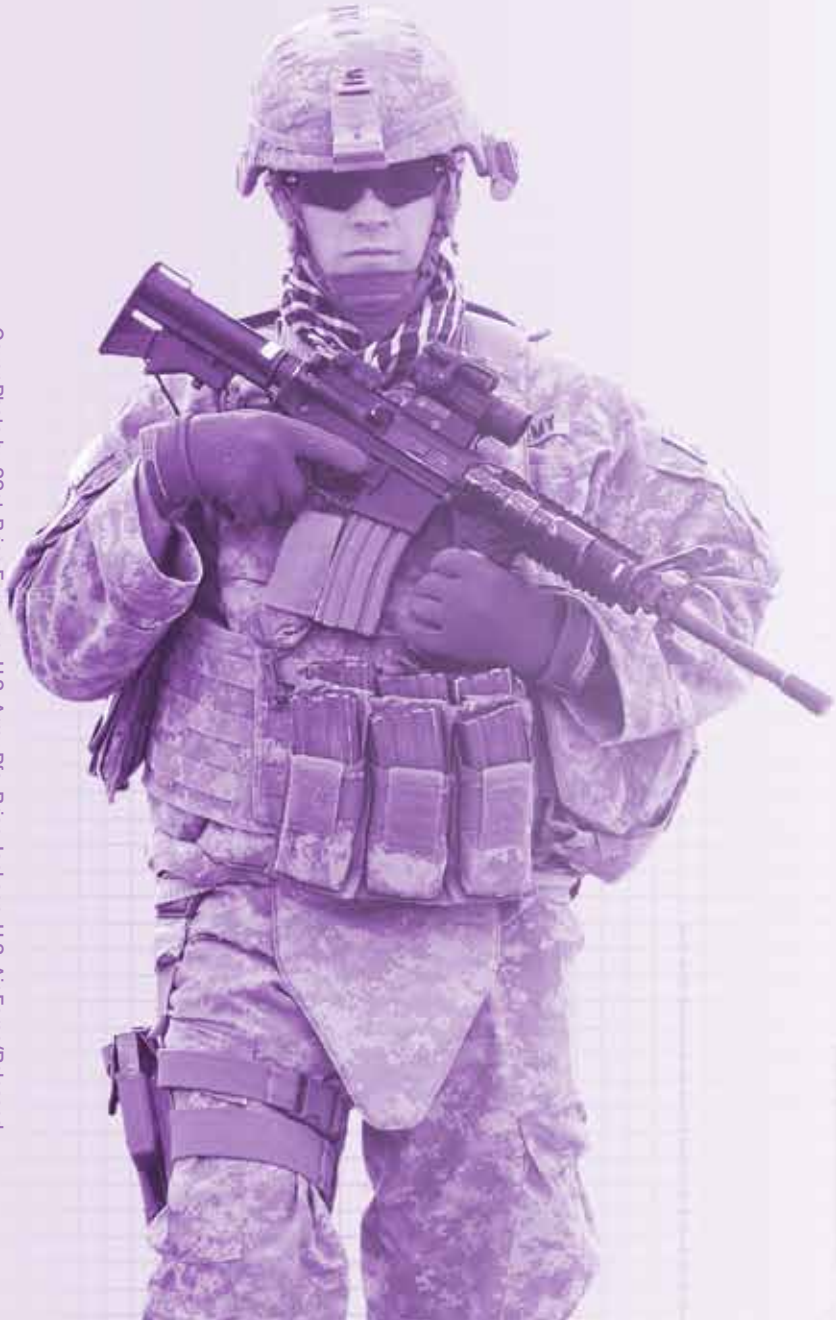
DEPARTMENT OF DEFENSE
PHYSICAL SECURITY EQUIPMENT

RDT&E

2011 PROGRAM SUMMARY



Cover Photo by SSgt. Brian Ferguson; U.S. Army Pfc. Brian Jackson, U.S. Air Force/Released

ACCESS CONTROL

ANALYTICAL SUPPORT

DECISION SUPPORT

DETECTION & ASSESSMENT

INSTALLATION & TRANSPORT SECURITY

PREVENTION

STORAGE & SAFEGUARDS

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

For calendar year 2011, the Physical Security Equipment (PSE) Research, Development, Test and Evaluation (RDT&E) Program continued to address evolving threats facing Department of Defense (DoD) personnel, their families, and critical infrastructure. 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 requirements while eliminating duplication of projects, ensuring systems integration, and promoting interoperability and sustainability.

The PSE RDT&E equipment and studies summarized in this document represent the culmination of identified 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 Calendar Year 2011, 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.

In August 2011, the Defense Installation Access Control project successfully demonstrated the capability to send information to the Physical Access Control System, when authoritative data determined an individual's fitness to an installation changed.

Also in 2011, the Joint Interface Group for Security Application Workspaces project team conducted an audit and analyzed existing DoD Command & Control software systems and then developed a system design that reduces the time and cost associated with Command & Control sensor data integration.

The Enhance Ion Mobility Spectrometry (IMS) Explosive Detection Systems project is trying to resolve long-standing issues with IMS technology to make it a more effective tool. Several materials are able to confuse the systems resulting in false alarms and there are problems associated with the collection of the target sample. The goal of this effort was to investigate ways to improve the performance of currently fielded IMS systems through software upgrades, hardware modification, and a new collection device. The project team analyzed potential confusants and evaluated current swipe technologies to identify ways to improve this important capability for the war fighter.

As part of on-going efforts to identify commercial physical security and force protection equipment currently available to combat terrorism world-wide, the Office of the Assistant Secretary

of Defense for Nuclear, Chemical, and Biological Defense Programs sponsored the Force Protection Equipment Demonstration VIII at the Stafford County Regional Airport in May 2011. 553 U.S. and 38 international vendors demonstrated more than 3,200 products to over 20,000 participants from across DoD, Federal, State, and local agencies and organizations involved in physical security and force protection missions. VIPs who attended the event included the Virginia Speaker of the House, General Officers, and Senior Executive Service officials from the U.S. and international allies. Even under the most adverse weather conditions in recent memory, the event provided exhibitors the opportunity to showcase their products in a challenging field environment.

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)) and the Military Services and the Defense Threat Reduction Agency (DTRA). 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.

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 war fighter. I hope you find this 2011 Summary beneficial in meeting your physical security needs.

Thomas Whittle, PE
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

Introduction to PSEAG Capability Areas . . . 3

Attack Tool & Material Resistance . . . 7

Automated Image Recognition Software . . . 8

AutoScan Under-Vehicle Inspection System . . . 9

Biometric Verification System (Sub-Component of the "Smart Magazine" Project . . . 10

Commercial-Off-the-Shelf Equipment Qualification . . . 11

Comparative Evaluation of Personnel Screening Systems . . . 12

Comparative Studies and Evaluations of COTS Explosive Detection Equipment . . . 13

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

Defense Installation Access Control Working Group Identity Management Enterprise Services Architecture . . . 17

Enhance Ion Mobility Spectrometry Explosive Detection Systems . . . 18

Force Protection Equipment Demonstration . . . 19

Hailing Acoustic Laser & Light Tactical System . . . 20

Integrated Defense Command and Control Common Operating Picture . . . 21

Integrated Ground Security Surveillance Response – Capability . . . 22

Interim Integrated Base Defense . . . 23

Intermodal Security Devices . . . 24

Joint Interface Group for Security Application Workspaces . . . 25

Lighting Kit, Motion Detector . . . 26

National Air Space Integration Demonstrator for Small Tactical UAS Alarm Response . . . 27

Navy Integrated Waterside Security Feasibility Study . . . 28

Performance Maintainability Kit for Explosive Detection Equipment . . . 29

Seismic-Acoustic Detection and Ranging System . . . 30

Sensor Fusion . . . 31

Shipboard Security Systems . . . 32

Shore-Line Monitoring System . . . 33

Table of Contents (cont.)

Single Crystal-Based, Acoustic Non-Lethal to Lethal, Scalable Engagement System for Expeditionary Swimmer Defense Applications 34

Smart Magazine. 35

Tactical Video Surveillance System 36

Appendix A. Information Repository for PSEAG Funded Programs 39

Appendix B. The DoD PSE RDT&E Program Organization and Structure 40

Appendix C. DoD Physical Security Equipment Action Group. 41

Appendix D. Security Equipment Integration Working Group 42

Appendix E. Joint Requirements Working Group. 43

Appendix F. DoD Security Policy Verification Committee 44

Appendix G. Points Of Contact 46

Appendix H. List of Acronyms. 47

INTRODUCTION

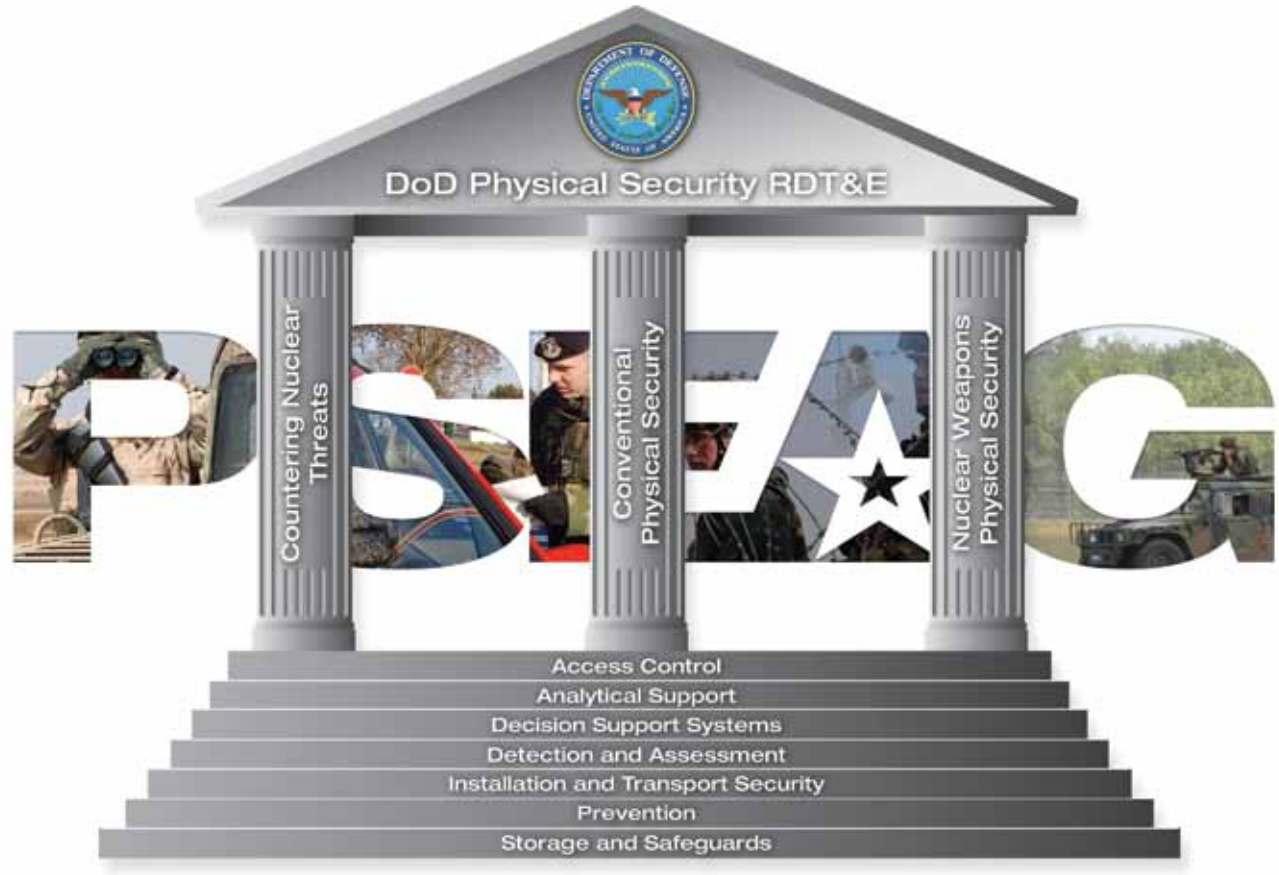
Department of Defense Physical Security Equipment (PSE) Research, Development, Test and Evaluation (RDT&E) Program Overview

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.

