Department of Defense

PHYSICAL SECURITY EQUIPMENT RDT&E

Program Summary

2010

Department of Defense

PHYSICAL SECURITY EQUIPMENT RDT&E

Cover Photo: Pfc. Richard W. Jones Jr., U.S. Army / Released

Program Summary 2010

Meeting the Physical Security and Force Protection Needs of the Department of Defense through System Effectiveness and Program Efficiency

The spectrum of constant and evolving threats facing Department of Defense (DoD) personnel and critical warfighting assets illustrates the continuing need and importance of a comprehensive, coordinated physical security (PS) and Force Protection (FP) response. The Physical Security Equipment (PSE) Research, Development, Test and Evaluation (RDT&E) Program is the primary mechanism by which DoD achieves this goal. The mission of the PSE RDT&E Program is to provide the Military Services and other DoD agencies with adequate planning, programming, and funding support for valid PSE materiel requirements while eliminating duplication of projects, pursuing the use of commercial off-the-shelf products, ensuring systems integration, and promoting interoperability and sustainability.

The PSE RDT&E equipment and studies summarized in this document represent the culmination of identified PS and FP requirements from the Services and coordinated with appropriate Office of the Secretary of Defense (OSD) and Joint Staff organizations, as well as identified findings and recommendations reported by ongoing Department policy and security reviews. Before initiating each RDT&E investment, the projects are processed through a Joint-Service review to ensure that they reflect collective solutions for related requirements and result in operationally useful and sustainable equipment to improve DoD's capability to fight and win wars.

During Fiscal Year 2010, the PSE RDT&E Program and its projects achieved numerous milestones and individual accomplishments which serve to reinforce the value and importance of this overarching initiative. Representative examples of these PSE successes include:

- Test and evaluation of 21 explosive detection systems [*Navy Explosive Detection Equipment (EDE) Program*]
- Completion of major software enhancement and site security risk assessments in preparation for final system implementation [*AVERT*]
- Transition of Phase II product to Field and Acquisition Sponsor [*Shipboard Security Containers*]
- Finalization of planning activities for transition to execution stage [*Interim Integrated Base Defense (I-IBD)*]
- Conduct of successful planning and execution demonstration at three installations [*Defense Installation Access Control (DIAC) system*]
- Fielding of 196 systems to Forward Operating Bases [*Battlefield Anti-Intrusion System (BAIS)*]
- Development of an overarching Strategic Plan for the Physical Security Equipment Action Group (PSEAG), and the completion of a project detailing the history of the organization and its legacy work in the physical security equipment arena
- Initiation of surrogate concept flight activities [*National Air Space Integration Demonstrator for Small Tactical UAS (STUAS) Alarm Response*]
- Installation of AutoScan beta versions at three facilities [*AutoScan Under Vehicle Inspection System (UVIS)*]
- Completion of multiple Combined Test Force Evaluations for Commercial-off-the-Shelf systems [*Commercial-off-the-Shelf Equipment Qualification (COTS Qual)*]

PSE RDT&E Program oversight and execution is facilitated through an active partnership between the Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters (OASD(NCB)/NM)) – as program overseer, and the Army, Marine Corps, Navy, and Air Force (the Military Services) and the Defense Threat Reduction Agency (DTRA) – as program executors. Specific PSE RDT&E Program management and oversight is then further delegated

to the DoD Physical Security Equipment Action Group (PSEAG) and the Security Policy Verification Committee (SPVC). These groups are comprised of representatives from the Military Services, in collaboration with the Joint Staff, other OSD organizations, and other vested physical security stakeholders. This collaboration ensures that the PSE RDT&E Program addresses capability gaps, meets operational needs, and conforms to Department policy.

Beyond providing oversight and collaborative functions for the PSE RDT&E Program, the PSEAG and the SPVC seek to maximize investments in this area by actively identifying efficiencies at every level. In light of changing DoD budgets, and evolving operational requirements, guidance and direction from both the President and Congress, it is important that the Department continuously evaluates its expenditures and approaches to ensure that material investments produce the most effective and efficient results.

This evaluation is especially important when applied to the surety of the DoD nuclear weapons stockpile. When considering the use of PSE alternatives for nuclear security, the SPVC is careful to exercise diligence in determining which security enhancements provide the greatest effectiveness in protecting the nuclear stockpile against potential threats. By accurately identifying the risk reduction-to-investment ratio of a proposed enhancement and its effect of resource stewardship, the SPVC is able to improve the acquisition process while simultaneously meeting more Service needs.

The PSEAG also applies this evaluation methodology as part of its own ongoing initiative to formulate and implement timely PSE programs in response to installation threats. Critical to this evaluation process is the maintenance of lines of coordination with the Joint Staff and the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) which, as with the nuclear surety area, ensures that the invested programs provide the greatest level of effectiveness and efficiency. A further benefit of this coordination is the identification of interoperable programs across physical security, chemical/biological defense, and counter-rocket/missile defense sectors for an enhanced installation force protection profile.

Within the context of tighter budgets, greater life-cycle costs, and escalating threats the utilization of a process-oriented acquisition strategy is a necessity in formulating a PSE RDT&E Program that provides supportable, cost-effective physical security and force protection technology to the warfighter.

I hope you find this 2010 Summary beneficial in meeting your PSE needs.

Thomas Whittle, PE

Acting Chairman,
Physical Security Equipment Action Group (PSEAG)

Table of Contents

Department of Defense Physical Security Equipment (PSE) Research, Development, Test and Evaluation (RDT&E) Program Overview . . . 1

PSEAG PROGRAM FUNDING . . . 2

Advanced Container Security Device . . . 5

Attack Tools and Material Resistance (ATMR) . . . 6

AutoScan Under-Vehicle Inspection System (UVIS) . . . 7

Battlefield Anti-Intrusion System (BAIS) . . . 8

Biometric Verification System (Sub-Component of the “Smart Magazine” Project) . . . 9

Commercial-Off-the-Shelf Equipment Qualification (COTS Qual) . . . 10

Comparative Studies and Evaluations of COTS Explosive Detection Equipment (EDE) . . . 11

Comparative Test and Evaluation (T&E): Colorimetric Trace Explosive Detection Device (EDE) . . . 14

Comparative Test and Evaluation (T&E): Short Range Threat Detection . . . 15

Correlation of Physical Security Radars to Identify Friend or Foe . . . 16

Force Protection Equipment Demonstration (FPED) . . . 17

Handheld THz Spectrometers . . . 18

Integrated Defense Command and Control Common Operating Picture (IDC2COP) . . . 19

Integrated Ground Security Surveillance Response – Capability (IGSSR-C) . . . 20

Interim Integrated Base Defense (I-IBD) . . . 21

Joint Conflict and Tactical Simulation Enhancements (JCATS) . . . 22

Joint Force Protection Advanced Security System (JFPASS) Joint Capabilities Technology Demonstration (JCTD) . . . 23

Lighting Kit, Motion Detector (LKMD) . . . 24

Long-Range 3D THz Radar Imager . . . 25

National Air Space Integration Demonstrator for Small Tactical UAS (STUAS) Alarm Response . . . 26

Physical Security Equipment Action Group (PSEAG) Strategic Plan . . . 27

Physical Security of Storage Magazines - Doors . . . 28

Shipboard Security Containers . . . 29

Tactical Surveillance System (TSS) . . . 30

Waterside and Shipboard Security – Sonar Augmentation . . . 31

Waterside and Shipboard Security – Ultra Wide Band Radar . . . 32

Weapons Tracking Seal . . . 33

XD-4: Automated Handheld Colorimetric System . . . 34

Table of Contents (cont.)

Appendix A. Information Repository 37
Appendix B. The DoD PSE RDT&E Program Organization and Structure 38
Appendix C. DoD Physical Security Equipment Action Group (PSEAG) 39
Appendix D. Joint Requirements Working Group (JRWG) 40
Appendix E. Security Equipment Integration Working Group (SEIWG) 41
Appendix F. DoD Security Policy Verification Committee (SPVC) 43
Appendix G. Administrative Points Of Contact 46
Appendix H. Technical Points Of Contact 47
Appendix I. List of Acronyms 48

INTRODUCTION

DEPARTMENT OF DEFENSE

PSEAG

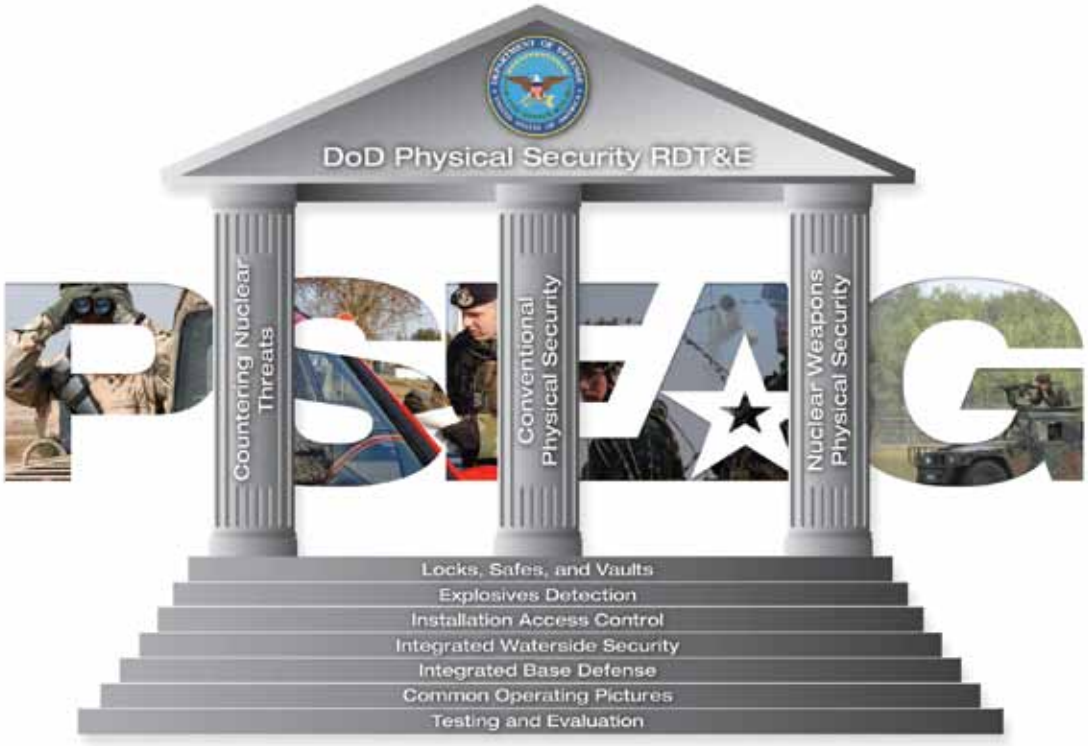
Department of Defense Physical Security Equipment (PSE) Research, Development, Test and Evaluation (RDT&E) Program Overview

The Department of Defense (DoD) Physical Security Equipment (PSE) Research, Development, Test and Evaluation (RDT&E) Program provides physical security equipment and analyses to meet the immediate and projected force protection challenges of the Services and the combatant commands (COCOMs). The PSE RDT&E Program is supported by three Thrust Areas through which the DoD and PSEAG focus their physical security activities:

- **Conventional Physical Security** – protection of personnel; prevention of unauthorized access to non-nuclear weapons equipment, installations, materials, and documents; and, safeguarding of the foregoing against espionage, sabotage, damage, and theft.
- **Nuclear Weapons Physical Security** – protection of nuclear weapons, and related equipment, installations, materials, and documents; and safeguarding of the foregoing against espionage, sabotage, damage, and theft.
- **Countering Nuclear Threats** – countering of radiological or nuclear incidents delivered through unconventional means, regardless of origins, across the full range of DoD Prevention, Protection, and Response activities.

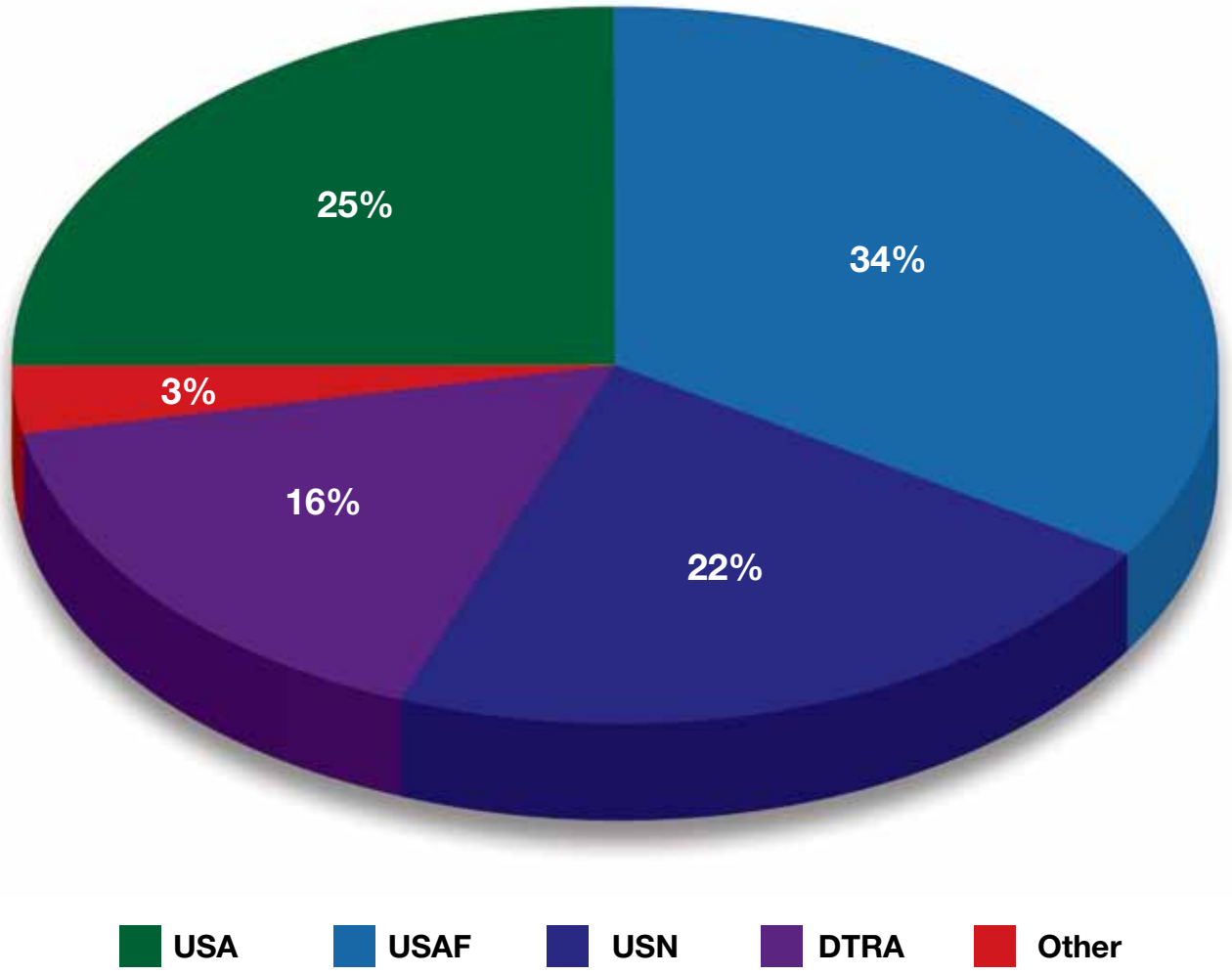
Underpinning this entire structure is a foundation of physical security equipment activities which are now organized into major initiatives, centered on key physical security requirements. These major initiatives bring together formerly disparate physical security equipment projects into more cohesive and synergistic physical security equipment programs, each with identifiable benefits and results for the end-user:

- **Defense Installation Access Control**
- **Joint Integrated Base Defense**
- **Integrated Waterside Security**
- **Common Operational Pictures**
- **Explosives Detection Equipment**
- **Locks, Safes, and Vaults Program**
- **Testing and Evaluation**



PSEAG Program Funding

This year's funding of over $52 million reflects the ongoing importance of the physical security mission for the Department of Defense (DoD) and the Military Services, and their continuing commitment to identifying and developing technologies for the protection of DoD personnel and critical assets.



