Law Enforcement Standards
OS	Office of Security
OSD	Office of Secretary of Defense
OSI	Office of Special Investigations
OSTP	Office of Science and Technology Policy
OUSD (AT&L)	Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics

P

PAPR	Powered Air Purifying Respirator
PDA	Personal Digital Assistant
PFPA	Pentagon Force Protection Agency
PI	Polygraph Institute
PNNL	Pacific Northwest National Laboratory
PP	Personnel Protection
PPE	Personal Protective Equipment
PS	Physical Security
PSD	Physical Security Directorate

Q

QR	Quadrupole Resonance

R

R&D	Research and Development
RAID	Redundant Array of Independent Disks
RD&E	Research, Development and Engineering
RF	Radio-Frequency
RTR	Real-Time Radiographic

S

S/CT	Department of State Office of the Coordinator for Counterterrorism
S&T	Science and Technology
SAST	Systems Administrator Simulation Trainer
SBCCOM	Solider and Biological Chemical Command
SC&OS	Surveillance, Collection and Operations Support
SCADA	Supervisory Control and Data Acquisition
SCBA	Self-Contained Breathing Apparatus
SCCU	Standoff Connectivity Control Unit
SCIF	Sensitive Compartmented Information Facility
SG	Surgeon General
SO/LIC	Special Operations and Low-Intensity Conflict
SOCOM	Special Operations Command
SOP	Standard Operating Procedure
SPAn32	Single Degree of Freedom Plastic Analysis
SPIDER	Stabilized Panoramic Intruder Detection and Recognition
SSD	Special Services Division
STR	Short Tandem Repeat
STU	Secure Telephone Unit
SWAT	Special Weapons and Tactics
SWC	Special Warfare Center
SWIG	Small Watercraft Inspection Guide

T

TACOM	Tank-Automotive and Armaments Command
TEU	Technical Escort Unit
TNT	Trinitrotoluene
TOS	Tactical Operations Support
TSA	Transportation Security Administration
TSD	Technical Security Division
TSWG	Technical Support Working Group
TTL	Tagging, tracking and locating

U

UCSD	University of California San Diego
USA	United States Army
USAF	United States Air Force
USAMRID	United States Army Medical Research Institute of Infectious Diseases
USCG	United States Coast Guard
USMC	United States Marine Corps
USMS	United States Marshals Service
USN	United States Navy
USPIS	United States Postal Inspection Service
USPS	United States Postal Service
USSS	United States Secret Service

V

VBIED	Vehicle-Borne Improvised Explosive Device
VIC	Vehicle Inspection Checklist
VIP	Very Important Person
VPAT	Virus Propagation Tool

W

WAC	Wall Analysis Code
WAN	Wide Area Network
WMD	Weapons of Mass Destruction
WMDOU	Weapons of Mass Destruction Operations Unit

Combating Terrorism
Technology Support Office
Technical Support Working Group