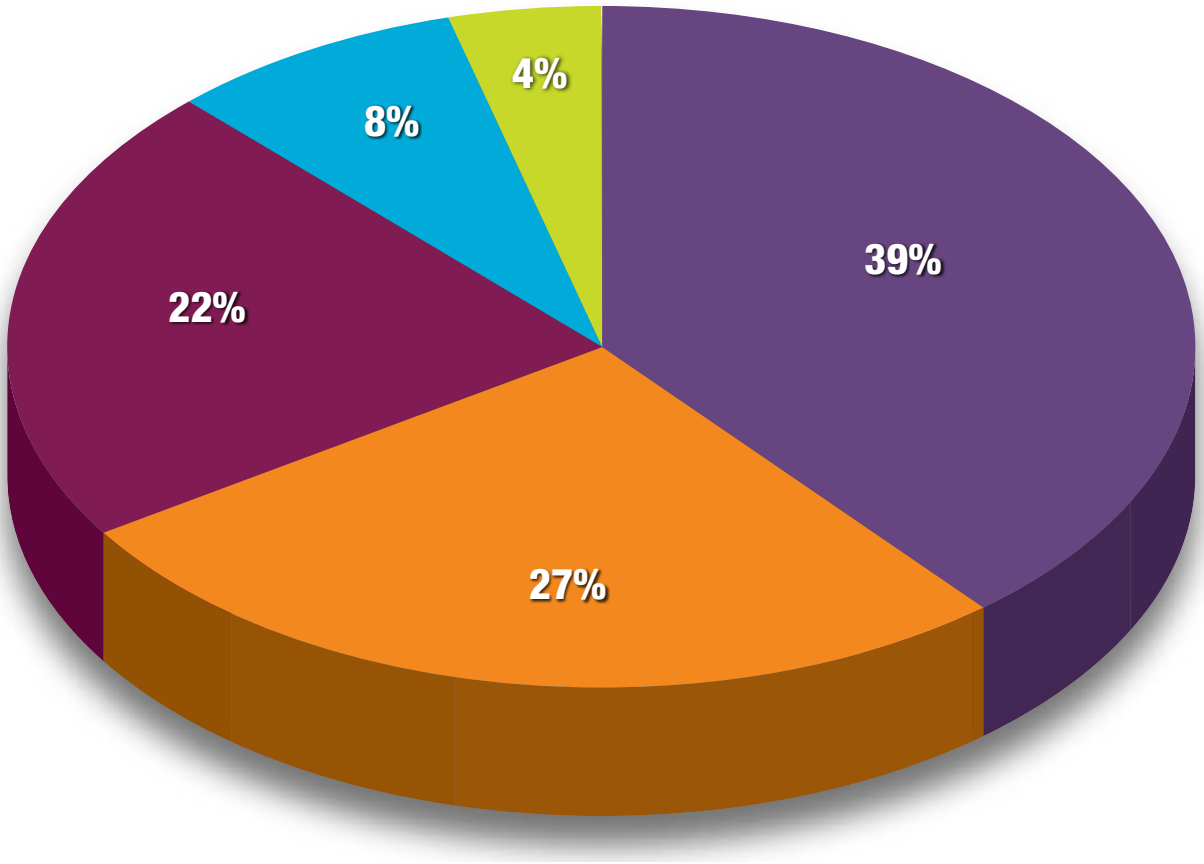
Underpinning this entire structure is a foundation of physical security equipment activities which are now organized into major initiatives, centered on key physical security requirements. These major initiatives bring together formerly disparate physical security equipment projects into more cohesive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

- **Access Control**
- **Analytical Support**
- **Decision Support Systems**
- **Detection and Assessment**
- **Installation and Transport Security**
- **Prevention**
- **Storage and Safeguards**



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.



Introduction to PSEAG Capability Areas

The Physical Security Equipment Action Group focuses funding to seven capability areas within the Physical Security realm. These capability areas contain: programs, processes, and equipment which enhance and strengthen capabilities for positive control and access into areas and resources; programs and processes focusing on strengthening capabilities for critical path analysis, 'what if scenarios', and cost-benefit analysis to aid in risk management decisions and investment strategies; programs and processes assessing and integrating gap analysis, identifying requirements, and prioritizing recommendations for strengthening and enhancing overall PSE and CWMD capabilities; programs and equipment enhancing extended detection and rapid assessment capabilities; programs, processes, and equipment enhancing and strengthening the layered, defense-in-depth security for fixed facility and mobile transportation security capabilities; capability focusing on preventing and reducing WMD and physical security threats, through information sharing, specific prevention technology development, and test and evaluation; and programs, processes, and equipment focused on enhancing and strengthening capabilities of asset protection involving close-in, inner zone security, and storage facilities/areas.

ACCESS CONTROL

- Large scale integrated and interoperable access control systems
- Continuous vetting of personnel at DoD facilities against relevant personnel databases
- Insider threat analysis
- Behavioral analysis and the use of training and systems to enhance personnel security

ANALYTICAL SUPPORT

- Execute an educational outreach program to coordinate program activities with interested communities (i.e. universities, research organizations, non DoD organizations, others)
- Develop the management and support capabilities to execute the RDT&E program for the DoD

DECISION SUPPORT

- Develop and publish security system and equipment interface and performance documents
- Develop software tools to support the evaluation of system performance requirements against stated threats
- Evaluate systems and equipment against stated capabilities and publish performance results

DETECTION & ASSESSMENT

- Land based wide area interior & exterior intrusion detection and assessment systems
- Contraband detection equipment (i.e. explosives, special nuclear material, weapons, and other relevant threats)
- Waterside and waterborne intrusion detection and assessment systems (i.e. sonar, radar, and imaging)

INSTALLATION & TRANSPORT SECURITY

- Integrated force protection and base defense systems (i.e. fully integrated capabilities against a broad spectrum of threats
- Base wide and regional common operating pictures
- Integrated waterside security systems to include land and waterside threat mitigation

PREVENTION

- Security awareness and training through the Force Protection Equipment Demonstration
- System capability analysis through a comprehensive test and evaluation
- Security gap analysis through the execution of table top exercises

STORAGE & SAFEGUARDS

- Material tracking and monitoring systems and equipment
- Advanced storage containers
- Safeguards effectiveness evaluations

ACTIVITIES

Attack Tool & Material Resistance (ATMR)

ATMR establishes the vulnerability of in-service physical security equipment to current forced entry, covert, and surreptitious threats. The objective of this effort includes:

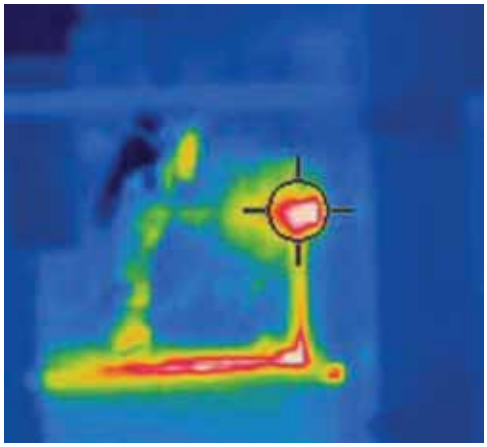
- Review and analysis of new, advanced attack tools and tool groups that have been prioritized for testing and certification of DoD physical security equipment.
- Test and evaluation of emerging attack tools and techniques, and the effectiveness of select materials and composites to mitigate attacks.
- Coordination of the Attack Resistance Working Group (ARWG) to review tools, techniques and materials for analyses, and to facilitate updates to applicable DoD and DoE documents.

Requirements:

- DoE Barrier Technology Handbook
- MIL-HDBK-1013/1A, Military Handbook, Design Guidelines for the Physical Security of Facilities, 15 December 1993.
- DoD 5100.76M Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
- OPNAVINST 5530.13C, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
- OPNAVINST 5530.14B, Physical Security Manual

Accomplishments:

- Controlled Impact Rescue Tool (CIRT)
- Hydro Demolition System
- Dual Saw
- Petrogen Cutting System
- MicroBlaster
- Plasma Cutting Tool
- Thermally resistant materials and material combinations

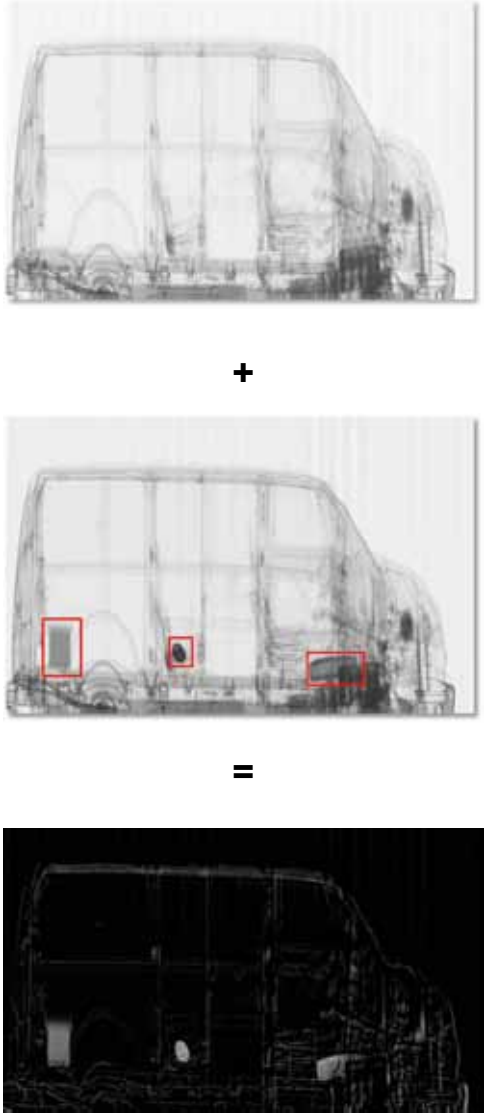


Key Dates / Milestones:

- FY10 ATMR project established and initial testing begins
- FY11 Historic test data submitted to Sandia National Laboratory for inclusion in Barrier Handbook
- FY11 Attack Resistance Working Group established; FY12 efforts defined
- FY12 Execution of several test sequences to include linear shape charges, advanced composite materials
- FY13-14 Ongoing Test and Evaluation

Automated Image Recognition Software

X-ray screening of vehicles is widely utilized at Government facilities to search for illicit cargo such as drugs, weapons, and explosives. The x-ray images produced can be complicated and time consuming to interpret. The objective of this effort is to develop an image recognition algorithm compatible with currently fielded systems to assist security personnel with the detection of potential threats or concealed illicit cargo.



Requirements:

- JUONS CC-0315, March 08
- IUBIP ICD, July 07
- IEDD ICD, February 06
- IBDSS CDD, February 05

Accomplishments:

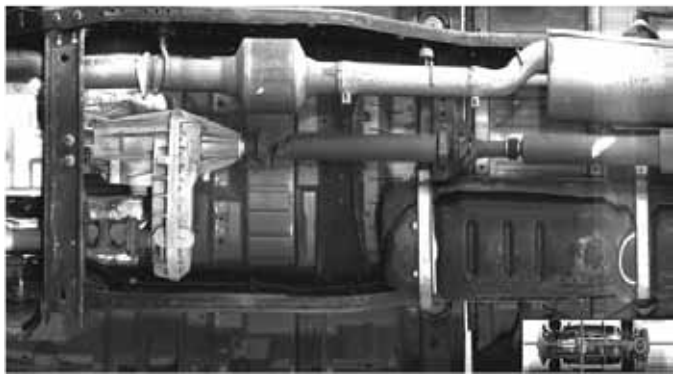
- Explored the feasibility of comparing vehicles under inspection to “clean” vehicle images to subtract out clutter and highlight anomalies utilizing Photoshop CS5 Extended

Key Dates / Milestones:

- Start Date August 2011
- End Date November 2012
- Complete assessment of feasibility with Photoshop CS5 December 2011
- Release BAA January 2012
- Select the Vendor for Initial Development April 2012
- Test systems from the software developer October 2012

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. Under development since 2007, AutoScan is currently being evaluated by Air Force Security Forces at MacDill Air Force Base (AFB), FL, Hill AFB, UT, and Gabreski Air National Guard Base, NY.



Requirements:

- DoD 5210.41M, Volume 3, Enclosure 3, paragraph 3d(4)(a)
- AFI 31-101, paragraph 2.4.3 through 2.4.3.1.3
- UFC 4-022-01, paragraph 7-3.2

Accomplishments:

- Reduced footprint of speed sensor. The smaller area greatly reduced the risk of vehicle damage.
- Completed development of 3G system architecture, reducing footprint, simplifying installation, and strengthening protection for system components.
- Integrated air knife allowing the system to be strong enough to withstand vehicular traffic and more economical to produce.
- Developed light-emitting diode (LED) replacement for halogen light scheme, lowering unit operating temperatures and extending life cycle.
- Completed expansion hub. Allows Integrated area scan camera, Stop light control and RFID reader.
- Increased image transfer speeds through the implementation of GigE Ethernet enhancements.