DEPARTMENT OF DEFENSE

PSEAG

Advanced Container Security Device

This project adapts the capabilities of the Department of Homeland Security (DHS) Container Security Device (CSD) to meet Navy/DoD physical security, explosive safety, anti-tamper, and situational awareness requirements for munitions transport and storage.

Requirements:

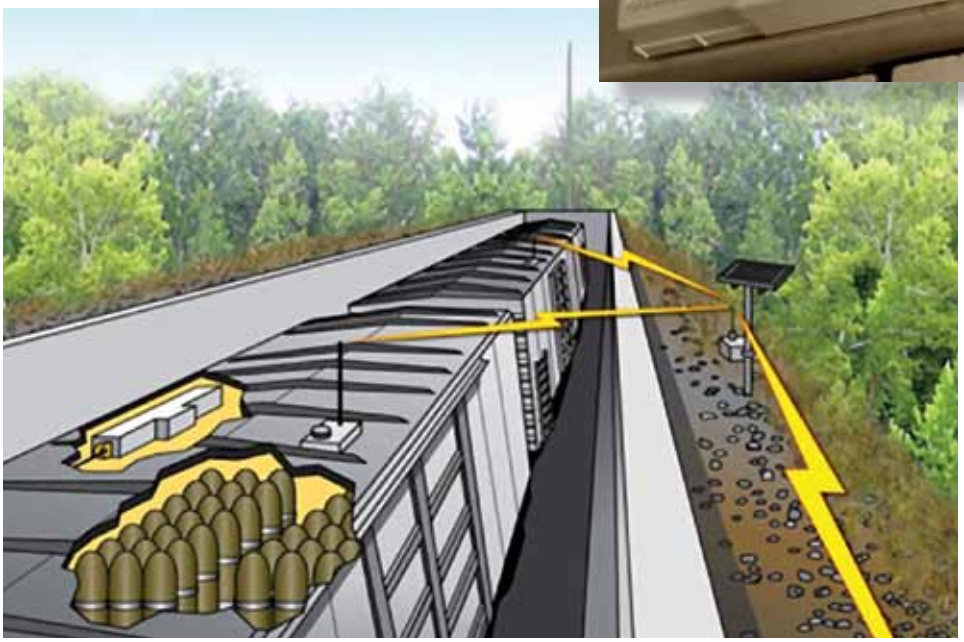
- Integrated Base Defense Security Systems (IBDSS) Capability Development Document (CDD), February 2005, Detection, Access Control
- Navy Anti-Terrorism / Force Protection (ATFP) Ashore CDD 4.7, 4.8, 4.9 & 4.10
- Chief of Naval Operations Instruction (OPNAVINST) 5530.13C
- Department of Defense (DoD) 5200.08-R, 9 April 2007, Security of Controlled Inventory
- Defense Transportation Regulation (DTR) 4500.9-R

Accomplishments:

- Obtained hazards of electromagnetic radiation to ordnance (HERO) Certification for 2nd Generation low-rate initial production (LRIP) Advanced Container Security Device (ACSD) (Naval Surface Warfare Center (NSWC) Dahlgren Certification Letter) for all munitions, zero standoff
- Continuing to conduct detection optimization tests

Key Dates / Milestones:

- Project Start Date: October 2009
- Concept Demonstration: August 2010
- Field Tests Complete: August 2011
- Performance Specification Available: May 2012
- Project End Date: September 2012



Attack Tools and Material Resistance (ATMR)

The Naval Facilities Engineering Service Center (NAVFAC ESC) has been tasked to establish the vulnerability of in-service physical security equipment to current forced entry, covert, and surreptitious threats. The objective of this effort includes:

- Review and analyze new, advanced attack tools and tool groups that have been authorized for testing and certifying Department of Defense (DoD) physical security equipment.
- Update the project's Test and Evaluation Master Plan (TEMP) to include the attack tools and materials selected for FY10 testing.
- Conduct forced entry testing using identified attack tools against selected composite material.
- Coordinate with Attack Resistance Working Group (ARWG) to facilitate updating the DoD MIL-HDBK 1013/1A and the Department of Energy (DOE) Barrier Handbooks with current attack resistance data.

Requirements:

- Several DoD Federal Specifications specify tool sets and test criteria for forced entry protection provided by physical security systems and components from conventional attack tools and methods

Accomplishments:

- Performed test and evaluation of various systems
- Developed test plan for a modular bunker
- Performed research in advanced, shape memory alloys

Key Dates / Milestones:

- Attack Tools and Resistant Material Review: On-going (Fiscal Year 2011 (FY11))
- Tools and Materials Test and Evaluation: On-going (FY11)

AutoScan Under-Vehicle Inspection System (UVIS)

AutoScan, developed by the Air Force Research Laboratory with industry partner Kachemak Research Development (KRD), enhances force protection by providing reliable threat detection capability at entry control points. This system is available in both portable and permanently-installable architectures. As vehicles drive over the AutoScan platform, the system operator receives a real-time image of the vehicle's undercarriage that is ready for inspection. From a safe, stand-off position, the operator can then zoom-in on any part of the image for closer inspection with multiple levels of detailed magnification. Furthermore, unlike manual inspection methods, AutoScan produces an image that can be stored for future comparison and analysis.

Requirements:

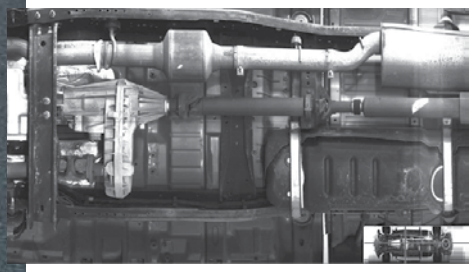
- Department of Defense (DoD) 5210.41M, Volume 3, Enclosure 3, paragraph 3d(4)(a)
- Air Force Instruction (AFI) 31-101, paragraph 2.4.3 through 2.4.3.1.3
- United Facilities Criteria (UFC) 4-022-01, paragraph 7-3.2

Accomplishments:

- Significantly improved water resistance of camera box, reducing likelihood of camera failure
- Installed test system at an airbase commercial gate, providing needed winter weather feedback
- Received approval for installation at in-ground test site, providing extreme thermal environment feedback
- Initiated development of "air knife" to clear debris from camera window
- Working with Security Forces Center, established Air Force Major Command (MAJCOM) relationship for requirements development, validation and refinement (Air Mobility Command)

Key Dates/Milestones:

- Project Start Date: February 2007
- Extreme Thermal Environment Operation: September 2011
- Light-Emitting Diode (LED) Light Source Development and Implementation: December 2011
- Image Enhancement / Anomaly Detection Capability: December 2011
- GigE versus Wireless Tradeoff Study: September 2011
- Project End Date: September 2012



Battlefield Anti-Intrusion System (BAIS)

The Battlefield Anti-Intrusion System (BAIS) is a compact sensor-based early warning system that provides early warning, detection and classification of intrusions for small units and troops during various tactical missions. It can be used either as a tactical stand-alone system or as a supplemental device for other security missions. To date, 1,325 systems have been fielded to U.S. Army and Army National Guard units and have proven highly reliable during operations in Theater. A separate BAIS Modernization Program has developed and tested an upgraded system that includes a Hand-Held Monitor/Transmitter and Sensor/Transceiver. A follow-on production contract was competitively awarded in August 2010 and included the upgrades resulting from the Modernization Program. These improvements continue to ensure current technology and improved performance are available to the field in the shortest time possible. A total of 4,112 systems are currently being produced and will be fielded in Fiscal Year 2011 (FY11).

Requirements:

- Platoon Early Warning Device II Operational Requirements Document, 11 September 2003

Accomplishments:

- Received additional 249 legacy BAIS and fielded 196 of those systems
- Participated in the Army Expeditionary Warfighting Experiment at Fort Benning, GA
- Completed development of the Sensor/Transceiver as part of the Modernization Program
- Awarded new production contract and initial delivery order for 4,112 systems

Key Dates / Milestones:

- Production Contract Award: 12 August 2010

Biometric Verification System (Sub-Component of the "Smart Magazine" Project)

The addition of a biometric verification system to the Internal Locking Device (ILD) lock creates a means of identifying a person by a physical feature exclusive only to that person. The ILD Biometric Verification System provides positive operator verification, allows entry tracking, and reduces potential vulnerabilities (key duplication, key integrity, lack of access record, etc.) inherent in a strictly mechanical locking system. The complete system consists of the ILD biometric lock; a DAP Technologies, Inc CE3240BW Handheld Computer, Add on Device, and programming / charging station; a stand-alone biometric fingerprint enroller; and Host Software with Operating User Guide. The Department of Defense (DoD) Lock Program has successfully developed and tested the biometric verification system, and will field demonstrate the technology through operational test and evaluation during Fiscal Year 2011 (FY11), at an operational base. Ordering information and support is available through the DoD Lock Program at (800) 290-76707, (805) 982-1212, DSN 551-1212, or via https://portal.navfac.navy.mil/go/locks.

Requirements:

- DoD Directive 5100.76M
- DoD Directive 3224.3, Physical Security Equipment
- DoD S5210.41M
- DoD 5210.65

Accomplishments:

- Completed initial test and evaluation of ILD biometric prototype and submitted results to contractor
- Met with contractor to discuss required changes to ILD biometric prototype based on Naval Facilities Engineering Service Center (NFESC) initial test and evaluation
- Developed a plan for final delivery of ILD biometric prototype and operational test systems meeting Phase III requirements
- Met with ILD manufacturer to discuss ILD biometric production/manufacturing processes and procedures

Key Dates / Milestones:

- Project Start Date: October 2007
- Prototype and Operational Test Systems Delivery: February 2011
- Operational Test System Installation: April 2011
- Operational Test and Evaluation: May-August 2011
- Project Transition Date: September 2011

Commercial-Off-the-Shelf Equipment Qualification (COTS Qual)

The Commercial-off-the-Shelf Equipment Qualification (COTS Qual) Program was initiated to analyze, select, test and evaluate new or improved perimeter and area sensors that will meet or exceed the requirements identified in the Integrated Base Defense Security System (IBDSS) Capability Development Document (CDD) Annex B, Intrusion Detection and/or Annex C, Asessment/Surveillance. The sensors will ultimately replace or augment existing similar capabilities with improved systems in intrusion detection and assessment capability for deployment in perimeter, flight line, access control, interior controlled facility, or avenue of approach applications. The intent of this program is to fill identified capability gaps and address obsolescence and diminishing manufacturing sources (DMS) issues. In Fiscal Year 2011 (FY11), beyond the items listed below, the following will undergo research, development, test and evaluation (RDT&E) pending approved requirements and funding: Wide Area Surveillance Thermal Imager / Long Range Thermal Imaging (WSTI/LRTI) Refresh; Tactical Automated Security System (TASS) communications module / hand-held monitor (CM/HHM); Sniper Detection; and, Passport Verification

Requirements:

- Integrated Base Defense Security Systems CDD, 17 February 2005
- Force Protection capability gaps are identified by U.S. Air Force Major Commands (MAJCOMs)

Accomplishments:

- Conducted cold weather qualification test and evaluation (QT&E) on two buried cable sensor systems
- Identified, tested and evaluated 4 Internet Protocol Security Cameras; approved 2 for inclusion on the Force Protection Security Systems (FPS2) Approved Equipment List
- Identified, tested and evaluated 1 Intrinsically Safe Sensor; sensor will be included on the FPS2 Approved Equipment List
- Evaluated 12 Fence Sensor request for information (RFI) submissions; selected 4 products from 3 vendors for formal testing
- Evaluated 19 Video Management System (VMS) RFI submissions; selected 4 products from 4 vendors for formal testing

Key Dates / Milestones:

- Project Start Date: 2008
- Complete Vindicator QT&E
- Complete Testing for Predator Elite and Wide Area Detection
- Complete Combined Test Force (CTF) of new Fence Sensors, VMS, and Video Motion Detection
- Complete cold weather testing of Flexible Solar Panels

Comparative Studies and Evaluations of COTS Explosive Detection Equipment (EDE)

As the Technical Direction Agent for the Department of Defense's (DoD's) Explosive Detection Equipment (EDE) Research, Development, Test and Evaluation (RDT&E) Program, the Naval Explosive Ordnance Disposal Technical Division (NAVEODTECHDIV) provides leadership in the pursuit of effective and suitable technology that meets the needs of Anti Terrorism/Force Protection personnel and Joint Service EOD for counter-improvised explosive device (IED) missions. This program seeks EDE that will effectively and economically confirm the presence or absence of energetic materials, IEDs, or IED components. The IEDs of concern may be contained in personal baggage, equipment, packages, postal mail, and cargo that may be conveyed by persons, vehicles, watercraft, and aircraft entering U.S. controlled areas. The EDE Program also addresses Joint Service EOD requirements for IEDs encountered downrange. The EDE Program manages research, development, testing and evaluation of technical approaches, development of measures of performance and specification, and testing of equipment under laboratory and operational conditions.

Beginning in 2002, with funding provided by the Physical Security Equipment Action Group (PSEAG) and other organizations, capability and limitation testing was performed on a wide variety of explosive detection equipment. All testing results are located on the PSEAG portal (https://www.us.army.mil/suite/folder/9892268).

Requirements:

- Acquisition personnel requiring independent government testing on various explosive detection technologies to determine which systems best meet their needs

Accomplishments:

- Over 40 reports published and posted on the PSEAG portal.
- All reports are available for government personnel and Law Enforcement Personnel

2010	
Characterization of the Ahura's FirstDefender RM & RMX for Bulk Explosive Identification	March
Characterization of the Ahura's TruDefender for Bulk Explosive Identification	March
COTS Evaluation of Rapiscan Eagle T1000 for Detection of Vehicle Borne Threats	March
Rapid Characterization of the Smiths Detection HazMatID (Software Version 3.1) for Bulk Explosive Identification	May
Characterization of GE Prototype Hardened MobileTrace for Trace Explosive Detection	August
Characterization of COTS Trace EDE and MWDs	October
2009	
Quick Look: Rapid Evaluation of Ahura's FirstDefender November 2008 Software and Chemical Library Upgrade (DecisionEngine MX 2.6.4) (classified)	February
Mobile Vehicle Explosive Detection Equipment (MVEDEX) Comparative Study for Detection of Vehicle Borne Threats	March
The Characterization of Smiths' IONSCAN Document Scanner for Trace Explosives Detection	April
Rapid Characterization of Smiths' HazMatID for Bulk Identification	May
COTS Evaluation of the Improved Shaped Energy System (OmniView Gantry Inspection System)	September
Characterization of the GE Security Itemiser FX for Explosive Detection	November
COTS Evaluation of the GaRDS Mobile	December

Comparative Studies and Evaluations of COTS Explosive Detection Equipment (EDE) (cont.)

2008	
Preliminary Summary of Smokeless and Black Powders Sample Analysis using the Ahura FirstDefender	April
Quick Look Report #1: Characterization of American Innovations' XD-2i with REF Reagent Formulations for Explosive Detection	April
COTS Evaluation of Remote/Standoff Explosive Detection System (R/SEDS)	May
Quick Look Report #1: Rapid Characterization of Ahura's FirstDefender for Bulk Explosive Identification (Classified)	May
Quick Look Report #2: Rapid Characterization of Ahura's FirstDefender for Bulk Explosives Identification	June
Quick Look Report #2: Characterization of American Innovations' XD-2i with REF Reagent Formulations for Explosive Detection	June
Characterization of AS&E ZBV Militarized Trailer (ZBV MilT) and SAIC Trailer-Mounted Military Mobile VACIS (T-MMV) for Detection of Vehicle Borne Threats	June
Quick Look Report #3: Rapid Characterization of Ahura's FirstDefender for Bulk Explosives Identification	August
Quick Look Report #3: Characterization of American Innovations' XD-2i with REF Reagent Formulations for Explosive Detection	August
Final Report: Characterization of American Innovations' XD2i for Explosive Detection – Standard and REF Formulations	September
COTS Evaluation of Rapiscan's GaRDS (Gamma Ray Detection System) Gantry for the Detection of Vehicle Borne Threats	October
Final Report: Rapid Characterization of Ahura's FirstDefender for Bulk Explosive and Explosive Precursor Identification	October
Quick Look Report #4: Rapid Characterization of Ahura's FirstDefender for Identification of Desensitized Homemade Explosives (classified)	October
Rapid Evaluation of RedX Defense's XPAK2 for Explosive Detection (Updated version April 2009)	December
Characterization of Commercial Off-The-Shelf (COTS) Handheld Explosive Detection Equipment (HHEDE) for Trace Explosive Detection	December
2007	
Characterization of the ChemSpectra XD-Prototype for Explosive Detection	February
Detection Capabilities of the QinetiQ SPO-20 Passive Millimeter Wave (PMMW) Sensor Against Person-Borne Threat Devices	February
Characterization of the Scintrex Trace VE6000 for Explosive Detection of Vehicle Borne Threats	July
Characterization of Commercial-Off-The-Shelf (COTS) Desktop Explosive Detection Equipment (DTEDE) for Trace Explosive Detection	September

Comparative Studies and Evaluations of COTS Explosive Detection Equipment (EDE) (cont.)

2006	
Detection Capabilities of the Trex Enterprises ST150 Passive MMW Imager Against Human-Carried Threat Devices	January
The Detection Capabilities of the QinetiQ SPO-20 Passive Millimeter Wave Sensor Against Human-Carried Threat Devices	February
The Characterization of the Implant Sciences QS-H100 REV C for Explosive Detection	February
Determining the ZBV Ability to Enable Detection of Organic Material	February
Test Report: Characterization of the AS&E Forwardscatter Z-Backscatter Van (FSD-ZBV) for Detection of Vehicle Borne Threats	November
Phase I Data Collection Using the Phillips ACQSIM–CT System for Explosive Detection	December
2005	
Characterization of Shaped Energy X-ray Inspection System	May
QinetiQ SPO-20 Passive Millimeter Wave (PMMW) Experimental Testing to Determine Detection Capabilities Against Human Carried Explosives Containing Metal	May
The Characterization of the Implant Sciences QS-H100 for Explosive Detection	May
Biosensor for Explosive Detection Foreign Comparative Study	July
2004	
Portal Explosive Detection Equipment Comparative Study	May
Vehicle Explosive Detection Equipment X Ray (VEDEX) Comparative Study	December
2003	
Evaluation of EDE for Detecting Explosives in Mail and Small Parcels (contracted TSA)	July
2002	
Comparative Study of Desktop and Handheld Trace EDE	December

Comparative Test and Evaluation (T&E): Colorimetric Trace Explosive Detection Device (EDE)

A Comparative Study for Colorimetric Trace systems, funded by the Physical Security Equipment Action Group (PSEAG), was completed at the end of July 2010. The purpose of the test was to assess the capabilities, limitations, and military utility of currently available Colorimetric Trace systems. Colorimetric systems detect explosives through resulting color changes.

Requirements:

- Navy Urgent Operational Needs Statement (UONS) (Portable chemical, biological, radiological, nuclear and high-explosive / weapon of mass destruction (CBRNE/WMD) Detector)
- Improvised Explosive Device Defeat (IEDD) Initial Capabilities Document (ICD)
- Joint Service Explosive Ordnance Disposal (JSEOD) ICD
- Integrated Unit Base Installation Protection (IUBIP) Joint Capabilities Document (JCD)

Accomplishments:

- Testing conducted from December 2009 to July 2010
- Prepared a presentation for the Counter-IED Senior Integration Group (CSIG) and U.S. Central Command (USCENTCOM) on the results of a rapid assessment of the systems for use in Afghanistan

Key Dates / Milestones:

- Publish Report: January 2011

Comparative Test and Evaluation (T&E): Short Range Threat Detection

A Comparative Study for Short Range Threat Detectors commenced in Fiscal Year (FY10). The Broad Agency Announcement (BAA), based on Joint Urgent Operational Needs Statement (JUONS) CC-0315 person-borne improvised explosive device / vehicle-borne improvised explosive device (PBIED/VBIED) Detect and Defeat, was published in on December 6, 2009. Initial evaluation of systems took place in February 2010 and testing commenced in June 2010, with the Brijot Gen 2A system. All data collection has been completed on the Brijot Gen 2A, L-3 Provision, Millivision Portal and Walkthrough, Thermal Matrix ACT, Smiths Eqo, and SET Corp. CounterBomber systems. The capabilities and limitations of each of the submitted systems will be complied in a report detailing the current status of short-range threat detection as it pertains to explosive threats.

Requirements:

- Analysis of Alternatives (AoA) for High Fidelity Weapons of Mass Destruction Identification, April 2009
- JUONS, CC-0315, March 2008
- Integrated Unit, Base Installation Protection Initial Capabilities Document (ICD), 13 July 2007
- Improvised Explosive Device Defeat ICD, 23 February 2006
- Integrated Base Defense Security System Capability Development Document (CDD), 17 February 2005
- U.S. Central Command (USCENTCOM) FY10-15 Integrated Priority List (IPL), 15 January 2008

Accomplishments:

- Selected systems submitted in response to the BAA
- Completed the Test Plan and received manufacturer training on all the systems
- Initiated data collection, system testing, and user analysis

Key Dates / Milestones:

- Testing Commenced: June 2010
- Publish Report: February 2011

Correlation of Physical Security Radars to Identify Friend or Foe

The Correlation of Physical Security Radars to Identify Friend or Foe (IFF) is designed to track authorized personnel and integrate this information for transfer and display on an established Command Control and Display System. The project is intended to operate in the air base defense environment and improve situational awareness outside the perimeter of an installation or specific restricted area. The effect is improved management, via a standardized interface display, of targets detected with wide area radar sensors. System operators can select a display that filters out authorized activity, thus permitting them to more easily identify unknown or unauthorized sensor detections and conduct assessment of the activity or direct responding patrols, as required. In Fiscal Year 2010 (FY10) a developmental test demonstrated the successful correlation of three radar sensors, integration with the established Air Force Security Forces command and control display equipment; and a 30% reduction in the number of individual tracks on the operator's display. The project has been expanded to personnel tacking and evaluation of suitable commercial-off-the-shelf (COTS) equipment will be conducted in FY11.

Requirements:

- Integrated Base Defense Security Systems Capability Development Document (CDD), 17 February 2005
- Department of Defense Nuclear Weapon Security Manual (U) DoD S-5210.41-M, Volume 1, 13 July 2009

Accomplishments:

- Issued Development Test and Evaluation Report (09-342)
- Developed IFF Personnel Tag specifications, including establishment of performance requirements and verification methods
- Issued Request for Information for IFF Personnel Tags and analyzed industry responses

Key Dates / Milestones:

- Developed Draft concept of operations (CONOPS) and Correlator Capability Objectives: FY07
- Performed Initial Proof-of-Concept Demonstration: October 2007
- Scenario Testing with Operator Controls: July 2008
- Full-Function Testing: August 2009
- Development Test and Evaluation (DT&E): December 2009
- Correlator Combined Test Force (CTF) Evaluation: FY11
- Qualification Test and Evaluation (QT&E) for Commercial Position Tags: FY11
- Project End Date and Service Transition: FY12

Force Protection Equipment Demonstration (FPED)

The Force Protection Equipment Demonstration (FPED) was initiated by the Chairman of the Joint Chiefs of Staff as a result of the 1996 bombing at Khobar Towers in Saudi Arabia and subsequent findings of the Downing Report. FPEDs have been held every two years since 1997 under the sponsorship of the Department of Defense (DoD) Physical Security Equipment Action Group, administered by the Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters, and executed by the Product Manager, Force Protection System (PM-FPS). The purpose of the event is to bring together DoD and Federal leaders from around the world and put them in contact with manufacturers who may have equipment solutions for their physical security and force protection needs. The last two events conducted in 2007 and 2009 have generated more than $200 million dollars in sales to Federal agencies used to address critical security shortfalls.

Requirements:

- Downing Report, 30 August 1996
- Addresses urgent and compelling needs from the field
- Provides immediate commercial-off-the-shelf solutions

Accomplishments:

- Conducted survey after FPED VII to capture sales generated as a result of that demonstration ($106 million dollars)
- Identified venue and sponsors for FPED VIII
- Launched event web site and administrative databases
- Signed Memorandum and Hold Harmless Agreements with the Stafford Regional Airport Authority
- Awarded subcontracts for show management, multimedia and web based support services in support of Phase I of the planning sequence (1 January 2010 – 30 September 2010)

Key Dates / Milestones:

- Second Security Meeting: 12 January 2011
- Second Project Officer Group (POG): 31 March 2011
- FPED VIII: 17-19 May 2011
- Distribution of FPED VIII Compact Disks: July – October 2011

Handheld THz Spectrometers

The purpose of this project is to develop a handheld (less than 10 lbs) THz Spectrometer to detect and identify explosives. The identified signatures are then matched to the database within the system. This project has two performers, Rensselear Polytechnical Institute (RPI) and EMCORE. The two phase RPI project will develop a handheld THz explosive detector. Phase I was a 12-month effort to develop and test an optical THz fiber laser that weighs less than 10 lbs. After satisfactory completion of Phase I, Phase II has been funded to gather spectroscopy measurements and integrate all electronics into a lightweight handheld explosive detector. The Explosive Detection Equipment (EDE) Program has been concurrently testing the developed systems. At the end of Phase II, three prototype handheld spectrometers will be delivered, along with the design documents, to undergo full testing (lab and field). EMCORE is developing a second Handheld Spectrometer that differentiates from RPI in the techniques by which the system works; emphasizing Frequency Domain Spectrometry (FDS) instead RPI's Time Domain Spectrometry (TDS).

Requirements:

- Integrated Unit, Base Installation Protection Joint Capabilities Document (JCD), 13 July 2007
- Joint Urgent Operational Needs Statement CC-0255, 26 September 2007
- Improvised Explosive Device Defeat Initial Capabilities Document (ICD), 23 February 2006
- Portable Chemical, Biological, Radiological, Nuclear and High Explosive (CBRNE) / Weapons of Mass Destruction Detector, Navy Urgent Operational Needs Statement, 31 December 2006
- Integrated Base Defense Security System Capability Development Document (CDD), 17 February 2005
- Joint Service Explosive Ordnance Disposal ICD, 1 June 2005
- CBRNE Sense ICD, 8 June 2005

Accomplishments:

RPI:

- Developed and demonstrated a light weight THz optical system
- Performed spectroscopy measurements of explosives and created a database
- Integrated the optics and the database to produce an entire handheld system weighing less than 10 lbs

Emcore:

- Collected spectroscopy on explosives at Naval Explosive Ordnance Disposal Technology Division (NEODTD)
- Designed and built an inexpensive, portable, battery operated, high speed, THz spectrometer
- Integrated fiber-based optics with phase control ability
- Demonstrated both transmission and reflection measurement modalities

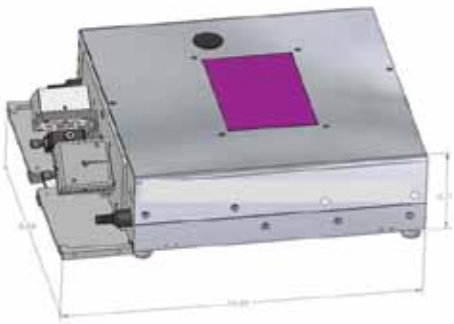
Key Dates / Milestones:

RPI:

- Deliver Ruggedized Prototypes: March 2011

Emcore:

- Deliver Prototype: January 2011
- Conduct T&E on Both Systems: April 2011



Integrated Defense Command and Control Common Operating Picture (IDC2COP)

The Integrated Defense Command and Control Common Operating Picture (IDC2COP) is being developed to support the United States Air Force (USAF) Security Forces mission at garrison locations and in expeditionary environments. IDC2COP provides law enforcement, force protection, and emergency management personnel with a variety of incident management capabilities such as automated incident management plotting, base defense planning, and quick response checklists. Its components include a map-based Common Operating Picture (COP) which fuses contingency planning tools, physical security sensors, assessment devices and blue-force tracking into a single display. Information generated by the system is shared across the operational domain through a self-forming, self-healing network utilizing role-based data sharing rules. In 2010, IDC2COP was integrated into the Joint Force Protection Advance Security System (JFPASS) Joint Capability Technical Demonstration (JCTD).