Key Dates / Milestones:

- Start date: February 2007
- End date: September 2012
- Anticipated major project milestones:
  - o Complete GigE versus Wireless trade-off study
  - o Analyze data obtained thus far
  - o Write software report
  - o Finalize 3G design
  - o Write and submit final report

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 has field demonstrated the technology through operational test and evaluation at an operational base. 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.

ILD Door Applications

Biometric System with ILD Lock

Biometric Verification System

Requirements

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

Accomplishments

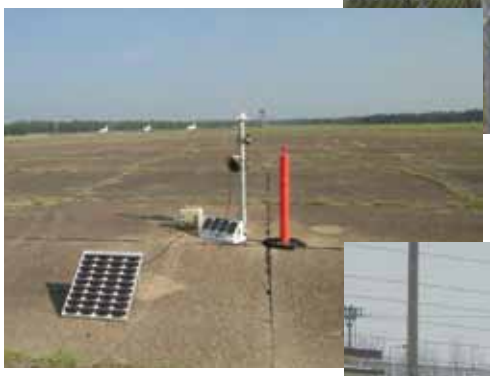
- Made changes to ILD biometric unit to better facilitate future production manufacturing
- Performed operating software update to ILD biometric Handheld unit
- Completed final test and evaluation of ILD biometric prototype and submitted results to contractor
- Installed ILD biometric system at an operational base to field demonstrate the technology through operational test and evaluation

Key Dates / Milestones

- Project Start Date – October 2007
- ILD Biometric Handheld unit software update – August 2011
- Operational Test System installation – September 2011
- Operational Test and Evaluation – September 2011 - March 2012
- Project Transition Date – December 2012

Commercial Off the Shelf Equipment Qualification (COTS Qual)

The 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, Assessment/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.



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:

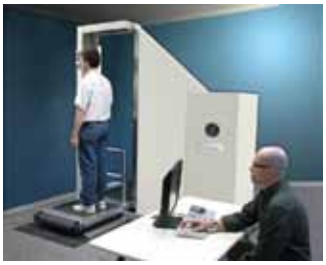
- Identified, tested, and evaluated three fence sensors; two successfully passed and were recommended for inclusion on the Force Protection Security Systems (FPS2) Approved Equipment List
- Identified, tested and evaluated an upgrade for the Vindicator Command and Control Display Equipment (CCDE); successfully added to the AFSFC Approved Equipment List.
- Evaluated seven Video Motion Detection (VMD) RFI submissions; selected three products from three vendors for formal testing
- Evaluated Flexible Solar Panels for TASS at Cold Weather Test Site
- Installed and monitored updated taut barbed wire fence sensor to confirm proper operation at low temperatures at cold weather test site; validated that vendor changes to electronic components were suitable for deployment in northern plains

Key Dates / Milestones:

- Project Start Date: 2008
- Complete testing of VMS and VMD
- Issue WAD RFI; determine qualified vendors; and complete test

Comparative Evaluation of Personnel Screening Systems

These personnel screening systems utilize ionizing radiation to quickly screen individuals at a point of entry for concealed threats on (Backscatter X-ray) and/or emplaced (Transmission X-ray) in the body. Results from this effort will allow for comparison among the various commercially available systems as well as provide effectiveness data for comparison to personnel screening systems utilizing millimeter wave imaging technology.



Requirements:

- Integrated Unit, Base Installation Protection ICD
- Improvised Explosive Device Defeat ICD
- Integrated Base Defense Security System CDD
- USCENTCOM FY10-15 Integrated Priority List (IPL)

Accomplishments:

- Released Source's Sought Notice (SSN) and received vendor solicitations
- Reviewed solicitation and selected vendors to participate in the test
- Initiated approval processes for testing of systems that utilize ionizing radiation

Key Dates / Milestones:

- Start Date: June 2011
- End Date: November 2012
- Start Test Event: May 2012
- Release Test Report: November 2012

Comparative Studies & 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

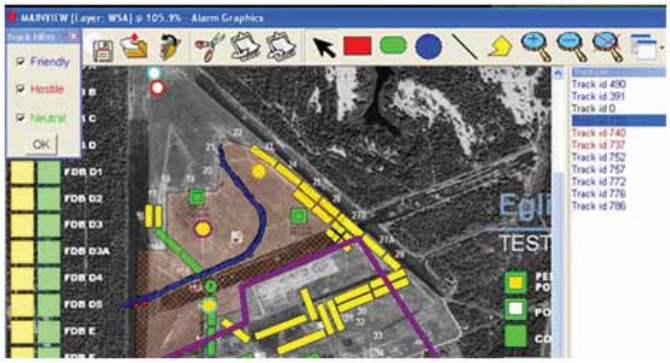
2011	
Comparative Evaluation of Commercial Off-The-Shelf (COTS) Colorimetric EDE for Trace Explosive Detection	January
Characterization of Molecularly Imprinted Polymers (MIPs) for Trace Explosive Detection	March
Comparison of Portable Raman Systems for Bulk Explosive Identification	March
Comparison of Commercial Off-The-Shelf (COTS) Infrared EDE for Bulk Explosive Detection	June
Evaluation of the ICx Technologies' (FLIR) Fido XT v4.03 Handheld Explosive Detector for Trace Explosive Detection and Use by the DR SKO Program	June
Energy Research Company's L-Cubed Prototype and Department of Homeland Security (DHS) Laser Induced Acoustics Sensor	July
Characterization of Automated Colorimetric EDE for Trace Explosive Detection	August

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
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

2008 (cont.)	
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 Gamma Ray Detection System (GaRDS) 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 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 COTS Desktop Explosive Detection Equipment (DTEDE) for Trace Explosive Detection	September
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

Correlation of Physical Security Radars to Identify Friend or Foe (IFF)

The IFF is designed to track authorized personnel and integrate this information for transfer and display on an established Command Control and Display Equipment (CCDE) 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, by tracking targets detected with overlapping 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 targets and conduct assessment of the activity or direct responding patrols, as required. In Fiscal Year 2011 (FY11) the correlation capability was fully integrated with the established Air Force Security Forces command and control display equipment in preparation of a Combined Task Force Evaluation in FY12.



Requirements:

- Integrated Base Defense Security Systems Capability Development Document (CDD), 17 February 2005

Accomplishments:

- Issued Development Test and Evaluation Report (09-342)
- Shift from detections to target tracking reduces number of displayed tracks and Operator Assessments
- Full integration with established CCDE using SEIWG ICD protocols
- Specified, purchased and installed the CCDE suite with correlation of radars
- Included integrated call-up and control of thermal imagers for assessing targets detected by radar
- Adopted Watch Items from Development Test in correlation software and CCDE display
- CCDE extended to support affiliation-based displays of tracked targets
- GPS-enabled Tags enhance the initial cross registration and maintenance of multiple overlapping radars

Key Dates / Milestones:

- 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: January – February 2012
- Project End Date and Service Transition: FY12

Defense Installation Access Control (DIAC) Working Group - Identity Management Enterprise Services Architecture (IMESA)

The overarching goal of the DIAC JCTD is the development of an IMESA. The architecture's primary purpose will be to vet the identities of everyone authorized to access a DoD installation against DoD, Federal, State and local authoritative data sources. The vetting of identities will start with biographic information and may eventually evolve to include biometric data outside of the JCTD structure. The architecture will enable Physical Access Control Systems (PACS) to rapidly, electronically and securely authenticate approved physical access credentials, provide continuous information management against authoritative databases, and support access enrollment, authorization processes and secure information sharing throughout the DoD and authorized Federal Agencies. This process enables Installations/Organizations to authenticate credentials and an individual's authorization and fitness to enter. The IMESA will greatly improve data sharing between the Services and other Federal Agencies and will prevent "bad actors" from entering our installations, vastly enhancing security of DoD personnel and resources worldwide.

Requirements:

- Section 1069 of the 2008 National Defense Authorization Act, now Public Law 110-181
- Directive Type Memorandum 09-012, Interim Policy Guidance for DoD Physical Access Control, dated 30 September 2010
- Finding 3.9 from the Fort Hood Report

Accomplishments:

- In March 2011, the DIAC WG Lead Agent briefed the Criminal Justice Information Center's (CJIS) Advisory Policy Board to request NCIC data for use in the IMESA. The board concluded the sharing of NCIC data with DMDC (non-law enforcement organization) was within CJIS policy guidance.
- In August 2011, a test using four designated Service test sites, integrated with IMESA components, successfully demonstrated the capability to send information to the PACS, when authoritative data determined an individual's fitness to an installation changed. The capability was paired with an interoperability layer service that ensured the data (change) was received at each location demonstrating a shared capability.
- In August 2011, a letter was signed out by the Deputy Under Secretary of Defense, Intelligence and Security to the Secretaries of Military Departments and Key DoD Agencies proposing that DMDC become the OPR for the IMESA which includes operations/sustainment. All recipients concurred.
- In December 2011 the DIAC Lead Agent briefed OSD JCTD Candidate Board on the IMESA concept which was well received. The Board approved the candidate package as an official JCTD during the Decision Board in February 2012.

Key Dates / Milestones:

- JCTD Start date: July 2012
- JCTD End date: July 2014

Technical Demonstrations

- Nov 12: Interoperability Layer Service, Local Pop Data Base, Continuous Information Management Engine and National Crime Information Center data base
- Jun 13: Terrorist Screening Data Base plus Share Service CJIS Info
- Feb 14: Integrate Revocation of Non-DoD Credentials and Initial Web Based NCIC Vetting

Operational Demonstrations

- Mar 13: Interoperability Layer Service, Local Pop Data Base, Continuous Information Management Engine and National Crime Information Center data base
- Dec 13: Terrorist Screening Data Base plus Share Service CJIS Info
- Jun 14: Integrate Revocation of Non-DoD Credentials and Initial Web Based NCIC Vetting

ACTIVITIES

Enhance Ion Mobility Spectrometry Explosive Detection Systems

Currently IMS is utilized in the leading trace explosive detection equipment on the market. IMS systems are sensitive with low limits of detection in the nanogram range and selective for specific explosive compounds. While IMS systems are effective, several materials are able to confuse the systems resulting in false alarms. Other difficulties with using IMS systems include problems associated with the collection of the target sample, and regulations with the radioactive source used to ionize samples for analysis. The goal of this effort is to investigate ways to improve the performance of currently fielded IMS systems through software upgrades, hardware modification, and a new collection device. This project consisting of three simultaneous efforts. The first effort will investigate the signals generated by target and confusant materials in an IMS. Comparisons will be drawn between the signals generated by a handheld system and more advanced laboratory systems. The goal of the effort is to reduce false alarms in handheld IMS performance by modifying the expected signal windows the IMS is monitoring and improving data analysis protocols. The second effort will be to reduce regulations associated with Ion Mobility Spectrometers by replacing the nickel 63 radiation source with non radioactive ionization source. Possible alternative ionization sources include a laser ionization source and a barrier discharge source. The third effort will focus on improving the sample collection device employed by IMS systems. Currently the swiping approach has variables in the pressure an operator applies to the surface of a swipe, the material of the swipe, and choosing the correct 'hot' spot to interrogate on the target. This phase will investigate ways to improve sample collection from surfaces by using other swipe materials or other possible collection devices.