Requirements:

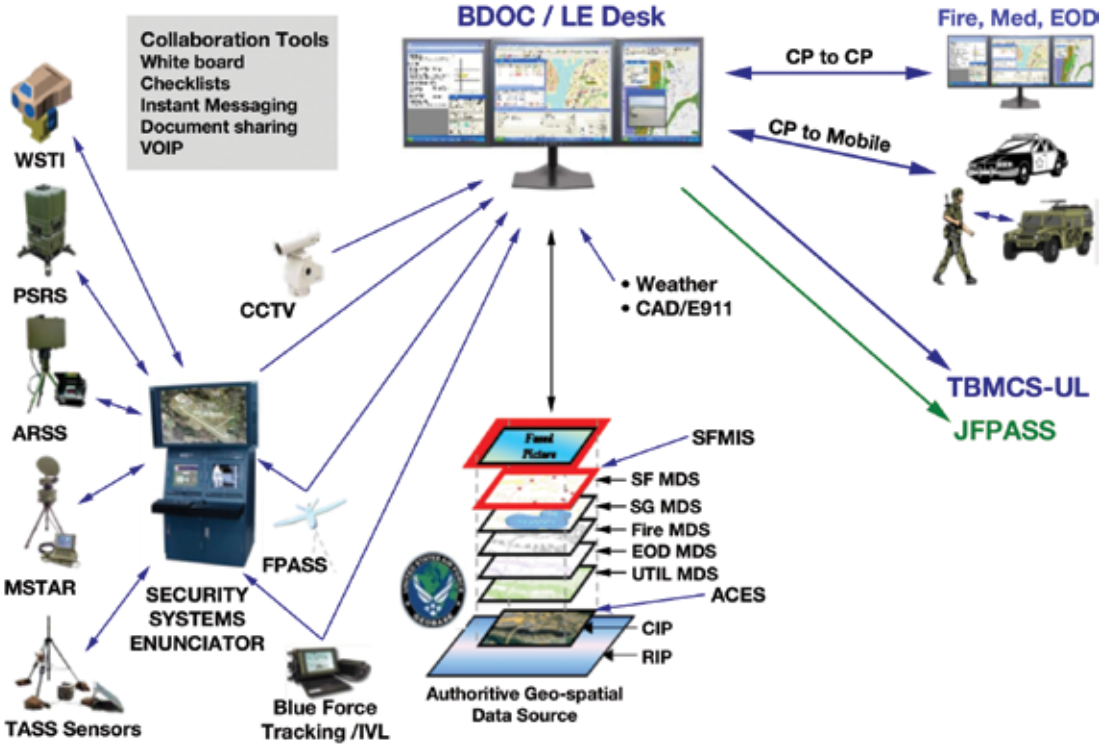
- USAF command and control concept for prototype Base Defense Operations Center (BDOC)
- Security Equipment Integration Working Group (SEIWG) architecture requirements
- Integrated Base Defense Security Systems (IBDSS) Capability Development Document (CDD), 17 February 2005

Accomplishments:

- Received Interim Authorization to Operate
- Conducted an operational demonstration at an active-duty installation

Key Dates / Milestones:

- Conduct operational deployments at several active-duty installations: Fiscal Year 2011 (FY11)
- Develop interfaces for Air Force Security annunciators and integrate with external legacy systems: March 2011
- Project End Date: 2011



Integrated Ground Security Surveillance Response – Capability (IGSSR-C)

The Integrated Ground Security Surveillance Response - Capability (IGSSR-C) is a Joint requirement to provide a layered approach to integrate sensors, sensor systems and unmanned systems with automated fusion capabilities to create an in-depth security, surveillance and response Force Protection (FP) Common Operational Picture capability for fixed, semi-fixed or expeditionary elements in all operating environments. This capability will enable rapid decision analysis, speed the response process and increase information dissemination along the chain of command, and with outside supporting organizations. The desired end state is to achieve interoperability with current and emerging FP systems used by Joint Forces, DoD agencies and multi-national forces. The desired objective is the ability to communicate and standardize rapid warnings to designated recipients throughout the Joint Services and agencies. The IGSSR-C will provide the critical ability to fuse detected activity information, regardless of format, that is mutually supporting across services and agencies. The goal is to develop a set of software centric capability solutions that will be scalable, modular and tailor-able to fixed, semi-fixed or expeditionary Joint Force installations.

Requirements:

Applicable Joint Capabilities Integration and Development System (JCIDS) requirement documents supporting this development effort are:

- Draft IGSSR-C Capability Development Document (CDD)
- Integrated Unit, Base Installation Program (IUBIP) Joint Capabilities Document (JCD), 17 July 2007
- IUBIP Capabilities Based Assessment (CBA), September 2007
- IUBIP Detect Assess Defend (DAD) Initial Capabilities Document (ICD), 2 October 2009
- IUBIP Interoperability Initial Capabilities Document (ICD), 15 September 2009
- Consequence Management (CM) ICD, 17 September 2010
- Chemical, Biological, Radiological, and Nuclear Consequence Management ICD, 13 April 2006
- Joint Urgent Operational Needs Statement (JUONS) # CC0201, CC0202, CC0214, CC0216, CC0235, CC0239, CC0240, CC0241 and CC0262

Accomplishments:

- Completed review and drafting support to Maneuver Support Center of Excellence (MSCoE) for the draft IGSSR-C CDD and the Army Requirements Oversight Council (AROC) CDD briefing
- Generated Incremental Technology/Capability Development Strategy and draft performance specification
- Published and assessed responses to a Request for Information to identify industry “fusion” solutions
- Prepared, coordinated and initiated staffing of the Milestone Decision Document (MDD) briefing and supporting documentation

Key Dates / Milestones:

- Project Start Date (Increment 1 Initiated) - 1 May 2010
- Increment 1 Milestone (MS) A: March 2011
- Increment 1 MS B: 2QFY12
- Increment 1 MS C: 2QFY14
- First Unit Equipped (FUE): 4QFY14
- Project End Date (Increment 3 MS C) - 30 September 2017

Interim Integrated Base Defense (I-IBD)

The Interim Integrated Base Defense (I-IBD) Program is designed to improve integration and interoperability of existing base defense systems leading to improved base operations. These improvements include automated display of threat data, fusion and correlation of base defense information via a common Graphical User Interface, assessment and dissemination of threat information, and reduction of troop-to-task ratio and training requirements. Efficiencies in base defense operations will be achieved through reduction of duplicative capabilities and support requirements. I-IBD is net-centric and able to operate within existing base local access network (LAN) and CENTRIX infrastructure with no new hardware or additional manning. The performance of existing integration systems and technologies such as Standard Ground Station and Joint Force Protection Advanced Security System will be enhanced through this development effort.

Requirements:

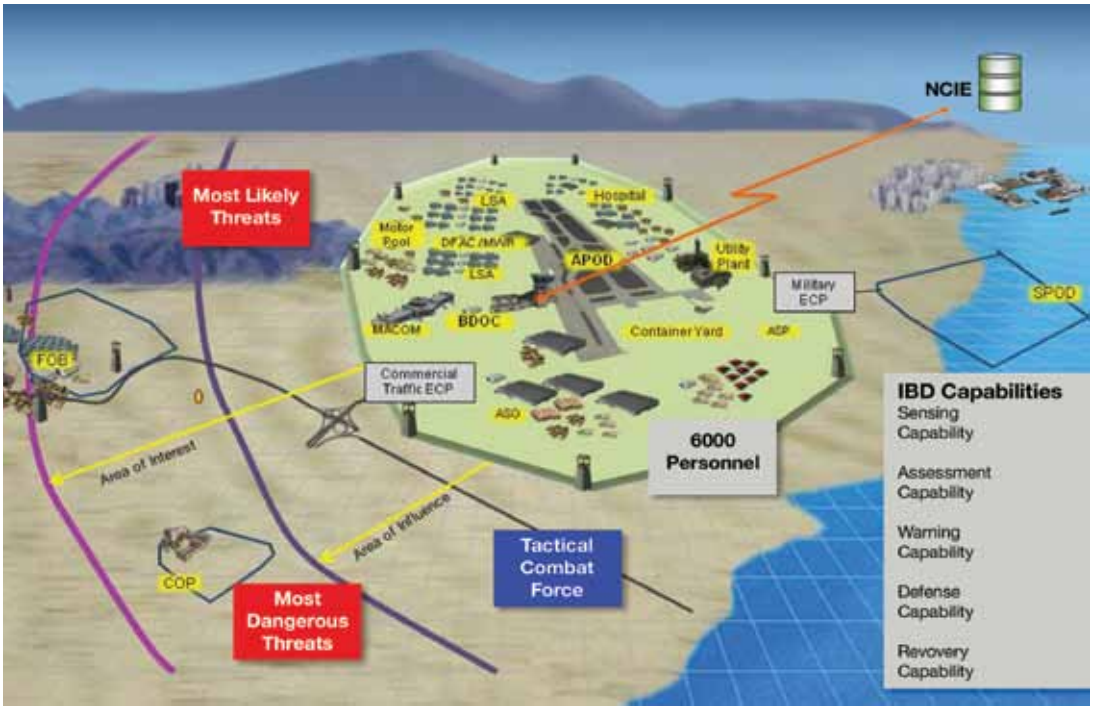
- U.S. Central Command (USCENTCOM) Issue Paper #5 identifying the need for integrated theater base defense operations and harmonized base defense systems and supporting technologies

Accomplishments:

- Completed I-IBD requirement analysis of over 30+ existing base defense systems to identify and prioritize technical requirements and development gaps; approximately eight systems were selected for initial integration development
- Completed technical analysis including the development of I-IBD System Connectivity Diagrams, interface requirement data definition and information exchange schema

Key Dates / Milestones:

- Initial Fielding Scheduled: 31 July 2011



ACTIVITIES

Joint Conflict and Tactical Simulation Enhancements (JCATS)

The Joint Conflict and Tactical Simulation (JCATS) software program is a constructive battlefield simulation of conflict, at the individual soldier and vehicle levels. This software program has been available since the 1980's and is used in modeling and simulation, and by the Services in determining possible outcomes for force-on-force exercises / training. The program is updated continually, and there is a Joint-Service board that oversees the upgrades and incorporates them into the software. For example, during 2010, the board requested that the Defense Threat Reduction Agency (DTRA), in partnership with the Lawrence Livermore National Laboratory (LLNL), develop a three-dimensional (3D) visualization enhancement (including: custom configuration, 3D models and textures, and 3D view for the JCATS Analyst Workstation) for the software.

Requirements:

- Joint-Service Board with oversight responsibility for JCATS upgrades and enhancements

Accomplishments:

- Completed three-dimensional (3D) visualization enhancement and incorporated into current version, JCATS 9.0
- Developed additional enhancements to the Analyst Workstation, support analysis, wide area network (WAN), and the capability to model persistent chemicals on the battlefield; incorporated these into JCATS 10.0 (2011 delivery)

Key Dates / Milestones:

- Project End Date: Fiscal Year 2011 (FY11)

Joint Force Protection Advanced Security System (JFPASS) Joint Capabilities Technology Demonstration (JCTD)

The purpose of the Joint Force Protection Advanced Security System (JFPASS) Joint Capabilities Technology Demonstration (JCTD) is to demonstrate the value of linking disparate Force Protection, Physical Security, Chemical Biological Radiological and Nuclear, and Incident Management systems into an integrated system of systems that reduces risks to U.S. forces, optimizes the use of manpower, and increases the commander's overall level of situational awareness. JFPASS is able to achieve these objectives through three functions: Fusion, Automation, and Integration. The heart of JFPASS is a data fusion engine that integrates multiple systems (e.g., gate access control and robotic systems) through the use of common interface standards within enterprise systems architecture. By integrating systems via a common architecture, the JFPASS fusion engine is able to apply correlation algorithms and leverage the strengths of each sub-system; thus allowing the system user to focus primarily on the "warn" and "response" functions. The JFPASS JCTD strategy consists of technical demonstrations (TD), led by the Technical Manager and operational demonstrations (OD), led by the Operational Manager; conducted at continental United States (CONUS) and outside the continental United States (OCONUS) installations.

Requirements:

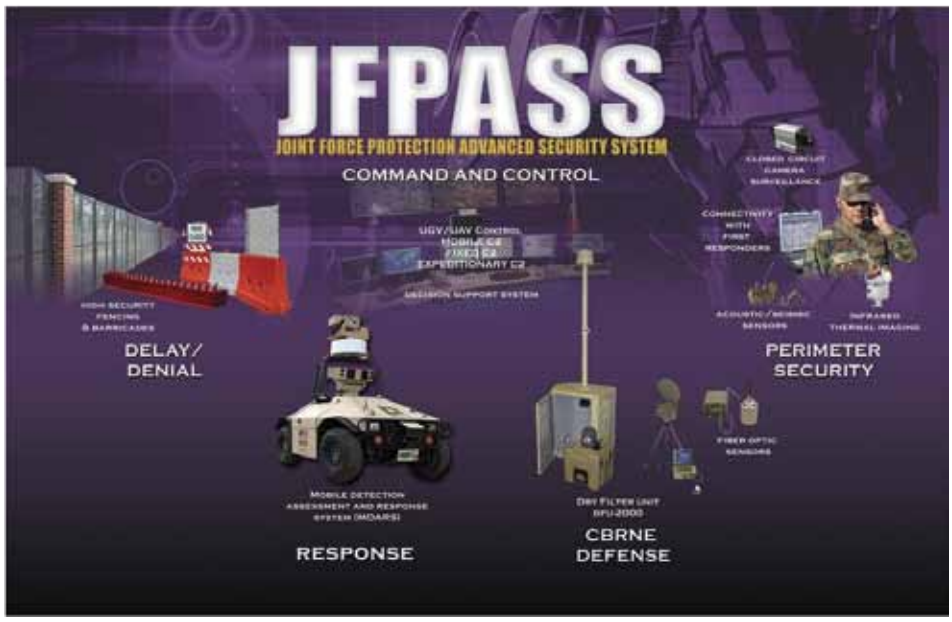
- U.S. European Command nominated this JCTD as a number one priority.
- Interoperability and Detect Assess Defend Initial Capability Documents resulting from the Integrated Unit, Base, and Installation Protection Capabilities-Based Analysis

Accomplishments:

- Conducted TD-2 and OD-2 at an operational OCONUS facility
- Assisted the Army in creation of the Integrated Ground Security, Surveillance and Response Capability Development Document for New Start program in Fiscal Year 2012 (FY12)
- Worked with the Rapid Equipping Force to field a system, the Combat Outpost Security System, which includes core JFPASS components
- Worked with North Atlantic Treaty Organization (NATO) partners for possible inclusion in Rapid Acquisition Program
- Worked with Interim Integrated Base Defense team to include capabilities in future U.S. Central Command (USCENTCOM) requirements

Key Dates / Milestones:

- Project Start Date: FY08
- Extended Use/Military Utility Assessment/Final Report: FY11
- Project End Date: FY11



ACTIVITIES

Lighting Kit, Motion Detector (LKMD)

The Lighting Kit, Motion Detector (LKMD) is a simple, compact, modular, sensor-based early warning system that provides a programmable response set of illumination and sound, resulting in increased operational reaction time for individuals, teams, squads, or platoons. LKMD may be used as a tactical, stand-alone system or as a supplemental device for use with other security systems or missions. LKMD is designed to provide early detection and warning in order to enhance force effectiveness and increase situational awareness during all types of combat operations or missions ranging from small scale contingencies and Military Operations in Urban Terrain up to high intensity combat. In all scenarios or environments, LKMD will provide the individual, team, or unit leader an increased ability to monitor more terrain longer with fewer personnel resources. Using the system as a part of an integrated, large, in-depth and layered situational awareness concept will further enhance force protection. A total of 8,800 systems are in production, with fielding to begin in Fiscal Year 2011 (FY11).

Requirements:

- Capability Production Document, 14 April 2008

Accomplishments:

- Awarded Delivery Order for Full Rate Production (8,800 systems)
- Successfully completed Performance Verification Testing

Key Dates / Milestones:

- Project Start Date: March 2003
- Project End Date: June 2009
- First Unit Equipped: 25 September 2010

Long-Range 3D THz Radar Imager

Tera-Hertz (THz) technology is being evaluated to rapidly screen personnel from a standoff distance for person-borne improvised explosive devices (PBIED). The Explosive Detection Equipment (EDE) Program manages a coalition consisting of subject matter experts from Jet Propulsion Lab (JPL), and Naval Facilities Engineering Support Center (NFESC). The current prototype, a collected image, and the envisioned final prototype are shown below. Efforts are also currently underway to produce a transportable prototype. This effort is scheduled to be funded for Joint Service Explosives Ordnance Disposal (EOD) development and acquisition beginning in Fiscal Year 2012 (FY12).

Requirements:

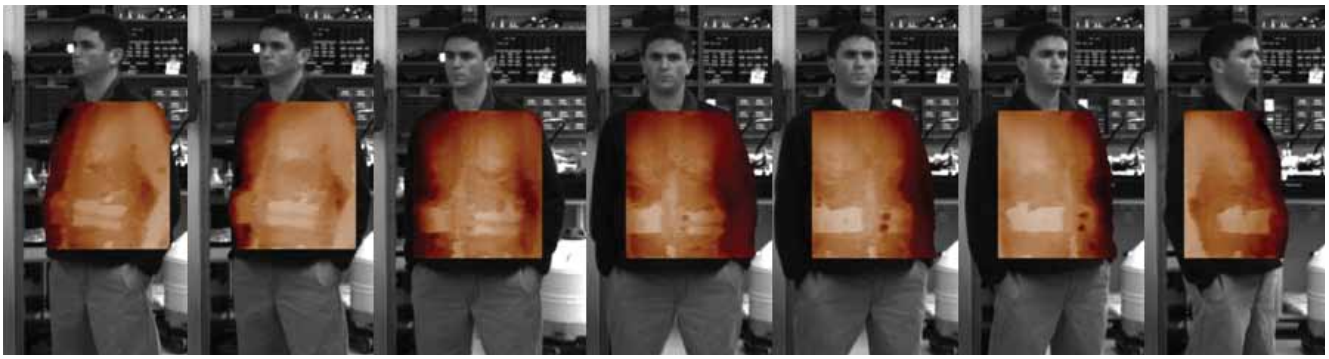
- Analysis of Alternatives (AoA) for High Fidelity Weapons of Mass Destruction Identification, April 2009
- Joint Urgent Operational Needs Statement, CC-0315, March 2008
- Integrated Unit, Base Installation Protection Initial Capabilities Document (ICD), 13 July 2007
- Improvised Explosive Device Defeat ICD, 23 February 2006
- Integrated Base Defense Security System Capability Development Document (CDD), 17 February 2005
- U.S. Central Command (USCENTCOM) FY10-15 Integrated Priority List (IPL), 15 January 2008

Accomplishments:

- Developed a THz 3D Imager, with increased standoff distance and reduced scan time; ruggedized and reduced system weight

Key Dates / Milestones:

- Deliver Rugged Prototype: June 2011
- Conduct Realistic PBIED test and evaluation (T&E) in Outdoor Environment: July 2011



National Air Space Integration Demonstrator for Small Tactical UAS (STUAS) Alarm Response

The Air Force Research Laboratory (AFRL/RXQF) is currently involved in the research and development of a National Air Space Integration Demonstrator for Small Tactical Unmanned Aerial System (STUAS) Alarm Response. This project is a Sense and Avoid payload development effort to support the United States Air Force (USAF) and United States Navy (USN) acquisition of the STUAS II platform. The effort will produce an approved means to fly a UAS from military airspace to an alarmed perimeter under the Class G airspace in an alarm response action prior to a Quick Response Force (QRF) being deployed. The developed payload will be standardization agreement (STANAG) 4586 compliant, utilize the USAF's Vigilant Spirit ground control, and will be ready for integration into STUAS II. The system will be evaluated with the USAF 90th Space Wing 90th Ground Combat Training Squadron (GCTS) at Camp Guernsey. This project had previously been working on a convoy support UAS and in October 2010 was realigned with Air Force Special Operations Command (AFSOC) and USAF needs to support domestic capability gaps in the upcoming STUAS II acquisition.

Requirements:

- Integrated Base Defense Security System (IBDSS)
- Office of the Secretary of Defense (OSD) Airspace Integration Plan for Unmanned Aviation
- USAF Unmanned Aircraft Systems Flight Plan 2009-2047
- STUAS Capability Development Document (CDD)

Accomplishments:

- Vigilant Spirit OCU Integration Phase I
- Down-selected Technology Readiness Level (TRL) 6-7 Sense & Avoid technologies for integration/testing in Fiscal Year 2011 (FY11)
- Completed demonstrator UAS fabrication
- Prepared for new guidance from AFSOC representative
- Began development of STUAS II "hub-and-spoke" concepts of operation for integration of unmanned systems into USAF 90th Security Forces Group's domestic training operations for alarm response

Key Dates / Milestones:

- Project Start Date: 9 November 2009
- Next milestone: Interim Program Review, Flight Test Plan Review
- Project End Date: 20 September 2012

Physical Security Equipment Action Group (PSEAG) Strategic Plan

The foundation of the Physical Security Equipment Action Group (PSEAG) dates back to 1976. The PSEAG was originally formed to more effectively pursue Department of Defense (DoD) solutions to physical security challenges by assisting in the requirements harmonization process and preventing duplications within research, development, test and evaluation (RDT&E) efforts across the services. These two responsibilities remain the focus of the PSEAG today, some 34 years later. In 1989, PSEAG changed substantially with the consolidation of the Services funding at the Office of the Secretary of Defense- (OSD) level for these efforts. As the PSEAG process has matured through the years and greater awareness and effort has been placed on physical security programs across the DoD, it has become paramount that unity of effort, coordination, and efficiencies be leveraged throughout the PSEAG program. In coordination with the physical security stakeholders from across the DoD, the development of a PSEAG Strategic Plan -- consisting of a Vision Statement, Mission Statement, Goals, Objectives, Strategies and Metrics -- will help focus efforts, ensure program wholeness and maximize long-term effectiveness. In order to meet the strategic goals, 22 initiatives were recommended for implementation. The implementation and execution of the approved initiatives will help ensure PSEAG remains a relevant organization that continues to make significant contributions. The application of strategic guidance will result in sound management processes, the best return on investment of limited RDT&E funds and ultimately, a viable program that supports all components of DoD.

Requirements:

- DoD Instruction 3224.03, October 2007
- DoD PSEAG Letter of Instruction, October 2007

Accomplishments:

- Developed and reached consensus agreement on PSEAG Vision Statement, Mission Statement and Goals
- Completed PSEAG Strategic Plan 2011-2015 Final Report
- Within the Strategic Plan development process, identified 22 initiatives that will facilitate meeting the Strategic Goals outlined within the plan
- Developed an implementation plan for consideration by PSEAG leadership to execute the 21 initiatives

Key Dates / Milestones:

- Project Start Date: June 2010
- Project End Date: December 2010

Physical Security of Storage Magazines - Doors

Improved attack technology has advanced to the point where conventional weapon storage magazines often do not meet physical security requirements. Magazine doors on structures used for storage of arms, ammunition and explosives (AA&E) must provide a known delay time against forced entry attacks. Fiscal Year 2010 (FY10) tasks also included integrating the door with a protected Internal Locking Device (ILD) system with a thermal relocker.

Requirements:

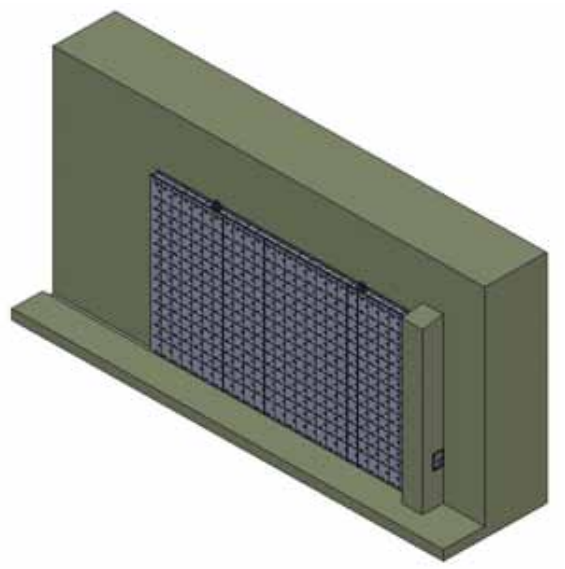
- Department of Defense Directive (DoDD) 5100.76M
- Delay and Denial – Office of the Assistant Secretary of Defense for Command, Control, Computers, and Intelligence (OASD (C3I)) Memo, 3 October 2001
- Office of the Under Secretary of Defense for Intelligence (OUSD(I)), Memo, 22 May 2003
- Naval Region Marianas (NRM) and Pacific Air Forces (PACAF), Eglin AFB
- Integrated Unit, Base Installation Protection (IUBIP) Initial Capabilities Document (ICD), January 2008
- Capability Gap Priority 19

Accomplishments:

- Red team testing of door panel design
- Design and testing of thermal relocker
- Prototyping and testing of integrated ILD locking system

Key Dates/ Milestones:

- Project Start Date: October 2006
- Project End Date / Final Report and Design: September 2010



Shipboard Security Containers

This project identifies security, operational, and functional requirements for shipboard security containers to ensure these containers meet storage, shock, vibration and mounting requirements. In coordination with the Chief of Naval Operations, Naval Sea Systems Command (NAVSEA), and Shipbuilders, tasks for this project include the development of Government Services Administration (GSA)-approved shipboard security containers and mounting systems; federal specifications for testing equipment for usage in shipboard and other harsh environments; and updates to policy requirements to mitigate current security vulnerabilities and standardize protection of classified information aboard ship. The current generation of products developed ensure that shipboard security containers are able to stay in place during all sea states, are operable when needed, and do not modify the GSA container in any significant manner. The new lightweight container products developed from this effort will meet the performance requirements of GSA Class 6 containers, also meeting environmental, functional, and operational requirements. Once the manufacturers' products are approved through GSA testing, they will be available for procurement.

Requirements:

- Federal Specification FF-L-2740
- Chief of Naval Operations Instruction (OPNAVINST) 5530.13C, September 2003
- N09/N2 requirement for containers to meet GSA Class 6 guidelines

Accomplishments:

- Completed final design for GSA Class 5 and 6 Container Drawer Insert for classified laptop storage
- Completed final test and evaluation on the Phase II shipboard security container with pedestal bottom
- Finalized and approved revision to Federal Specification AA-F-358H
- Awarded contract to manufacture prototype GSA Class 5 and 6 container drawer insert for classified laptops

Key Dates / Milestones:

- Project Start Date: October 2008
- Phase III Drawer Insert delivery: February 2011
- Drawer Insert Test and Evaluation: March-May 2011
- New Lightweight Container Capabilities Recommendations: April 2011
- Phase III Policy and Fed Specs Updates: July 2011
- Lightweight Container Proof of Concept Design: August 2011
- Phase III Transition: September 2011
- Lightweight Container Test and Evaluation: March 2012
- Lightweight Container Specification: December 2012
- Lightweight Container Transition: March 2013
- Project Transition Date: September 2013

Tactical Surveillance System (TSS)

The Tactical Surveillance System (TSS) is a modular, scalable system, that will be tailorable to support both short and long term security and surveillance requirements, enabling the Commander to detect, locate, characterize, identify and track activities of interest. It enhances the Commanders' situational awareness by providing Near-Real-Time imaging sensors that increase security and improve the ability to counter threats at greater ranges. Being left in place for extended periods of time, TSS provides a dedicated surveillance capability that is unaffected by changing ambient light levels and environmental conditions. TSS will be capable of transmitting video, audio and control signals, and providing a manual, automatic, or programmable slew-to-cue capability; as well as monitoring other security sensors such as the Lighting Kit, Motion Detector and Battlefield Anti-Intrusion System. Additional capabilities include monitoring Military Police Theater Internment Facilities, and providing persistent surveillance in support of Combat Engineer Route Clearance operations.

Requirements:

- Draft TSS Capabilities Development Document (CDD)
- Soldier as a System (SaaS) Initial Capabilities Document (ICD), 21 October 2005
- Joint Explosive Hazard Defeat (JEHD) ICD, 1 May 2006
- Integrated Unit, Base Installation Protection (IUBIP) Detect Assist Defend, Initial Capabilities Document (ICD), February 2008
- Operational Needs Statement (ONS), CC-0143, CC-0296h
- Joint Urgent Operational Needs Statement (JUONS), CC-0073, CC-0296g

Accomplishments:

- Submitted the draft CDD for final review to the Maneuver Support Center of Excellence (MSCoE)
- Completed Program Affordability Analysis for the CDD
- Prepared a Total Life Cycle Cost Estimate for the CDD
- Generated a Cost Benefit Analysis to the CDD

Key Dates / Milestones:

- Project Start Date: 1QFY04 [then called Tactical Video Surveillance System]
- Start of World Wide Staffing: December 2010 (Anticipated)
- Materiel Development Decision: September 2011 (Anticipated)

Waterside and Shipboard Security – Sonar Augmentation

The Sonar Augmentation program has been working on utilizing both passive and active clues to better classify targets of interest identified by an active swimmer detection system. The project started by 'looking between the pings' at the radiated noise down a particular beam that had been identified by the active targeting portion. Signatures associated with diver noise were then used to create replicas for comparison to the signals received at the sound head. Ongoing work has begun to concentrate on the details within the active return. Currently the project is focused on feature extraction from the active portion of known data sets containing both real and false targets.

Requirements:

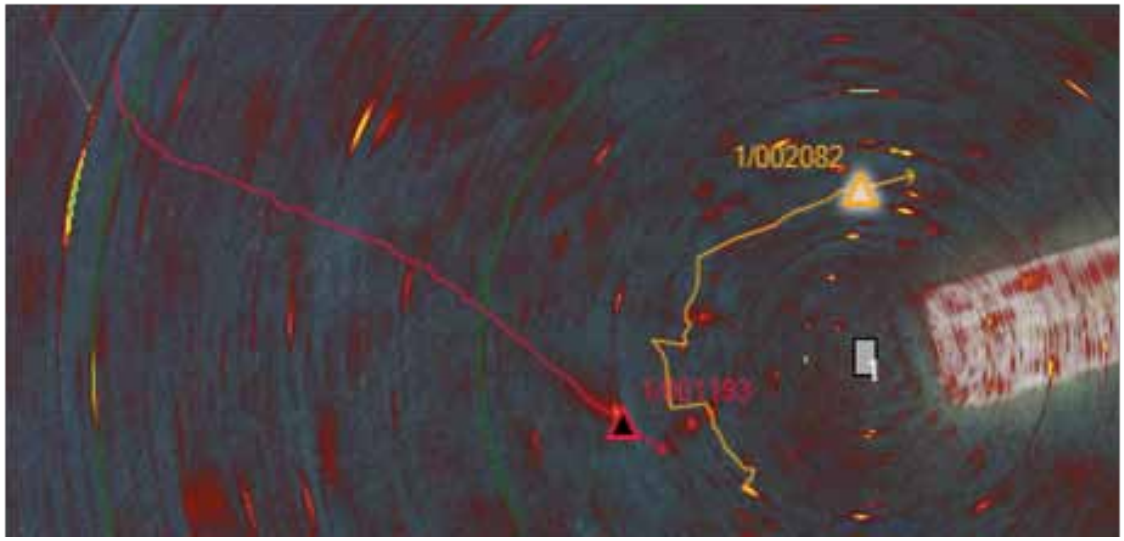
- Maritime Expeditionary Security Force (MESF) Initial Capabilities Document (ICD) & Draft Capability Production Document (CPD) – currently at Chief of Naval Operations (OPNAV)
- Anti-Terrorism / Force Protection (ATFP) Ashore Fiscal Year 2008 (FY08) Program Execution Guidance
- Integrated Swimmer Defense (ISD) User Operational Evaluation System 2 (UOES2) Letter of Requirements Matrix

Accomplishments:

- Algorithm produced target classification in less time than that required by the commercial-off-the-shelf (COTS) system
- Algorithm produced fewer false classifications of targets compared to the COTS system

Key Dates / Milestones:

- Project Start Date: FY10
- Project End Date (algorithm turned over to the Integrated Swimmer Defense Program): FY10



Waterside and Shipboard Security – Ultra Wide Band Radar

The Ultra Wide Band (UWB) Radar project utilizes a small perimeter security radar to create a tracking and classifying virtual fence capability. The ultimate goal of the project is to deliver a capability at a Technology Readiness Level (TRL) of 7-8 that can provide perimeter intrusion detection, target classification, and target track (limited field) through a virtual fence system. The virtual fence will provide a solution that is both more palatable to the environmental community in, and around the shore, and has the capability to discriminate between human and non-human targets.