Requirements:

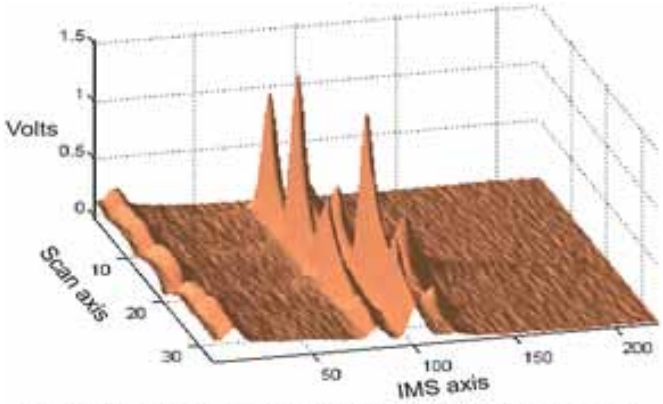
- Joint Urgent Operational Needs Statement CC-0315
- Joint Urgent Operational Needs Statement CC-0490
- Integrated Unit, Base Installation Protection ICD
- Joint Urgent Operational Needs Statement CC-0255
- Improvised Explosive Device Defeat ICD
- Portable Chemical, Biological, Radiation, Nuclear, Explosive (CBRNE)/Weapons of Mass Destruction Detector, Navy Urgent Operational Needs Statement
- Integrated Base Defense Security System CDD
- Joint Service Explosive Ordnance Disposal ICD
- CBRNE Sense ICD

Accomplishments:

- Began analyzing potential confusants
- Started evaluating current swipe technologies
- Began ionization technique system engineering study

Key Dates/Milestones:

- Characterize False Alarms and Confusants
- False Alarm/Confusants experiments and propose analysis changes
- Evaluation of Potential Ionization Technologies
- Develop Plan for Ionization Incorporation
- Evaluate Sampling Improvements
- Implement Improved Sampling
- System Testing

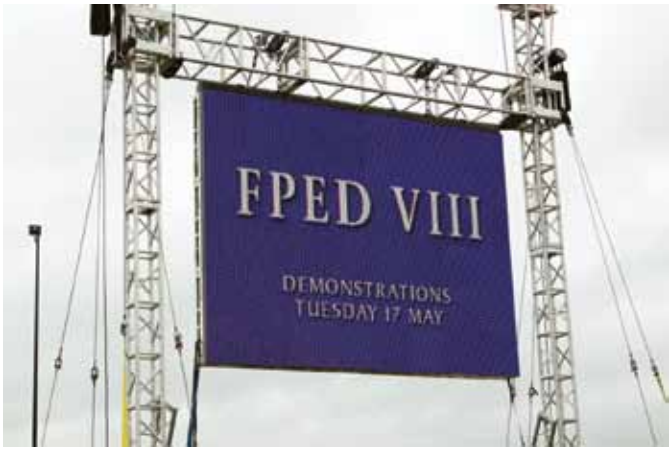


TSD-IMS data of a representative Composition B sample

ACTIVITIES

Force Protection Equipment Demonstration (FPED)

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 by the DoD Physical Security Equipment Action Group, administered by the Office of the Assistant Secretary of Defense for Nuclear and Chemical and Biological Defense Programs/ Nuclear Matters, and executed by the Product Manager, Force Protection Systems. 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 2009 and 2011 have generated more than $275 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:

- Executed FPED VIII, Stafford Regional Airport, 17-19 May 2011
- Completed event After Action Report (AAR)
- Conducted post event awards ceremony with JPEO (BG Scarbrough) and key organizations at Stafford County
- Conducted post event survey to determine sales generated as a result of the demonstration ($170 million dollars)
- Distributed more than 4,500 FPED VIII CD's to the user community

Key Dates / Milestones:

- Develop Memorandum of Agreement between JPMG and NDIA for event execution in 2013

Hailing Acoustic Laser & Light Tactical System (HAL2TS)

The HAL2TS is a portable non-lethal based system that will provide the United States Navy with an effective layered defense option. HAL2TS allows the sailor to take preventive measures to avoid "deadly force" outcomes, while optimizing personnel safety through self-protection and enhanced distance threat engagement. The complete HAL2TS system consists of commercial-off-the-shelf (COTS) equipment including an acoustic warning device (e.g. hailer), visual warning device (e.g. dazzling laser), and illumination device (e.g. white light). The integration of these technologies, into a single unit, will alleviate the strain on limited crew operations by allowing all three devices to be controlled by a single operator. The HAL2TS system can meet the broad capability needs of the Navy and empower personnel to enforce exclusion zones around High Value Assets (HVA) in order to deter and interdict perceived threats in restricted-access and open waters, piers, and waterside facilities.

Requirements:

- Counter-Materiel Joint Non-Lethal Effect Initial Capabilities Document (ICD), March 2009
- Counter-Personnel Joint Non-Lethal Effects ICD, March 2009
- Escalation of Force ICD, July 2009
- Maritime Expeditionary Security ICD, May 2007
- Naval Surface Warfare Center, Dahlgren Division (NSWCDD) Warning Device Solicitation N001781-2Q3900 identifying need for non-lethal systems, October 2011

Accomplishments:

- Issued Request for Information (RFI) and analyzed industry responses
- Selected system components for prototype development and procured 90%
- Developed initial system performance requirements and designs

Key Dates / Milestones:

- Project Start Date (Phase I Initiated): August 2011
- RFI Issued: October 2011
- Developed Draft operational scenarios: November 2011
- Initial Proof-of-Concept Demonstration and Evaluation: May 2012
- Operational Demonstration: June 2012

Integrated Defense Command and Control Common Operating Picture (IDC2COP)

The 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 first responders with a variety of incident management capabilities such as near real-time/dynamic sharing of tactical situational awareness, GPS and blue force tracking, automated generation and placement of incident response elements (e.g. cordons, TCP, road closers, etc.), Building notification/evacuation management, automation of incident report and Quick Response Checklist (QRC) and instant messaging. 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 2011, IDC2COP participated in Mobile Unified Capabilities (MUC) and Joint Expeditionary Forces Experiment (JEFX), aligning Security Forces requirements with Air Force Communications Unified Capabilities (UC) Strategic Master Plan.

Requirements:

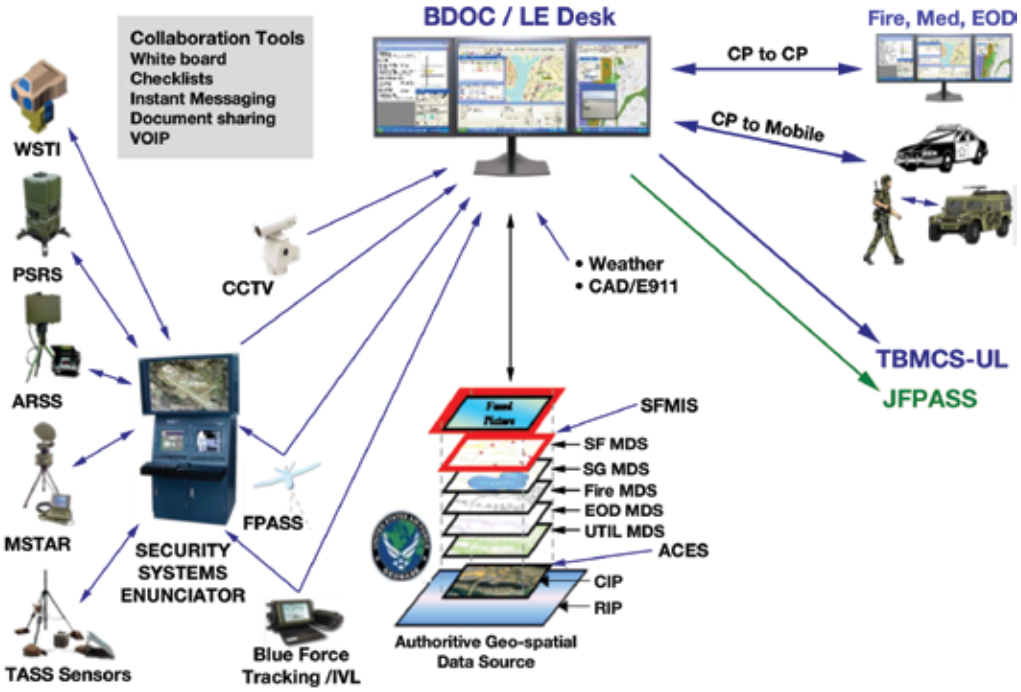
- USAF command and control concept for prototype Base Defense Operations Center (BDOC)
- Security Equipment Integration Working Group (SEIWG) architecture requirements
- Integrated Base Defense Security Systems (IBDSS) Capability Development Document (CDD), 17 February 2005

Accomplishments:

- Participation in Mobile Unified Communications Experiment I
- Initiated transition efforts of Program Management to System Program Office (SPO) – SPAWAR
- Obtained Interim Authority to Operate (IATO) for IDC2COP version 1 (non-wireless)
- Initiated Integration efforts with Installation Incident Management System (IIMS)
- Deployment under Interim Authority to Test Authority

Key Dates / Milestones:

- Initiation development of IDC2COP Wireless Configuration: December 2011
- Independent IA Assessment: September 2011
- Version 1 deployment at Spangdahlem AB: CY 2011
- Project End Date: Version 1 September 2012



ACTIVITIES

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

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 ability to provide and fuse detected activity information, regardless of format, that is mutually supporting across services and agencies is critical. 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:

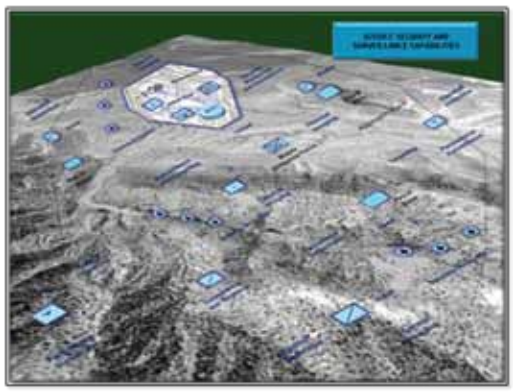
- Draft IGSSR-C Capability Development Document (CDD)
- IUBIP JCD, 17 July 2007
- IUBIP Capabilities Based Assessment Capabilities Based Assessment (CBA), September 2007
- IUBIP Detect Assess Defend (DAD)Initial Capabilities Document (ICD), 2 October 2009
- IUBIP Interoperability Initial Capabilities Documents (ICD), 15 September 2009
- Consequence Management (CM) ICD, 17 September 10
- Chemical, Biological, Radiological, and Nuclear Consequence Management ICD, 13 April 06
- Joint Urgent Operational Needs Statement (JUONS) # CC0201, CC0202, CC0214, CC0216, CC0235, CC0239, CC0240, CC0241 and CC0262

Accomplishments:

- Assisted MSCoE in adjudication of 1 Star comments on the draft IGSSR-C CDD
- Completed staffing and approval process on the IGSSR-C Performance Specification
- Initiated an analysis of government developed “fusion” solutions
- Designed, built and tested for performance and functionality a Recording & Playback test fixture to support candidate fusion engine capability evaluation
- Completed effort on the System Engineering Plan, Technical Development Strategy, Test & Evaluation Strategy, Life Cycle Cost Estimate and initiated effort on the Acquisition Plan and a Program Protection Plan
- Completed all required Operational and System View Architectures

Key Dates / Milestones:

- PSE RDT&E Program start date - 1 May 2010, Increment 1 effort initiated
- Projected PSE RDT&E Program end date - 30 September 2017, Increment 3 MS C
- First Unit Equipped (FUE) - 4QFY14



Interim Integrated Base Defense (I-IBD)

The I-IBD effort is being conducted to improve efficiencies, integration, and interoperability of existing base defense systems. These improvements include fusion, automation, and integration; reduction in duplicative capabilities; assessment and dissemination of threat information; reduction in troop to task ratios and training requirements; and improvement in base defense systems interoperability. I-IBD is able to operate with existing area LAN and CENTRIX infrastructure with no new hardware or additional manning. This overview will focus on four major parts: Increment I, Increment 2, Joint Defense Operations Center (JDOC) Collapse and Network Integration Evaluation (NIE).