Requirements:

- Naval Facilities Engineering Command (NAVFAC) Anti-Terrorism / Force Protection (ATFP) Ashore General Enclave Performance Specification
- Department of Defense (DoD) Directives 3020.40 and 3020.45
- DoD Instruction 2000.16, 5200.08, 5200.8R
- Chief of Naval Operations Instruction (OPNAVINST) 5530.14C Ch2

Accomplishments:

- Achieved real-time tracking
- Developed faster 3-D imaging
- Upgraded radio sets increased pole-to-pole spacing

Key Dates / Milestones:

- Project Start Date: Fiscal Year 2009 (FY09)
- Design Test: FY11
- Operational Test to meet AT-FP Ashore P-Spec: FY12
- Project End Date: FY12 (anticipated)

Weapons Tracking Seal

This project leverages approved Department of Homeland Security (DHS) and U.S. Transportation Command (USTRANSCOM) global communications and tracking tag concepts to provide an automated chain of custody for weapons and other assets. The Weapons Tacking Seal project will provide DoD with the following benefits: tamper evidence, improved situational awareness, targeting and interdiction capability in case of theft. The tracking seals used by DHS are reusable, ruggedized devices with a simple operator interface, which are interoperable in intermodal transport. Use of these tags within a structured, web-based Command, Control, Communications, Computer, and Intelligence (C4I) network provides material shippers with near real time situational awareness of the sealed shipment with regards to location, and information on container door openings. When used in conjunction with Advanced Container Security Device system, the proposed material tracking tags help system operators meet physical security and situational awareness requirements when shipping sensitive items.

Requirements:

- Integrated Based Defense Security System (IBDSS) Capability Development Document (CDD), February 2005, Detection, Access Control
- Navy Anti-Terrorism / Force Protection (ATFP) Ashore CDD 4.7, 4.8, 4.9 & 4.10
- Chief of Naval Operations (OPNAVINST) 5530.13C
- Department of Defense (DoD) 5200.08-R, 9 April 2007, Security of Controlled Inventory
- Defense Transportation Regulation (DTR) 4500.9-R

Accomplishments:

- Hazards of electromagnetic radiation to ordnance (HERO) Certification Tests completed for one commercial-off-the-shelf (COTS) item on all munitions, zero standoff; awaiting final approval letter

Key Dates / Milestones:

- Project Start Date: October 2009
- Concept Demonstration: August 2010
- Field Tests Complete: August 2011
- Performance Specification Available: May 2012
- Project End Date: September 2012

XD-4: Automated Handheld Colorimetric System

Colorimetric chemistry has a long-standing history as an explosive detection technique, through the utilization of specific chemicals which change color in the presence of explosives. However, traditional systems and kits which rely on colorimetric chemistry have limitations in that they require the operator to not only interpret if the chemical changed color in the presence of an explosive, but also to identify the explosive itself. In order to address these limitations, the Explosive Detection Equipment (EDE) Program has managed ChemSpectra's development of an automated handheld colorimetric explosive detection system. The ChemSpectra device, the XD-4, automatically notifies the uses of both the type and relative percentage of explosive encountered. Currently, three prototypes have been delivered to Naval Explosive Ordnance Disposal Technical Division (NAVEODTECHDIV) for test and evaluation.

Requirements:

- Navy Urgent Operational Needs Statement (UONS) (Portable chemical, biological, radiological, nuclear, and high-explosive / weapon of mass destruction (CBRNE/WMD) Detector)
- Improvised Explosive Device Defeat (IEDD) Initial Capabilities Document (ICD)
- Joint Service Explosive Ordnance Disposal (JSEOD) ICD
- Integrated Unit Base Installation Protection (IUBIP) Joint Capabilities Document (JCD)

Accomplishments:

- Manufacturer delivered three prototypes and provided training to NAVEODTECHDIV

Key Dates / Milestones:

- XD-4 Testing Commences: February 2011
- Test Report: May 2011

APPENDICES

DEPARTMENT OF DEFENSE

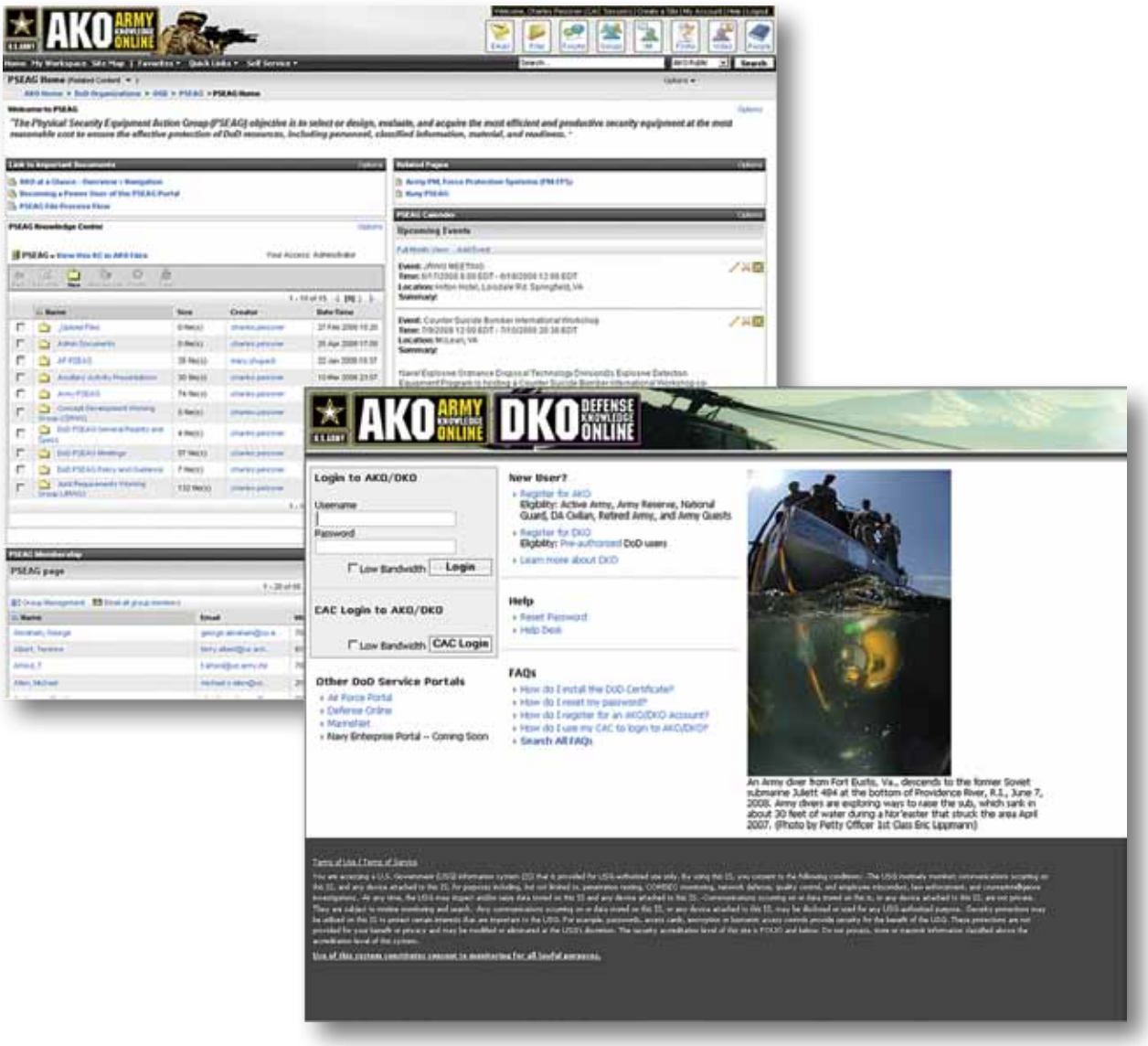
PSEAG

APPENDICES

Appendix A. Information Repository

The Physical Security Equipment (PSE) Research Development Test and Evaluation (RDT&E) Program uses the Army Knowledge Online (AKO) / Defense Knowledge Online (DKO) portal through which the Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters (OASD(NCB)/NM)) collaborates, shares, and transfers information to users in the field. The portal is designed to foster collaboration between force protection (FP) communities. In addition, it promotes and allows the collection, organization, and dissemination of information to its members. All registered portal users are able to access information and studies on the latest FP equipment and on policy documents that provide guidance on the development and use of physical security equipment.

To register / enroll for access to the AKO / DKO portal, visit: https://www.us.army.mil

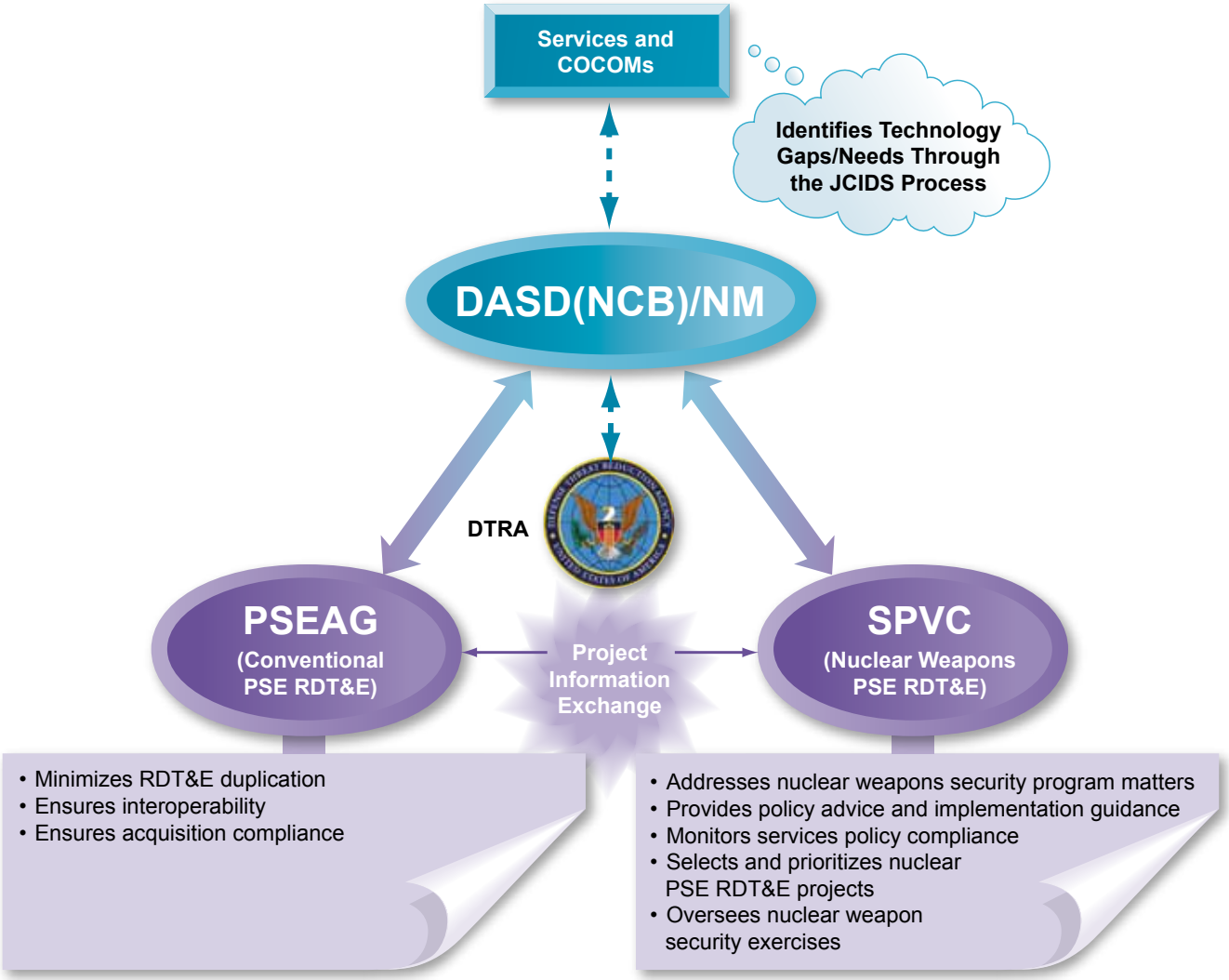


APPENDICES

Appendix B. The DoD PSE RDT&E Program Organization and Structure

The Department of Defense (DoD) Physical Security Equipment (PSE) Research, Development, Test and Evaluation (RDT&E) Program responds to the material needs expressed by the Services and the Combatant Commands (COCOMs). Physical security equipment capabilities, or gaps in capabilities, are identified by the COCOMs and Services via the Joint Capabilities Integration and Development System (JCIDS) in response to national- and Office of the Secretary of Defense (OSD)-level guidance. Requirements for the development of material solutions derived from this process may be referred to the Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters (OASD(NCB)/NM)) for DoD PSE RDT&E Program funding in advance of a defense acquisition milestone decision to implement an acquisition strategy to meet the capability need. The OASD(NCB)/NM) coordinates PSE material development with representatives from the Army, Navy, Air Force, Marine Corps, and the Defense Threat Reduction Agency (DTRA).

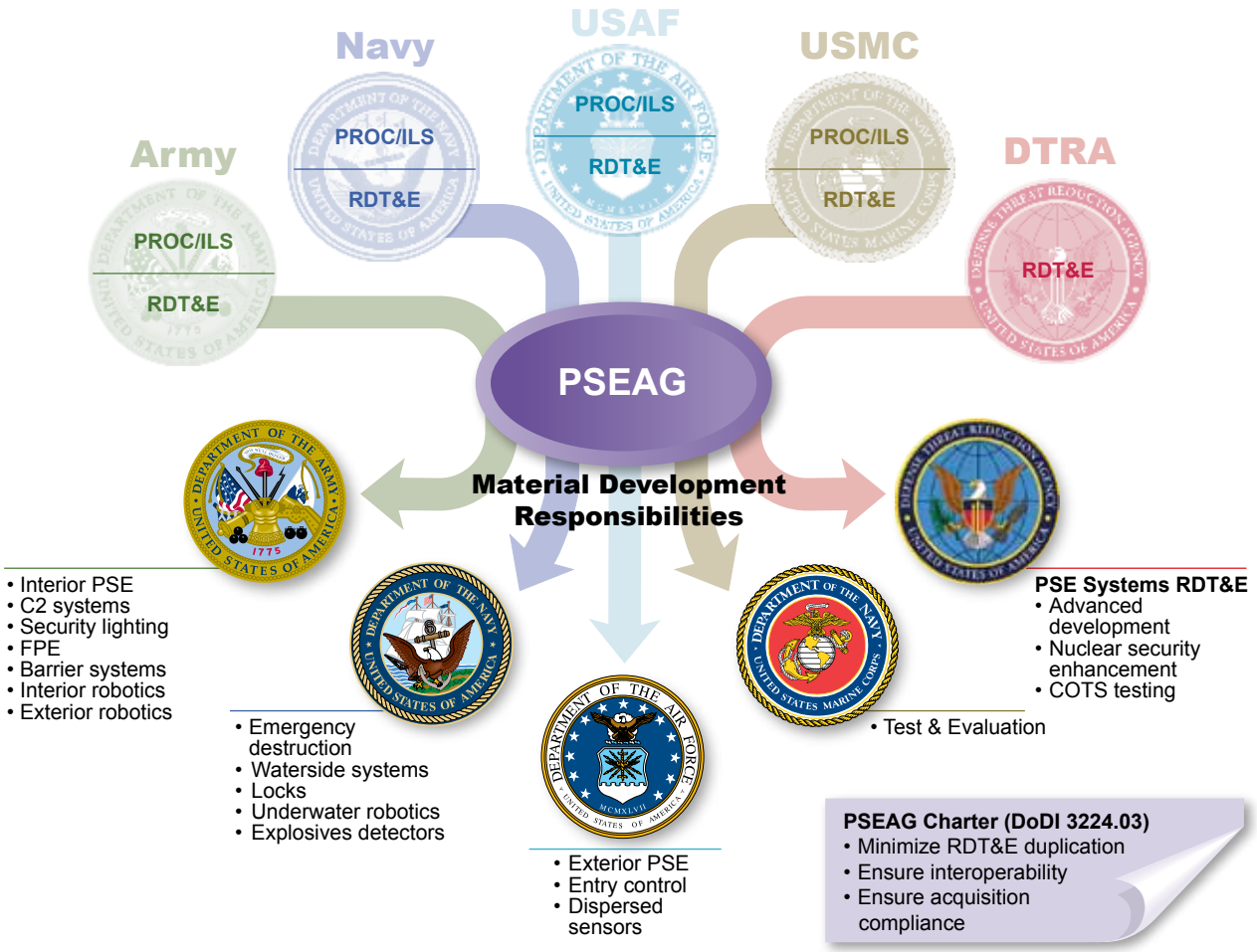
The OASD(NCB)/NM) uses the Physical Security Equipment Action Group (PSEAG) to assist with the review, selection, and implementation of conventional security-related equipment development efforts. The OASD(NCB)/NM) uses the Security Policy Verification Committee (SPVC), established by directive to oversee the physical security of nuclear weapons systems, and to assist with the review, selection, and implementation of nuclear weapon security-related efforts. The PSEAG, SPVC, and their associated working groups coordinate operational requirements and associated projects to avoid duplicative efforts and maximize the acquisition process in joint collaboration.



Appendix C. DoD Physical Security Equipment Action Group (PSEAG)

PSEAG Organization and Structure

The Physical Security Equipment Action Group (PSEAG) is comprised of primary voting members from the Services and the Defense Threat Reduction Agency (DTRA), with a complement of advisory personnel from the Joint Staff, other Deputy Assistant Secretaries of Defense, the Defense Intelligence Agency (DIA), the Department of Energy, and other Federal agencies. Oversight of the PSEAG is executed by the Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters (OASD(NCB)/NM)).



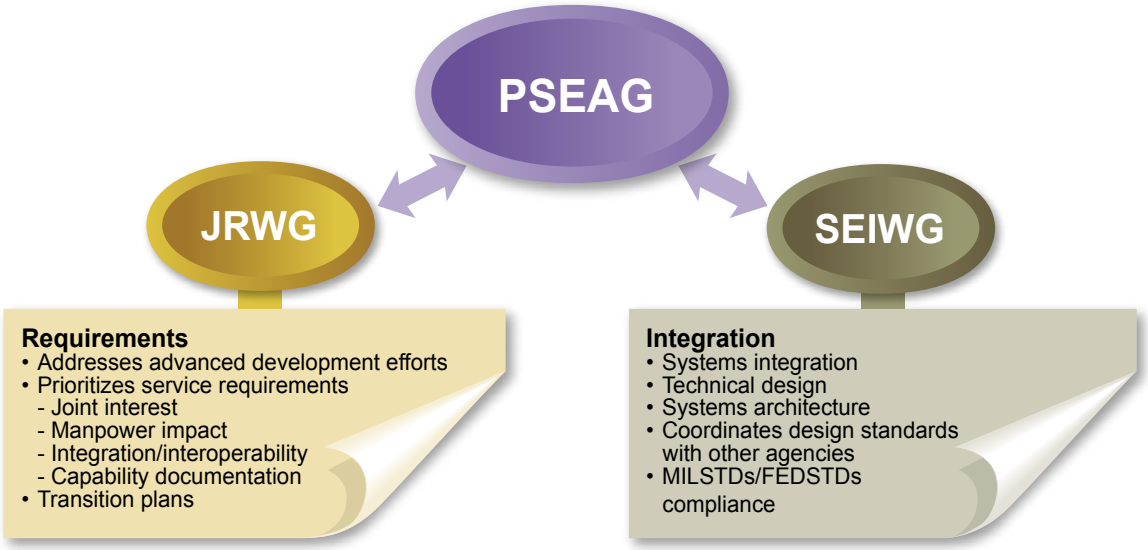
APPENDICES

Appendix C. DoD Physical Security Equipment Action Group (PSEAG) (cont.)

Working Groups

Within the PSEAG, two subgroups execute the key functions that direct the program to reach the intended objectives:

- Joint Requirements Working Group (JRWG) – reviews the Services' research, development, test and evaluation (RDT&E); Advanced Component Development and Prototypes (ACD&P); and, System Development and Demonstration (SDD) physical security equipment proposals for harmonization and to eliminate duplication of effort prior to submission to the PSEAG.
- Security Equipment Integration Working Group (SEIWG) – assists in reducing security systems costs by ensuring that new systems integrate with existing systems, and by minimizing architectural redesign.



A more detailed summary of each working group may be found in the proceeding appendices.

Appendix D. Joint Requirements Working Group (JRWG)

The Joint Requirements Working Group (JRWG) is an action officer-level working group responsible for the review and harmonization of all newly identified Department of Defense (DoD) Physical Security Equipment Action Group (PSEAG) projects. In addition, the JRWG may also perform other missions at the request of the PSEAG Chair. Led by its Chairman who serves as the focal point for the execution of the JRWG duties; facilitates review of Services physical security equipment (PSE) capability requirements to determine joint interest; and, maintains current files of Service PSE capability requirements and meeting minutes, the JRWG is comprised of the following members:

Voting	Non-Voting / Advisory
U.S. Army	Defense Threat Reduction Agency
U.S. Navy	U.S. Army Product Manager, Force Protection Systems
U.S. Air Force	U.S. Army Military Police School
U.S. Marine Corps	U.S. Air Force Electronic Systems Center, Force Protection SPO
	U.S. Marine Corps Systems Command
	U.S. Marine Corps Combat Development Command
	U.S. Navy Commander, Fleet Forces Command
	U.S. Navy Systems Command AT/FP Leadership Team
	Chair, Security Equipment Integration Working Group (SEIWG)
	Joint Staff, J-34

In addition to supporting project harmonization efforts, JRWG Voting Members submit draft capabilities documents on PSE efforts for coordination with DoD PSEAG Service components, and provide the JRWG any final copies of signed capabilities documentation.

The JRWG's requirements Harmonization mission is accomplished through the collection of project data and subsequent review and discussion with the Voting Members. Several months prior to the annual Harmonization Meeting, the JRWG issues a data call to the Services for on-going (e.g., calendar year), proposed budget year (BY), and the following BY +1 for research, development, test, and evaluation of conventional PSE projects in response to capability needs identified in the Joint Capabilities Integration and Development System or Joint Urgent Operational Needs process. The JRWG then convenes to review the project proposals and harmonize the submissions, with results briefed during the subsequent PSEAG Executive Session.

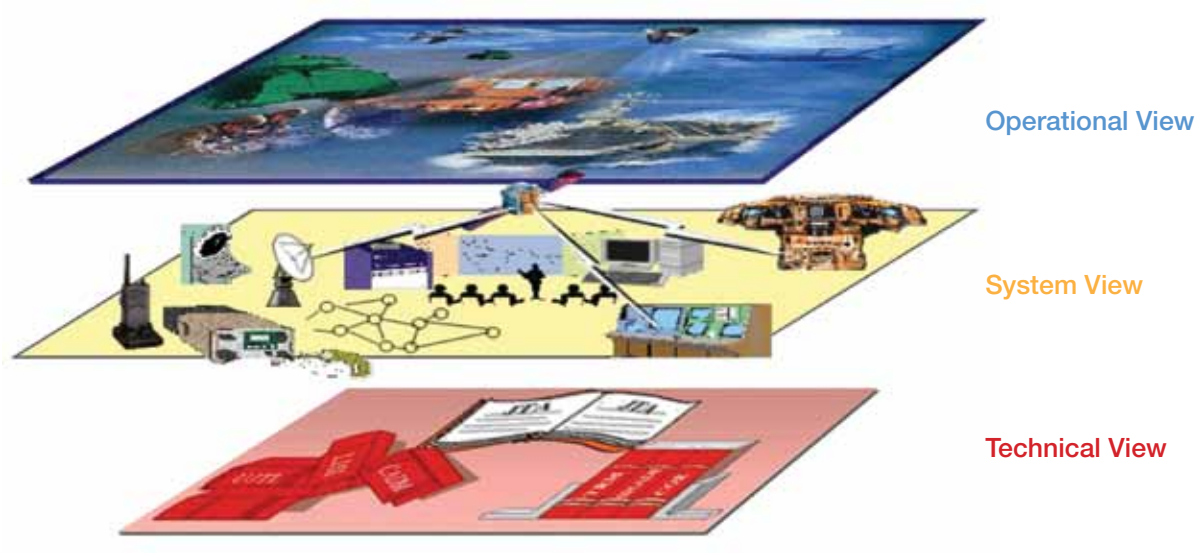
During the FY11 Harmonization process, JRWG members reviewed 32 Service submissions (five from the Army, 17 from the Navy, seven from the Air Force, and three Special Projects). Following this review, the Services then "scored" each project submission as *Fund* or *Do Not Fund*, with each representative required to provide comments and justification for any *Do Not Fund* recommendations. The results of this meeting were briefed at the June 2010 PSEAG meeting.

Following recommendations made by the "Capabilities–Requirements Workshop" during the June 2010 PSEAG meeting, the JRWG is in the process of reviewing how to: a) more effectively harmonize requirements in order to reduce technology duplication and increase the probability of project success; b) incorporate other DoD Agencies in the harmonization process; c) foster relationships with the combatant commands (COCOMs) and other agencies; and d) seek a more active role in requirements from the U.S. Marine Corps.

Appendix E. Security Equipment Integration Working Group (SEIWG)

As a standing subcommittee of the PSEAG, the Security Equipment Integration Working Group's (SEIWG) mission is to coordinate and influence system architecture, technical design, and systems integration for all physical security equipment to be used within the Department of Defense (DoD). In support of this DoD wide effort, the SEIWG has a multi-service membership that includes the US Air Force, Army, Navy, and Marine Corps.

To accomplish its far reaching mission, the SEIWG is developing a joint physical security equipment (PSE) technical architecture for application to all DoD PSE design and acquisition efforts. The architecture is known as the Joint Force Protection Reference Architecture. As shown in the figure below, the architecture consists of three "views", the Operational View (OV), the System View (SV), and the Technical View (TV). The Operational View depicts and describes the operational requirements with the elements, tasks, and activities involved in meeting those requirements, as well as information flows required to accomplish operational mission requirements. The System View describes and interrelates the existing or postulated system designs, technologies, equipment, and other resources intended to support the operational requirements. The Technical View describes the profile of rules, standards, and conventions governing systems implementation.



Joint Force Protection Reference Architecture

The Joint Force Protection Reference Architecture will ensure that all future DoD security systems, for all four military services, integrate with existing systems and with each other, and minimize the need for physical redesign. This translates to increased protection against international and domestic threats at lower costs and in less time.

To date, the SEIWG has developed an OV-1, OV-2, OV-3, OV-4, OV-5, OV-6c, SV-1, SV-4, SV-5, SV-6, and a TV-1 with multi-service utility. The SEIWG has also generated a lexicon for architectural view terminology.

The *Anti-Terrorism/Force Protection (AT/FP) Joint Technical Standards Profile Technical View* (TV-1), SEIWG 0400, is a compilation of approximately 620 standards relating to AT/FP equipment for use by all the Services in the 2010/2011 timeframe. The goal of the TV-1 is to provide a program manager with a resource for identifying current AT/FP applicable standards and assessing relevancy to force protection programs. Adherence to the standards presented in the TV-1 document will promote interoperability and commonality at every level of force protection.

Appendix E. Security Equipment Integration Working Group (SEIWG) (cont.)

The TV-1 document was initially published by the SEIWG in May 2007 and updated in May 2009. The SEIWG plans to publish the next update in May 2011. The TV-1 is available as a Microsoft Access database with a user-friendly interface with extensive search filtering capabilities.

In addition to the Joint Force Protection Architecture products, the SEIWG has developed, and is continuing to develop, Interface Control Documents (ICDs) and standards for AT/FP equipment for use during the acquisition and development of future physical security equipment. In May 2009, the SEIWG published SEIWG ICD-0101A which defines the structure and sequencing of information for communication between AT/FP systems using XML. This ICD is currently being successfully used by both industry and by all four Services. The ICD standardizes XML schemas focusing on the communication interface between the Command and Control Display Equipment (CCDE) and the Two-State Detection Sensors, Line of Detection Sensors, Wide Area Detection Sensors, Video Motion Detection Systems, Explosive Detection Systems, Mobile Surveillance/Assessment Systems, Fixed Surveillance/Assessment Systems, Access Control Systems, Delay/Denial Systems, Mass Notification Systems, Peer, Backup, or remote CCDE Nodes, and response devices including Remotely Operated Weapons. Standardizing these interfaces increases the interoperability of equipment provided by various vendors and enables a comprehensive integration maximizing benefits in safety, operational and situational awareness, alarm response and costs. In addition to standardizing the communication in the hierarchal relationship between the CCDE and sensors, the ICD also addresses CCDE-to-CCDE communication. The SEIWG is currently developing an updated version of the ICD, known as SEIWG ICD-0101B, which will provide additional XML communication standardization for Chemical, Biological, Radiological, and Nuclear sensors. The SEIWG expects to publish this update in February 2011.

The SEIWG is also developing a similar ICD that standardizes the communication between a CCDE and an Integrated Base Defense Command and Control (IBDC2) system, SEIWG ICD-0300. The SEIWG expects to approve and release this standard for use in April 2011.

In addition to the two XML-related ICDs, the SEIWG developed and maintains the Radio Frequency (RF) Data Transmission Interfaces standard known as SEIWG 005C. This standard was first developed by the SEIWG in 1981 and has undergone several revisions over the years. Currently, the SEIWG is substantially revising the standard to reflect the major advances in RF communication. The SEIWG plans to approve and release SEIWG 005D in July 2011.

With the maturation of these products over the next year, the SEIWG anticipates that the AT/FP systems for every Service will migrate toward a cohesive architecture consisting of products from many vendors seamlessly exchanging information. Adherence to the AT/FP ICDs and standards identified in the TV-1 will result in reduced acquisition and development time, minimized RDT&E, increased Service interoperability and interchangeability, and easier maintenance. In turn, these factors will result in a safer environment for the military and its assets.

For more information on the work being conducted by the SEIWG or the documents being developed by the SEIWG, please contact any of the SEIWG representatives listed below.