Requirements:

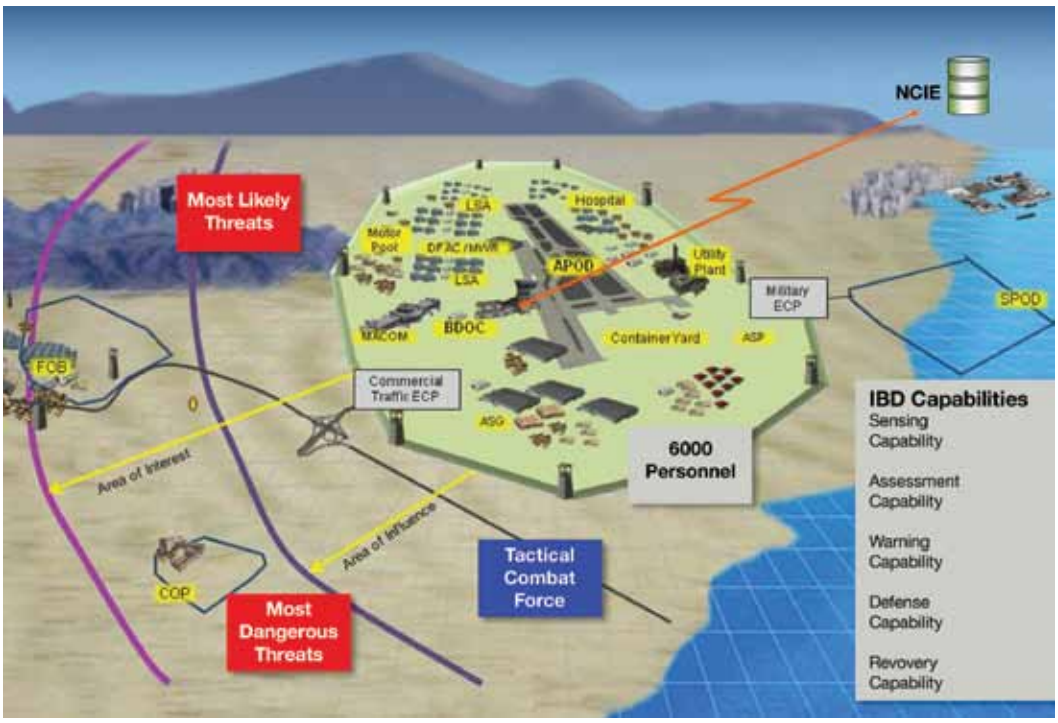
- Base Expeditionary Targeting & Surveillance System – Combined (BETTS-C) JUONs CC-0296 Mod 4
- Rapid Equipping Force 10-liner for Joint Defense Operations Center (JDOC) Collapse at Bagram Air Base
- Ground Based Operational Security System (Expeditionary) (G-BOSS(E)) Capabilities Development Document

Accomplishments:

- Integrated Fusion, Automation and Integration, proving value-add, reduction of troops to task and efficiencies gained.
- Conducted analysis of technical solutions to provide full motion video between G-BOSS and CX-I
- Tracked Increment 1 solutions to provide interoperability with BETTS-C systems and other CENTOM sensors
- Coordinated core IBD capabilities in accordance with ASA(ALT) Office of the Chief Systems Engineer IBD reference design for Fusion and Automation, Biometrics use at an Entry Control Point (ECP)

Key Dates / Milestones:

- Conduct analysis, architectural and technical solutions for I-IBD Increment 2 interoperability with Centrix Network: December 2011
- Complete planning and architectural views for Phase I of JDOC Collapse: December 2011
- NIE 13.1 Systems Under Evaluation selection: March 2010
- Conduct analysis and architectural drawing to upgrade I-IBD Increment 1: July 2012



ACTIVITIES

Intermodal Security Devices

The Intermodal Security Devices project provides the war fighter with the ability to remotely monitor the security status of temporary AA&E storage in accordance with DoD 5100.76M policy requirements. Develop remote monitoring capability for permanent and temporary storage of Arms, Ammunition, and Explosives (AA&E). Demonstrate the integration of Advanced Container Security Device (ACSD) breach detection sensor of Army Next Generation Wireless Communications (NGWC) mesh network, meeting operational, explosive safety, and information assurance requirements. Demonstrate high, medium and low performance/cost sensor an applications for AA&E storage using NGWC mesh network.

Benefits: improved situational awareness, while reducing required manpower.

Goal: Improve situational awareness of temporary and permanent AA&E assets while reducing operations cost.

Bottom Line: As demonstrated, the system provides enhanced monitoring of AA&E, while reducing manpower. Many other applications possible.

Requirements:

- Supports IBD CDD Detect 1,6,7;
- Navy ATFP Ashore CDD 4.7, 4.8, 4.9 & 4.10
- OPNAVINST 5530.13C Standards for Secure Holding Areas
- DoD 5200.08-R Integration/Modernization
- OPNAV 5530.14E
- DoD Directive 5100.76M
- Army Regulation 190-11

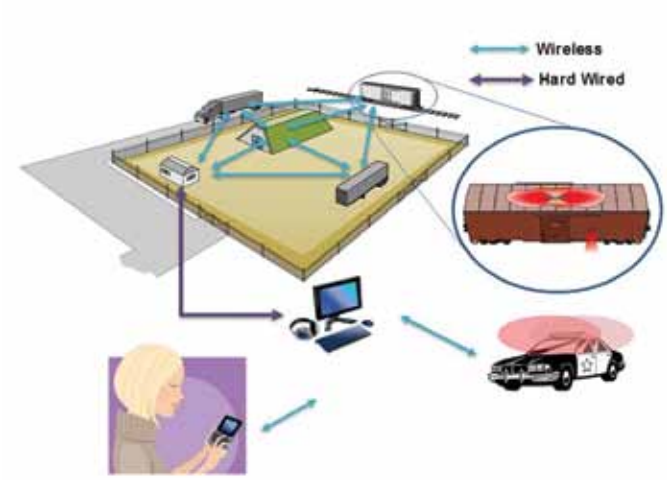
Accomplishments:

- ACSD sensor improvements:
  - o Ability to integrate with NGWC mesh network
  - o Improved volumetric sensing performance
- Procure NGWC mesh network components
- Smart Phone Technology Integration into NGWC for AA&E applications
- Enhance Intermodal Security Test bed to include truck, CONEX, air cargo assets

Key Dates / Milestones:

- Start date: January 2010
- Expected end date: September 2012

Advanced Container Security Device Volumetric Sensor



Mesh Network and Sensors Integrated with Local and Regional Command and Control Assets

Mesh Network and Sensors in a Remote Location

ACTIVITIES

Joint Interface Group for Security Application Workspaces (JIGSAW)

The JIGSAW is a joint program promoting a unified approach to assembling the required component 'pieces' of DoD Command & Control (C2) systems. These interoperable pieces involve sensor systems and the associated software interfaces used to visualize the sensor data in Force Protection (FP) environments across all Service/Agency lines.

The JIGSAW approach implements a Service Oriented Architecture (SOA) that will host sensors in a 'secure sensor cloud' allowing data subscriptions from 'Software Interface Modules' (SIMs). These SIMs can then be assembled to support Integrated Base Defense applications such as Forward Operating & Fixed Base perimeter surveillance. This cost effective communication approach will allow integration of associated control systems such as Access Control, Intrusion Detection, Fire & Emergency Services and Weapons Systems.

Requirements

- Audit and analyze existing DoD Command & Control software systems.
- Develop a system design that reduces the time and cost associated with Command & Control sensor data integration.

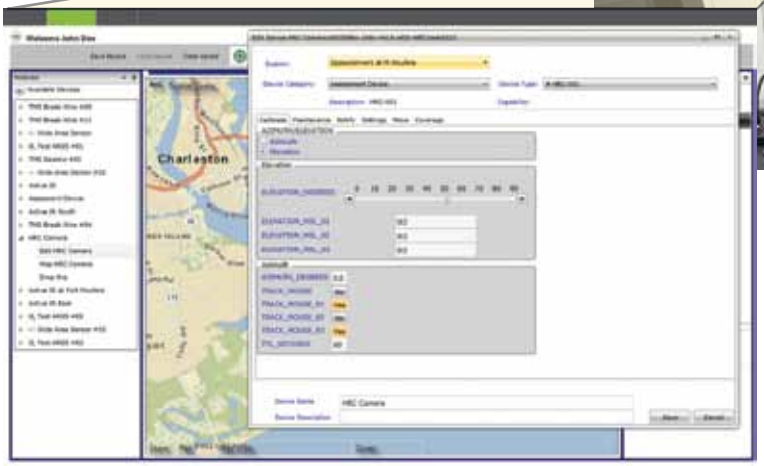
Accomplishments

- Completed Command & Control systems audit including 28 different packages used by the DoD.
- Created a browser-based modular user interface architecture that supports sensor integration modules. Modules can be deployed automatically and run in Command and Control Display Equipment (CCDE) and C2 applications without modifying the core application framework.

Key Dates/Milestones

- Completed CCDE Audit: February 2011
- Presented conceptual demonstration at FPED: May 2011
- Software development of JIGSAW framework initiated: July 2011
- Device Interface Abstraction Database Build Completed: October 2011
- Completed initial device of JIGSAW Interface Management (SLIM) tool allowing sensor manufactures to easily design their sensor device's JIGSAW compliant data interfaces and deploy an installable sensor interface definition: February 2012
- Completed initial JIGSAW CCDE / C2 browser –based application with capabilities to administer JIGSAW devices, render GIS displays and setup JIGSAW module authentication: February 2012
- Device Management and Modular CCDE Initial Demonstration: September 2012

JIGSAW
JOINT INTERFACE GROUP FOR SECURITY APPLICATION WORKSPACES



Lighting Kit, Motion Detector (LKMD)

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.

Requirements:

- Capability Production Document, 14 April 2008

Accomplishments:

- First Unit Equipped: 25 September 2010
- Completed Initial Production Delivery of 8,800 systems: September 2011
- Fielded 5,705 systems in FY11

Key Dates / Milestones:

- Start Date for PSE RDT&E: March 2003
- End Date for PSE RDT&E: June 2009

LKMD Indoor Training

LKMD Outdoor Training

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

AFRL/RXQF is currently involved in the research and development of a National Air Space Integration Demonstrator for STUAS Alarm Response. This project is a Sense and Avoid payload development effort to support the USAF and 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 in Class G airspace in an alarm response action prior to a QRF being deployed. The developed payload will be 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 GCTS at Camp Guernsey. This project had previously been working on a convoy support UAS and in October 2010 was realigned with AFSOC and USAF needs to support domestic capability gaps in the upcoming STUAS II acquisition.

Requirements:

- IBDSS
- OSD Airspace Integration Plan for Unmanned Aviation
- USAF Unmanned Aircraft Systems Flight Plan 2009-2047
- STUAS CDD

Accomplishments:

- Selected Tier II Class UAS demonstrator system and acquired power plants and airframes
- Developed a disposable Tier II test bed for sense and avoid testing
- Identified sense and avoid strategies and began concept development
- Integrated AFSOC user objectives
- Developed power supply controller board to include fail safe and critical power assurance
- Conducted testing of autonomous control module development
- Completed testing library for STANAG and autopilot
- Finished tests of UAS antenna tracking system
- Received autopilot systems as the baseline compatibility systems
- Conducted first phase of SME interviews
- Developed power supply controller board to include fail safe and critical power assurance
- Completed training plan for AFRL to conduct test-bed UAS platform initial flights

Key Dates / Milestones:

- Start Date: 9 November 2009
- End Date: 20 September 2012

Navy Integrated Waterside Security Feasibility Study (IWS)

The intent of the IWS Feasibility Study is to take a broad approach to the process of understanding RDT&E requirements for the improvement of waterside security specific to the Navy at conventional and nuclear bases, with an eye on potentially broader applications for all the Services that have bases and installations with waterside security concerns. The overall purpose of the study is to review waterside security postures at select CONUS and OCONUS naval stations, naval submarine bases, naval weapons stations and naval air stations in order to gain a greater understanding of policy, command/control, and physical security equipment integration; to identify capability gaps and associated vulnerabilities; and to identify those gaps that may be mitigated through the application of physical security equipment R&D efforts.

Requirements:

- USFFC ATFP IPCL
- Navy SSP Security Deviations
- USFFC Anti-terrorism OPORDER (Jun 2009)
- USFFC Defensive AT CONOPs (Nov 2009)

Accomplishments:

- Research team completed eight site visits to naval stations, air stations, sub bases and weapons stations to collect data, interview command personnel and conduct discussions with physical security leadership.
- Presented preliminary findings to U.S, Fleet Forces Command (USFFC) and Commander, Navy Installations Command (CNIC) ATFP staff officers.
- The preliminary findings were used to inform the planning and preparation for a Navy PSEAG sponsored Integrated Waterside Security workshop set for 2012.
- Attended annual Navy Anti-Terrorism Program, Integrated Capabilities Requirements Review Board (ICRRB) at the Pentagon: August 3-5, 2011

Key Dates / Milestones:

- Develop short list of leading AT/FP functional areas with apparent capability gaps or shortfalls yet to be addressed
- Participate in the annual USFFC Navy Anti-terrorism EA Conference and the Anti-terrorism Warfare Improvement Program (AT-WIP) Conference with key Navy Afloat, Ashore and Expeditionary stakeholders: June 2012
- Continue to refine IWS Workshop results to develop the requirements for a technology demonstration in FY-13 with potentially wide applicability within Navy and Marine Corps

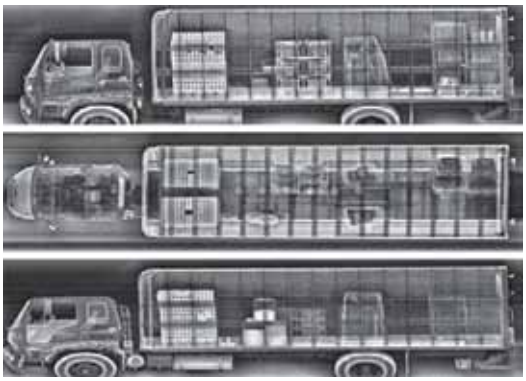
Performance Maintainability Kit for Explosive Detection Equipment

A variety of trace explosive detection, small bulk identification and Vehicle Borne Improvised Explosive Device (VBIED) detection equipment has been fielded for use by the DoD. Once fielded, it can be difficult for users to assess if their equipment is working as designed. Additionally, once detection equipment is put into service, operators may go long periods of time before an alarm occurs or before a positive threat detection occurs. These long time periods between alarms can lead to degradation of the user's sampling technique or image analysis skills reducing the effectiveness of the detection equipment.