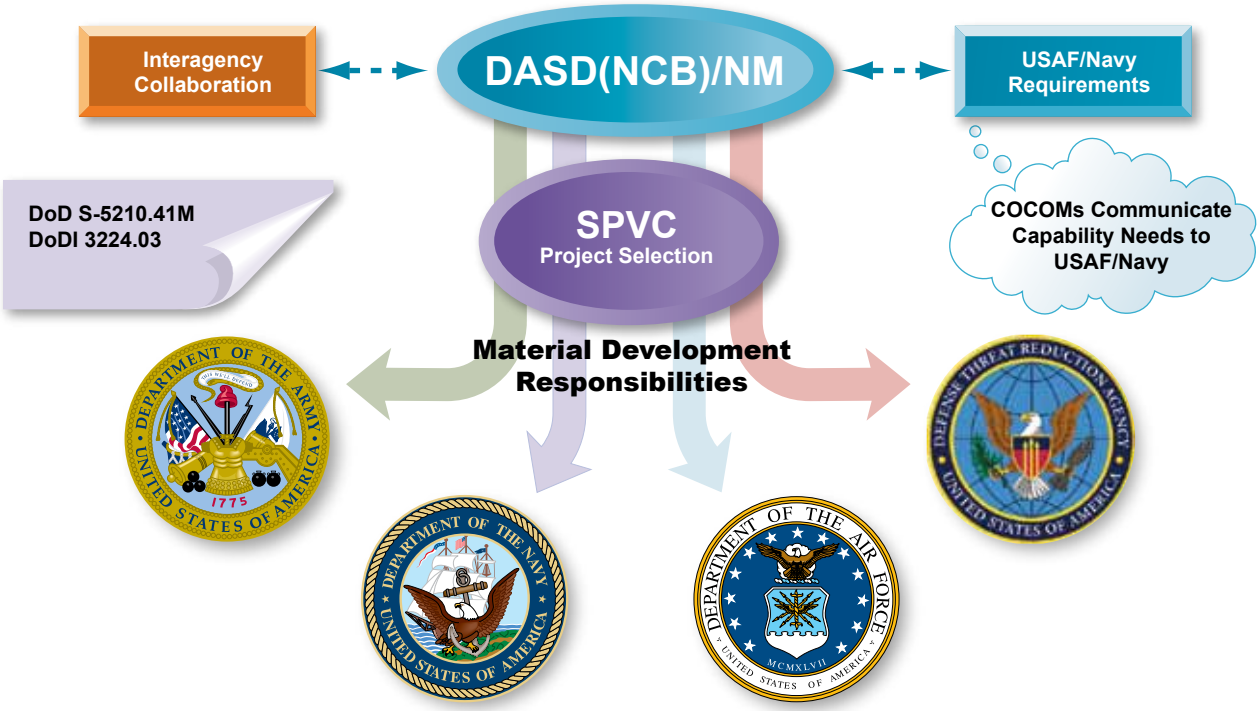
Service Representative	Organization
Mr. Brad Davis	USAF
Mr. Rodney Rourk	USMC
Mr. Richard Goehring	U.S. Army
Mr. Edward Layo	U.S. Navy

In addition, MITRE Corporation has established a SEIWG Document Repository on its MITRE Force Protection SEIWG SharePoint website, containing all SEIWG approved documents, and intended for use by Industry and the DoD. To access the repository, the SEIWG invites all interested parties to e-mail SEIWG@hanscom.af.mil to request a site application. Bi-annually the SEIWG also publishes a newsletter highlighting note-worthy SEIWG information such as new releases and current work efforts. To receive a copy of the newsletter, send an e-mail request to SEIWG@hanscom.af.mil.

Appendix F. DoD Security Policy Verification Committee (SPVC)

SPVC Organization and Structure

For the purposes of joint collaboration of nuclear weapon physical security capability, the Security Policy Verification Committee (SPVC) functions much like the Joint Requirements Working Group (JRWG) in the Physical Security Equipment Action Group (PSEAG) process. It harmonizes requirements submitted by the Air Force or the Navy for commonality and the reduction of duplication. The SPVC also prioritizes nuclear security Physical Security Equipment (PSE) research, development, test and evaluation (RDT&E) efforts base on risk reduction to the stockpile. They also consider solutions derived from interagency collaboration with the Department of Energy and the Nuclear Regulatory Commission (NRC). Material solutions are recommended to Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters (OASD(NCB)/NM)) for endorsement to the Air Force and Navy for acquisition programs.

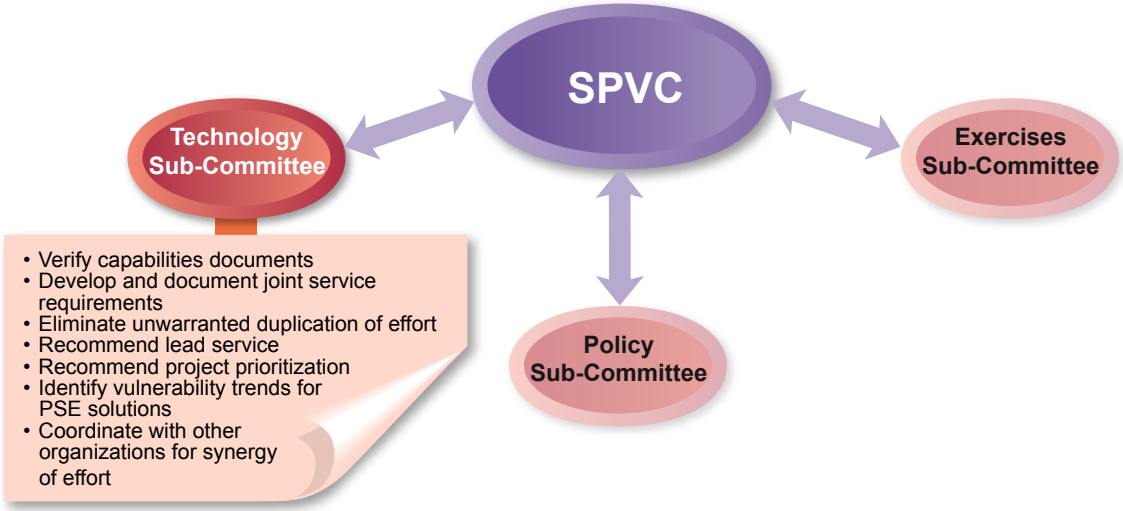


Appendix F. DoD Security Policy Verification Committee (SPVC) (cont.)

Sub-Committees

The SPVC employs three sub-committees to assist in accomplishing its objectives:

- **Policy Sub-Committee** – reviews nuclear weapon security-related policy issues. The sub-committee develops and recommends security policy modifications to the SPVC.
- **Technology Sub-Committee** – reviews nuclear weapon PSE RDT&E project proposals and recommends projects through the SPVC to the Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters (OASD(NCB)/NM)) for approval. The sub-committee reviews security exercise trends and security policy deviations reports to identify areas where technology may provide the most efficient and cost-effective solutions. The sub-committee also coordinates project information with other PSE-related agencies to identify areas for collaboration and to eliminate duplicative efforts.
- **Exercise Sub-Committee** – maintains oversight of the nuclear security force-on-force exercise program and associated engineering tasks. This sub-committee also establishes and maintains the exercise schedule and coordinates with the Services to execute and support the exercises.



Appendix I. List of Acronyms

Acronym	Definition
3D	three dimensional
AA&E	arms, ammunition, and explosives
ACD&P	Advanced Component Development and Prototypes
ACSD	Advanced Container Security Device
AFB	Air Force Base
AFI	Air Force Instruction
AFMC	Air Force Materiel Command
AFRL	Air Force Research Laboratory
AFSOC	Air Force Special Operations Command
AKO	Army Knowledge Online
ANGB	Air National Guard Base
AP	armor piercing
AoA	analysis of alternatives
AROC	Army Requirements Oversight Council
ARWG	Attack Resistance Working Group
AT/FP	anti-terrorism/force protection
ATMR	Attack Tools and Material Resistance
BAA	Broad Agency Announcement
BAIS	Battlefield Anti-Intrusion System
BDOC	Base Defense Operations Center
BY	budget year
C2	command and control
C2ISR	command, control, intelligence, surveillance and reconnaissance

Acronym	Definition
C4I	command, control, communications, computers and intelligence
CBA	capabilities- based assessment
CBRN	chemical, biological, radiological and nuclear
CBRNE	chemical, biological, radiological, nuclear and high-explosive
CCDE	Command and Control Display Equipment
CDD	Capability Development Document
CENTRIX	Combined Enterprise Regional Information Exchange
CM	consequence management
CM / HHM	Communication Module / Hand-Held Monitor
COCOM	combatant commander
CONOPS	concept of operations
CONUS	continental United States
COP	common operating picture
COPSS	Combat Outpost Security System
COTS	commercial-off-the-shelf
CPD	capability production document
CSD	Container Security Device
CSIG	Counter-IED Senior Integration Group
CTF	Combined Test Force
DAD	detect, assess, defend
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency

Appendix I. List of Acronyms (cont.)

Acronym	Definition
DIAC	Defense Installation Access Control
DKO	Defense Knowledge Online
DMS	diminishing manufacturing sources
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDI	Department of Defense Instruction
DOE	Department of Energy
DSS	Defense Security Service
DT&E	development test and evaluation
DTEDE	desktop explosive detection device
DTR	Defense Transportation Regulation
DTRA	Defense Threat Reduction Agency
EDE	explosive detection equipment
EM	electromagnetic
ESC	Electronics Systems Center (U.S. Air Force)
FDS	Frequency Domain Spectrometry
FEDSTD	Federal standard
FP	force protection
FPE	force protection equipment
FPED	Force Protection Equipment Demonstration
FPS2	Force Protection Security Systems
FSD-ZBV	Forwardscatter Z-Backscatter Van
FUE	first unit equipped
FY	fiscal year

Acronym	Definition
GaRDS	Gamma Ray Detection System
GCTS	Ground Combat Training Squadron
GSA	Government Services Administration
HERO	hazards of electromagnetic radiation to ordnance
HHEDE	handheld explosive detection equipment
HQ AF	Headquarters, Air Force
HQDA	Headquarters ,Department of the Army
IBDC2	Integrated Base Defense Command and Control
IBDSS	Integrated Base Defense Security Systems
ICD	Initial Capabilities Document / Interface Control Document
IDC2COP	Integrated Defense Command and Control Common Operating Picture
I&E	Assistant Secretary of the Navy (Energy, Installations and Environment)
IED	improvised explosive device
IEDD	improvised explosive device defeat
IFF	Identify Friend or Foe
IGSSR-C	Integrated Ground Security Surveillance Response – Capability
I-IBD	Interim-Integrated Base Defense
ILD	Internal Locking Device
ILS	integrated logistics support
IPL	Integrated Priority List

Appendix I. List of Acronyms (cont.)

Acronym	Definition
ISD	Integrated Swimmer Defense
IUIBP	Integrated Unit, Base Installation Protection
JCATS	Joint Conflict and Tactical Simulation Enhancements
JCD	Joint Capabilities Document
JCIDS	Joint Capabilities Integration and Development System
JCTD	Joint Capabilities Technology Demonstration
JEHD	Joint Explosive Hazard Defeat
JFPASS	Joint Force Protection Advanced Security System
JFPRA	Joint Force Protection Reference Architecture
JPL	Jet Propulsion Laboratory
JPEO-CBD	Joint Program Executive Office for Chemical and Biological Defense
JPMG	Joint Program Manager Guardian
JRWG	Joint Requirements Working Group
JSEOD	Joint Service Explosive Ordnance Disposal
JUONS	Joint Urgent Operational Needs Statement
KRD	Kachemak Research Development
LAN	local access network
LED	light-emitting diode
LKMD	Lighting Kit, Motion Detector
LLNL	Lawrence Livermore National Laboratory

Acronym	Definition
LRIP	low-rate initial production
MAJCOM	Major Command (U.S. Air Force)
MDD	Milestone Decision Document
MESF	Maritime Expeditionary Security Force
MILSTD	military standard
MS	milestone
MSCoE	Maneuver Support Center of Excellence
MVEDEX	mobile vehicle explosive detection equipment
MWD	military working dog
NATO	North Atlantic Treaty Organization
NAVEODTECHDIV	Naval Explosive Ordnance Disposal Technical Division
NAVFAC	Naval Facilities Engineering Command
NAVFAC ESC	Naval Facilities Engineering Service Center
NAVSEA	Naval Sea Systems Command
NEODTD	Navy Explosive Ordnance Disposal Technology Division
NFESC	Naval Facilities Engineering Service Center
NPSEAG	Navy Physical Security Equipment Action Group
NRC	Nuclear Regulatory Commission
NRM	Naval Region Marianas
NSWC	Naval Surface Warfare Center

Appendix I. List of Acronyms (cont.)

Acronym	Definition
OASD(C3I)	Office of the Assistant Secretary of Defense for Command, Control, Computers, and Intelligence
OASD(NCB)/NM	Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters
OCONUS	outside the continental United States
OD	operational demonstration
ONS	Operational Needs Statement
OPNAV	Chief of Naval Operations
OPNAVINST	Chief of Naval Operations Instruction
OSD	Office of the Secretary of Defense
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
OV	Operational View
PACAF	Pacific Air Forces
PBIED	person-borne improvised explosive device
PM-FPS	Product Manager, Force Protection Systems
PMMW	passive millimeter wave
POG	Project Officer Group
PS	physical security
PSE	physical security equipment
PSEAG	Physical Security Equipment Action Group
QRF	Quick Reaction Force
QT&E	qualification test and evaluation

Acronym	Definition
REF	Rapid Equipping Force
RDT&E	research, development, test and evaluation
RF	radio frequency
RFI	request for information
RPI	Rensselear Polytechnical Institute
R/SEDS	Remote / Standoff Explosive Detection System
SaaS	Soldier as a System
SAIC	Science Applications International Corporation
SDD	System Development and Demonstration
SEIWG	Security Equipment Integration Working Group
SME	subject matter expert
SPAWAR	Space and Naval Warfare Systems Command
SPAWARSYSCEN	Space and Naval Warfare Systems Center
SPVC	Security Policy Verification Committee
STANAG	standardization agreement
STUAS	Small Tactical UAS
SV	System View
TASS	Tactical Automated Security System
TD	technical demonstration
TDS	Time Domain Spectrometry
TEMP	Test and Evaluation Master Plan

Appendix I. List of Acronyms (cont.)

Acronym	Definition
THz	terahertz
T-MMV	Trailer-Mounted Military Mobile VACIS
TRL	Technology Readiness Level
TSA	Transportation Security Administration
TSS	Tactical Surveillance System
TSWG	Technical Support Working Group
TV	Technical View
UAS	unmanned aerial system
UFC	United Facilities Criteria
UOES2	User Operational Evaluation System
UONS	Urgent Operational Needs Statement
USA	United States Army
USAF	United States Air Force
USCENTCOM	U.S. Central Command
USEUCOM	U.S. European Command
USMC	United States Marine Corps
USN	United States Navy
USTRANSCOM	U.S. Transportation Command
UWB	ultra wide band
VBIED	vehicle-borne improvised explosive device
VEDEX	vehicle explosive detection equipment x-ray
VMS	Video Management System
WAN	wide area network

Acronym	Definition
WMD	weapons of mass destruction
WSSS	Waterside and Shipboard Security
WSTI / LRTI	Wide Area Surveillance Thermal Imager / Long Range Thermal Imaging
ZBV MilT	ZBV Militarized Trailer

Department of Defense Physical Security Equipment RDT&E Program Summary 2010