The objective of this effort is to develop a kit, requiring no special handling or storage requirements, that contains test materials which provide the users a means to evaluate the functionality of their equipment. The kit could also be utilized as a tool to enable EDE users to practice sampling techniques, image analysis and alarm resolution protocols. 20 trace/small bulk kits and 10 vehicle kits will be produced for fielding to sites designated by PSEAG

Requirements:

- JUONS CC-0315, CC-0490, CC-0255
- Integrated Unit, Base Installation Protection ICD
- Improvised Explosive Device Defeat ICD
- Portable Chemical, Biological, Radiation, Nuclear Explosive (CBRNE)/Weapons of Mass Destruction Detector, Navy Urgent Operational Needs Statement
- Integrated Base Defense Security System CDD
- Joint Service Explosive Ordnance Disposal ICD
- CBRNE Sense ICD
- Notional Concept 07-07 High Fidelity Weapons of Mass Destruction Identification Kit



Accomplishments:

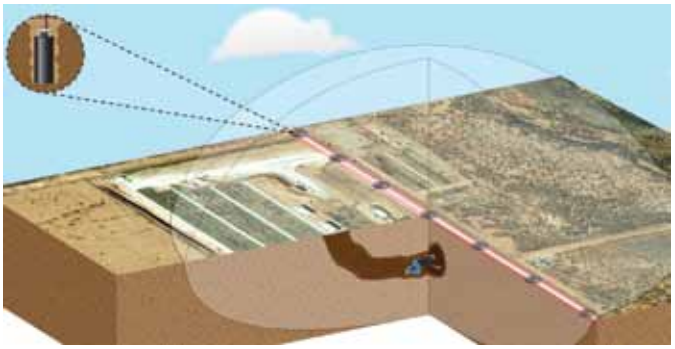
- Reviewed previous test results to determine optimal material and objects for vehicle kit
- Developed a concept for a imager performance test based on the ANSI

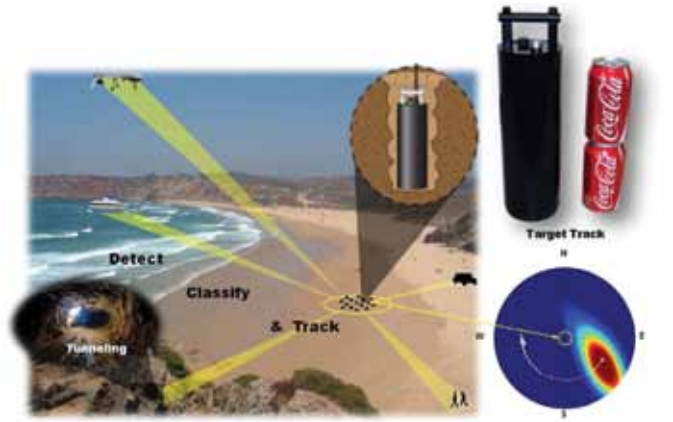
Key Dates / Milestones:

- Start Date: April 2011
- End Date: March 2013
- Complete design and testing of Kit: October 2012

Seismic-Acoustic Detection and Ranging (SADAR) System

SADAR is a covert intruder-detection system which passively and autonomously analyzes Seismic-Acoustic (SA) energy to determine the range, direction, speed and classification of the intruder(s). This evolutionary SA technology leverages an array of advanced solid-state sensors that exhibit up to 5X greater sensitivity than commercial-off-the-shelf geophones. A smart central node coherently processes peripheral sensors' time-synchronized signals across an expanded bandwidth to detect, classify, and track multiple targets simultaneously in near-real time. Technology development and demonstrations are being orchestrated by the Air Force, Navy and DTRA to characterize SADAR's vast military utility for Anti-Terrorism/Force Protection (ATFP) in all domains: terrain surface (crawlers, walkers, runners, vehicles, animals), underground (tunneling), littoral/maritime (swimmers, motorboats, jet boats, shallow submersibles), and air (UAVs, ultralights, rockets, fixed and rotary wing aircraft). The work is derived from an earlier effort by the Engineer Research and Development Center (ERDC) of the US Army Corps of Engineers entitled, "Optimally Designed Wireless Seismic/Acoustic Ordnance Impact Characterization System." Quantum Technology Sciences, Inc. is the contractor.





Requirements:

- ATFP capability gaps are identified by U.S. Air Force Major Commands (MAJCOMs)
- Integrated Base Defense Security Systems (IBDSS) Capability Development Document (CDD), February 2005, Detection, Assessment/Surveillance
- Naval Facilities Engineering Command (NAVFAC) ATFP Ashore General Enclave Performance Specification
- DoD Directives 3020.40 and 3020.45
- DoD Instruction 2000.16, 5200.08, 5200.08R
- Chief of Naval Operations Instruction (OPNAVINST) 5530.14C

Accomplishments:

- System hardware design and optimal configuration studies underway for first functional prototype
- Software development and rapid classification algorithms underway for hardware integration
- Quality and manufacturing plan developed
- Operationally relevant test sites identified and in coordination for summer demonstrations

Key Dates / Milestones:

- Start Date: November 2011
- System Requirements Review: February 2012
- Prototype Demonstrations: June & July 2012
- Project End Date: October 2012

Sensor Fusion

Currently Fourier Transform Infrared and Raman systems are available in handheld form factors. The systems are complementary in their performance with each having their own unique strengths and weaknesses. It is often found that materials one system cannot identify well the other is capable of identifying. This effort would select the best performing Raman and IR systems from our previous comparative testing for a systems integration effort. These two systems will be integrated into a single handheld unit, thus providing both technologies with a reduced equipment footprint.

Requirements:

- Joint Urgent Operational Needs Statement CC-0490
- Integrated Unit, Base Installation Protection ICD
- Joint Urgent Operational Needs Statement CC-0255
- Improvised Explosive Device Defeat ICD
- Portable Chemical, Biological, Radiation, Nuclear Explosive (CBRNE)/Weapons of Mass Destruction Detector, Navy Urgent Operational Needs Statement
- Integrated Base Defense Security System CDD
- Joint Service Explosive Ordnance Disposal ICD
- CBRNE Sense ICD
- Notional Concept 07-07 High Fidelity Weapons of Mass Destruction Identification Kit

Accomplishments:

- Determine optimal Raman and IR based systems from previously conducted comparative studies by the EDE Program
- Award a contract
- Kickoff meeting held with requirements for the proposed effort

Key Dates / Milestones:

- Contract Award: February 2012
- Prototype development begins: October 2012
- Critical Design Review: January 2013
- Prototype tested at NAVEODTECHDIV: April 2013
- Field Prototypes delivered: June 2013
- Three prototypes delivered to NAVEODTECHDIV for test and evaluation. Test Report posted on PSEAG portal.

Shipboard Security Systems

This project ensures that protection of classified information and materials aboard ship and other DoD mobile platforms meet established physical security protection requirements while withstanding the shock, vibration, and environmental conditions found in their operational environments. Deliverables for this project include the security container tie down system; GSA approved shipboard security containers and mounting systems; federal specifications for manufacturing and testing physical security equipment; and updates to policy requirements, to mitigate current security vulnerabilities and standardize protection of classified information aboard DoD mobile platforms .At the completion of this project, a new class of GSA approved security container used to secure classified materials aboard DoD mobile platforms will be developed. This new container will have an integral mounting system, be structurally capable of withstanding its environmental stresses, provide application flexibility, and provide the same physical security resistance, while reducing overall container weight by half.

Requirements:

- DoD Directive 5200.1-R, January 1997
- OPNAVINST 5530.13C, September 2003
- SECNAVINST M-5510.36, June 2006

Accomplishments:

- Produced final GSA Class 5 & 6 Container Drawer Insert proof of concept for storing classified laptop computers
- Delivered container drawer insert to acquisition sponsor for analysis and feedback
- Delivered final container drawer insert drawing package to sponsor
- Evaluated and analyzed lightweight container physical requirements and testing parameters

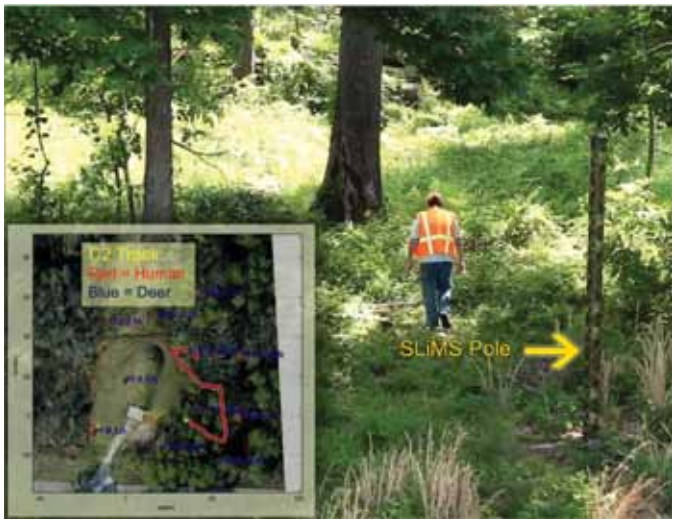
Key Dates / Milestones:

- Project Start Date – October 2008
- Drawer Insert Proof of Concept delivered – February 2011
- Drawer Insert Test and Evaluation – March-June 2011
- New Lightweight Container Capabilities Evaluation – December 2011
- New Lightweight Container Test Requirements – April 2012
- New Lightweight Container Draft Specification – July 2012
- New Lightweight Container Prototype – April 2013
- New Lightweight Container Test and Evaluation – September 2013-June 2014
- Lightweight Container Final Specification – June 2015
- Project Transition Date – September 2015

Shore-Line Monitoring System (SLiMS)

The SLiMS is an all-weather virtual fence. It is an all-digital system with Ultra-Wide Band (UWB) radars and advanced algorithms to Detect, Track, and Classify targets based on geometry. It discriminates bipeds (humans) and quadrupeds (deer), and ignores birds and small animals resulting in order-of-magnitude lower Nuisance Alarm Rates and False Alarm Rates (NAR/FAR).

SLiMS is the only Intrusion Detection System (IDS) which classifies targets without needing cameras or other sensors. SLiMS provides an environmentally acceptable solution where no other sensors are suitable or capable: along shorelines, light woods, and marshes. The goal of the project is to deliver a Technology Readiness Level (TRL) 7-8 system ready for procurement as Commercial-Of-The-Shelf (COTS).



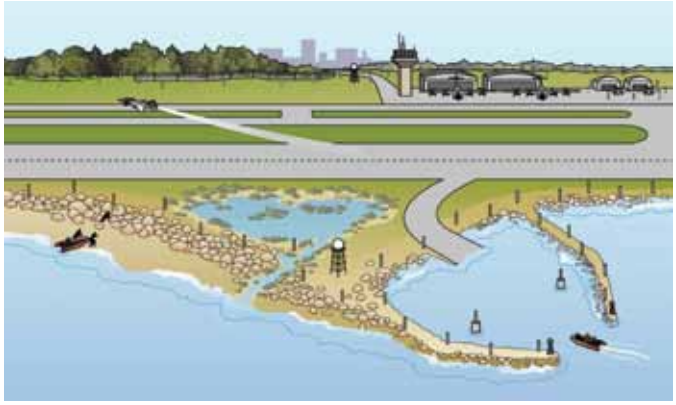
SLiMS at Redstone Arsenal – Summer 2011

Requirements:

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

Accomplishments:

- Automatic Target Classification
- Environmental Packaging
- Deployable/Testing Prototypes
- Performance Testing
- Spectrum & HERO Certification Tests



SLiMS Deployment at Naval Air Station

Key Dates / Milestones:

- Project Start Date: Fiscal Year 2009
- Performance Test: FY11 – FY12
- HERO and Spectrum Certification: FY12
- TRL 7 System for Operational Test: FY12
- Operational Test to Meet AT/FP Ashore P-Spec: FY13
- TRL 8 System: FY13
- Project End Date: FY13 (anticipated)

Single Crystal-Based, Acoustic Non-Lethal to Lethal, Scalable Engagement System for Expeditionary Swimmer Defense Applications

The objective of the Single Crystal-Based, Acoustic Non-Lethal to Lethal, Scalable Engagement System for Expeditionary Swimmer Defense Applications project is to design, build, integrate and test a single-crystal based, low frequency acoustic swimmer engagement system. The SC Swimmer Engagement System shall be compact, lightweight, scalable and operator selectable (from non-lethal to lethal), providing a man-portable non-lethal and lethal capability to engage open and closed circuit divers. This project leverages previous transducer development funded by the Office of Naval Research and NUWC Division Newport internal investments. In FY11-12, a single crystal-based, non-lethal to lethal engagement transducer shall be optimized, prototyped and tested. In FY13, this transducer shall be combined with power electronics and packaging to demonstrate an integrated acoustic engagement system design. This project will provide a transition quality compact expeditionary capability that provides seamless, non-lethal to lethal engagement of threat swimmers to the Integrated Swimmer Defense POR.

Requirements:

- Naval Expeditionary Combat Command (NECC) Maritime Expeditionary Security Force (MESF) Initial Capabilities Document (ICD)
- Joint Non-lethal Effects Capabilities Based Assessment Functional Needs Analysis

Accomplishments:

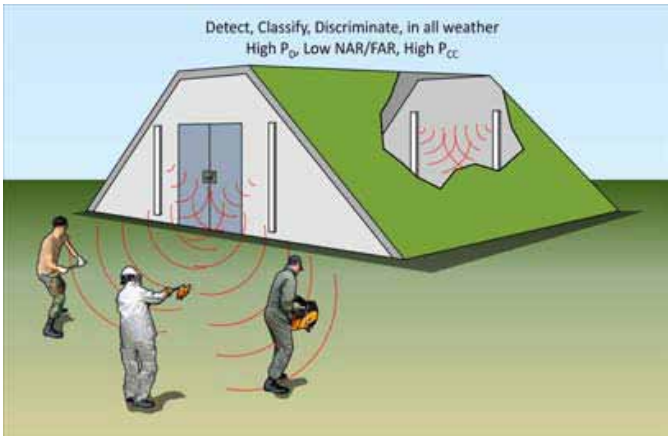
- Single crystal engagement transducer design optimized optimization to meet lethal/non-lethal swimmer engagement levels complete
- Optimized design provides two resonances targeting lung resonance (lethal engagement) and swimmer aversion response (non-lethal engagement)
- Estimated transducer weight 60 lbs or less
- Transducer produces 202 dB re 1 μPa @ 1m in non-lethal engagement frequency region

Key Dates / Milestones:

- Project Start Date: September 2011
- SC Transducer Optimization Complete: December 2011
- SC Transducer Construction Complete: July 2012
- SC Transducer In-water Performance Validation: September 2012
- Integrated SC Swimmer Engagement System Prototype Complete: July 2013
- In-water Evaluation of SC Swimmer Engagement System Prototype: September 2013
- Transition to Integrated Swimmer Defense Program: October 2014

Smart Magazine

Current magazine designs are typically 1940-60s vintage that do not accommodate the operational needs of today's weapon storage. Nor are they capable of providing sufficient security against emerging threats without rigorous and costly security force attendance. Smart Magazine addresses the magazine as a system, with architecture of layered functionality. The Physical & Structural design provides a cost-saving hardened structure meeting seismic, explosive, and security requirements, while reducing the ESQD footprint. Mechanical components assure reliable operation of the door, and include dead bolt, multi-point locking devices for superior attack resistance. Electrical components allow remote re-locking, biometric authorization, and support a sensor package that can detect, classify, and discriminate attackers in all-weather before they reach the door, and audit stored weapons. Electronic components communicate events to auditing and notification systems on stealth wireless communications. The entire layered concept provides a tough and Intelligent, self-protecting, self-monitoring magazine.



Requirements:

- DoD 5100.76M Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
- NAVFAC AT/FP Ashore – Performance Specification for the Anti-Terrorism Force Protection General Enclave – 20100729 NAVY ATFP PERF GENCLV – 29 July 2010.
- OPNAVINST 5530.13C, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
- OPNAVINST 5530.14B, Physical Security Manual
- DoD Directives 3020.40 and 3020.45
- DDESB Letter on Protective Construction 21 Oct 2008

Accomplishments:

- Demonstrated multipoint locking system, thermal re locker, and biometric key authorization
- Demonstrated sensor capability for automatic classification (human/deer) High PD, Low NAR/FAR, High PCC
- Completed HERO certification tests for all key sensors.
- Validated improved fragment and blast resistant wall sections by explosive safety tests

Key Dates / Milestones:

- Project Start Date: FY 2009
- Performance Test: FY11 – FY12
- HERO and Spectrum Certification: FY12
- TRL 7 System for Operational Test: FY12
- Operational Test to Meet AT/FP Ashore P-Spec: FY13
- TRL 8 System: FY13
- Project End Date: FY13 (anticipated)

Tactical Video Surveillance System (TSS)

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.

Requirements:

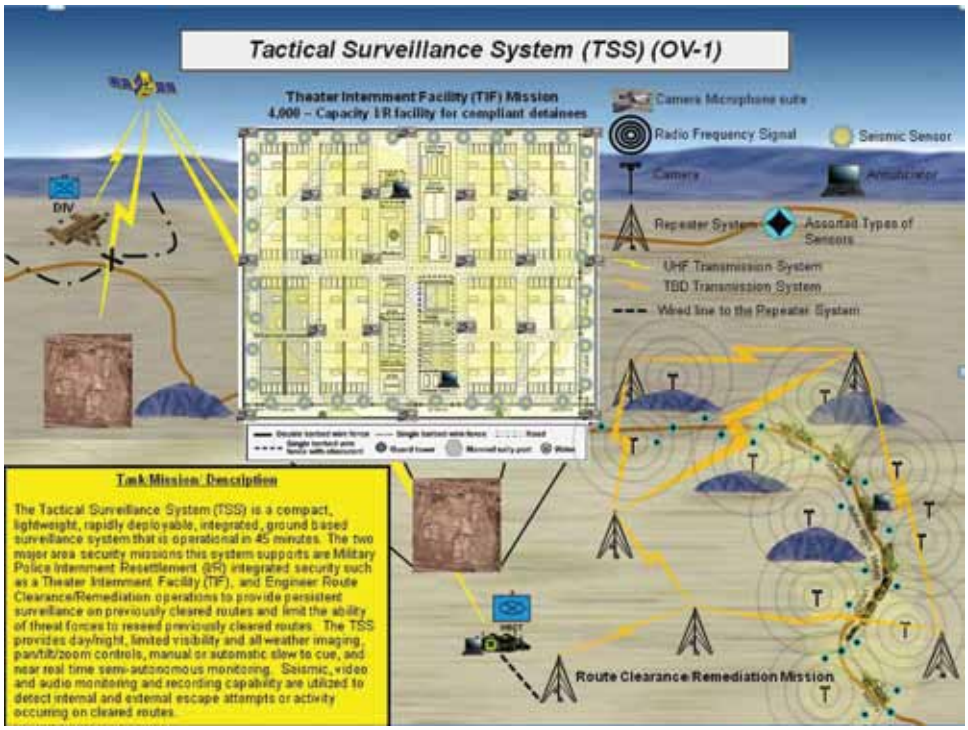
- Draft TSS Capabilities Development Document (CDD)
- Soldier as a System (SaaS) Initial Capabilities Document (ICD), 21 October 2005
- Joint Explosive Hazard Defeat (JEHD) ICD, 1 May 2006
- Integrated Unit, Base, Installation Protection (IUBIP) Detect Assist Defend, Initial Capabilities Document (ICD),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

Accomplishments:

- Draft CDD completed World Wide Staffing
- Began development of Department of Defense Architecture Framework Views

Key Dates / Milestones:

- Start date of PSE RDT&E Program – 1QFY04 [then called Tactical Video Surveillance System]
- Anticipated Materiel Development Decision – 2QFY13



ACTIVITIES

APPENDICES

Navy
USAF
Army
PROC&S
RDT&E
PSEAG
Material Development Responsibilities
(DASD NCB/NM)
PSEAG Charter (DoDI 3224.03)
• Minimize RDT&E duplication
• Ensure interoperability
• Ensure acquisition compliance
PSEAG
• Minimizes RDT&E duplication
• Ensure interoperability
• Ensure acquisition compliance
SPVC
PHYSICAL SECURITY ENTERPRISE PROGRAM
PSEAG
Introducing the PSEAG Intranet
PHYSICAL SECURITY ENTERPRISE & ANALYSIS GROUP

Appendix A. Information Repository for PSEAG Funded Programs

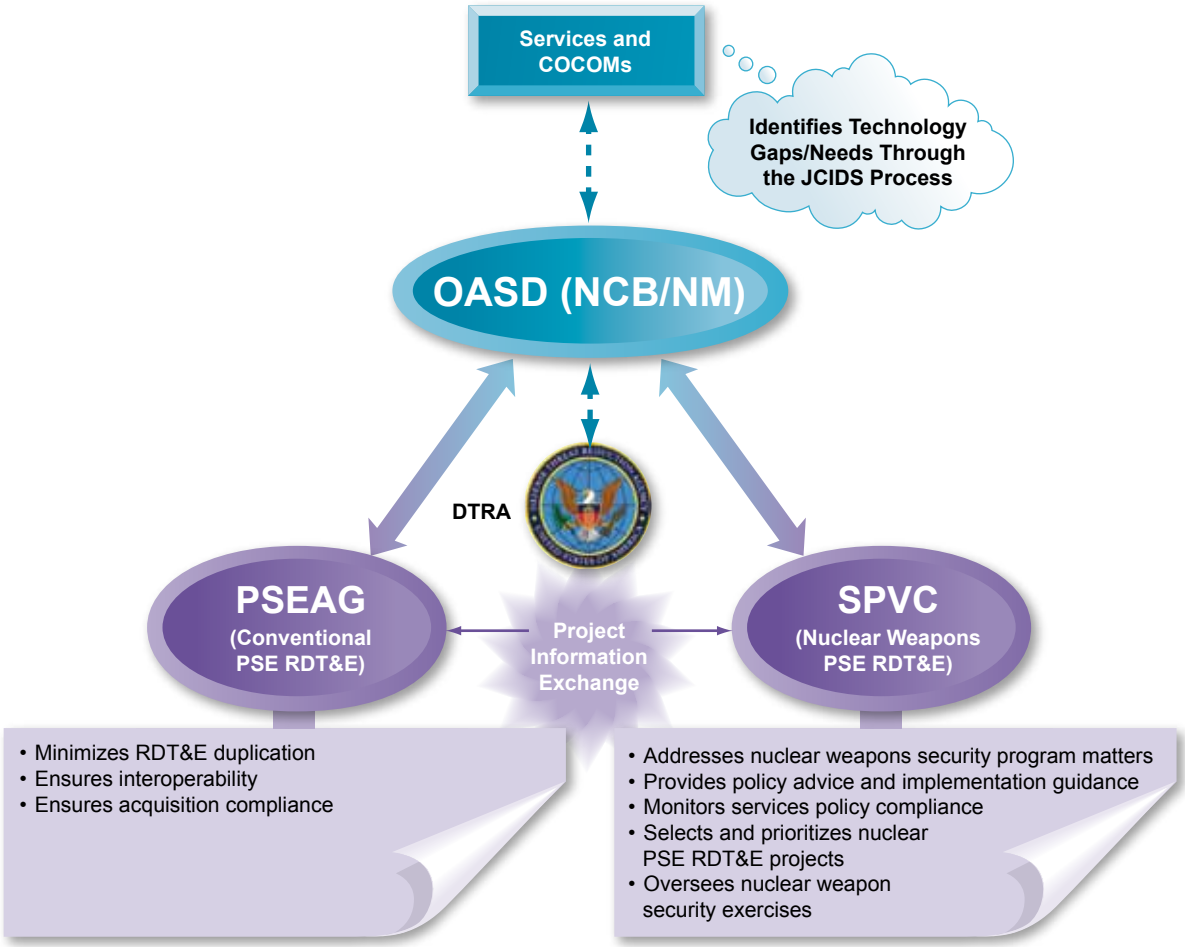
The Physical Security Equipment Action Group (PSEAG) is currently developing an intranet portal (left) that will allow Program Area Managers (PAM)s, government representatives, support contractors and other approved users to access a wealth of Physical Security Equipment related information, upload reports, view PSEAG History projects and collaborate in a secured environment. 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.

The electronic PSEAG (ePSEAG) is a project management tool that will be accessible from the PSEAG Intranet that will be used by PSEAG representatives to track RDT&E funding for various PSEAG funded projects (right). This project management tool will allow for the identification of capability gaps, and to request RDT&E funding for new projects. This tool modernizes the once tedious paper process, and standardizes the format for all future projects. The ePSEAG system will also allow for users to enter financial and schedule data for projects, from which the system will generate reports and display project health information for use by managers and in conducting project reviews. The ePSEAG system will also become an archive of project data and a useful tool for referencing old projects and reporting on historical data.

APPENDICES

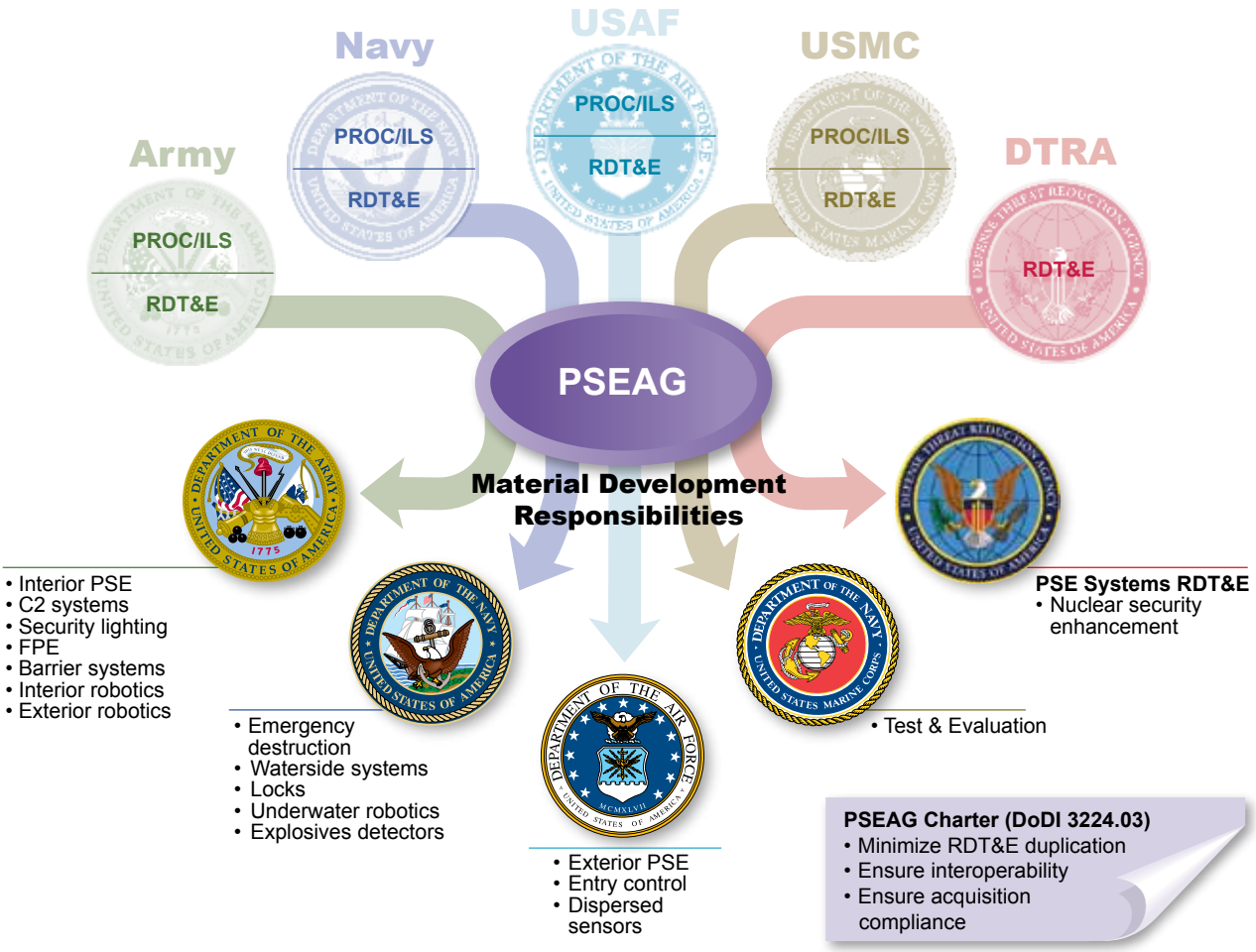
The Department of Defense (DoD) Physical Security Equipment (PSE) Research, Development, Test and Evaluation (RDT&E) Program responds to the material needs expressed by the Services and the Combatant Commands (COCOMs). Physical security equipment capabilities, or gaps in capabilities, are identified 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.



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 D. Security Equipment Integration Working Group (SEIWG)

As a permanent working group of the Department of Defense (DoD) Physical Security Enterprise & Analysis Group (PSEAG), the SEIWG's mission is to coordinate and influence system architecture, technical design, and systems integration of all physical security equipment to be used within the DoD. SEIWG's strategy for addressing general and specific Service / Agency Physical Security Equipment (PSE) requirements includes:

- Providing DoDAF Architecture products/views
- Providing Interoperability Standards
- Sharing Information

SEIWG has four (4) main goals for establishing its Service/Agency approach to PSE:

- Provide DoD and its industry partners the means to achieve Physical Security Equipment interoperability
- Coordinate and influence system architecture, technical design, and systems integration of Physical Security Equipment to be used within DoD
- Develop Interoperability Standards to guide the Military services and their industry partners in development of Physical Security Equipment
- Ensure new systems integrate with existing systems and minimize architectural redesign

The SEIWG strives to accomplish a cohesive and collaborative environment. Not only are Joint DODAF Architecture Views developed, but the SEIWG provides a subject matter expert (SME) to tailor them for individual service programs. Not only are Joint ICDs produced, a SME is provided to aid in their implementation and to offer the tools to validate compliance. To ensure future DoD security systems for all four military services, the SEIWG shares with Services and Agencies: requirements, use cases, capabilities, ideas and lessons learned, and applies them as input to update and improve SEIWG products. 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. The benefits of such collaboration include:

- Save time and speed delivery to the warfighter
- Reduce duplicative Research, Development, Test & Environment (RDT&E) costs
- Reduce errors and increased lessons learned
- Increase interoperability
- Advance goal of "plug and play" solutions

Appendix E. Joint Requirements Working Group (JRWG)

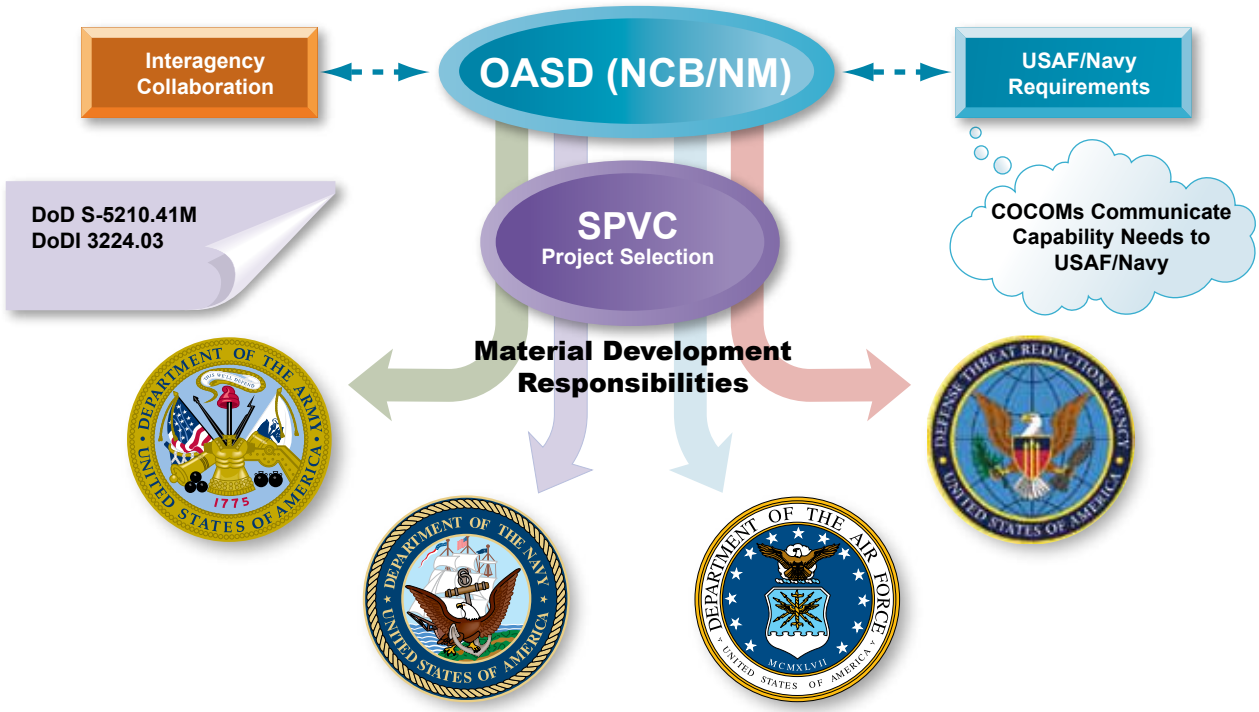
The Joint Requirements Working Group (JRWG) is an action officer-level working group responsible for the review and harmonization of all newly identified Department of Defense (DoD) Physical Security Equipment Action Group (PSEAG) projects. In addition, the JRWG may also perform other missions at the request of the PSEAG Chair. The JRWG Chairman 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
U.S. Army
U.S. Navy
U.S. Air Force
U.S. Marine Corps

Non-Voting / Advisory
Defense Threat Reduction Agency
U.S. Army Product Manager, Force Protection Systems
U.S. Army Military Police School
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
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 ongoing (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. 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 JRWG is 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 and other agencies; and d) seek a more active role in requirements from the U.S. Marine Corps.

The SPVC functions much like the Physical Security Equipment Action Group (PSEAG) in that it harmonizes nuclear physical security requirements submitted by the Air Force and the Navy. The SPVC 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, National Nuclear Security Administration, and the Nuclear Regulatory Commission. 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.



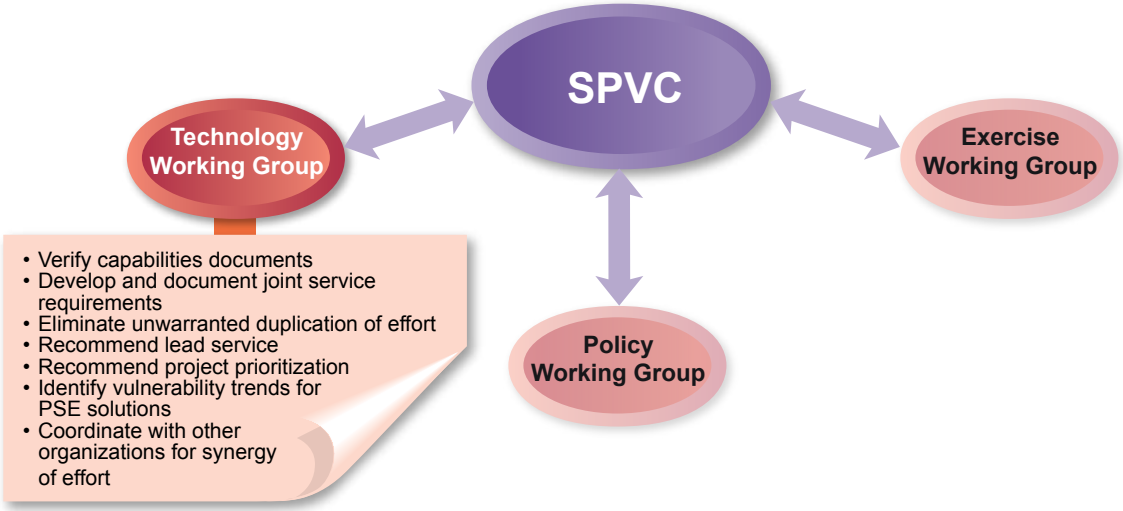
Working Groups

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

- **Policy Working Group** – reviews nuclear weapon security-related policy issues. The working group develops and recommends security policy modifications to the SPVC.

- **Technology Working Group** – 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 working group 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 Working Group**– 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 H. List of Acronyms

Acronym	Defenition
AA&E	Arms, Ammunition, and Explosives
AAR	After Action Report
ACSD	Advanced Container Security Device
AFB	Air Force Base
AFRL	Air Force Research Laboratory
AFSOC	Air Force Special Operations Command
ANGB	Air National Guard Base
ANSI	American Standards Institute
ARWG	Attack Resistance Working Group
ASA(ALT)	Assistant Secretary of the Army for Acquisition, Logistics and Technology
AT/FP	Anti-Terrorism/Force Protection
ATMR	Attack Tool & Material Resistance
BDOC	Base Defense Operations Center
BETTS-C	Base Expeditionary Targeting & Surveillance System - Combined
C2	Command and Control Display Equipment
CBRNE	Chemical, Biological, Radiation, Nuclear, Explosive
CCDE	Command and Control Display Equipment
CDD	Capability Development Document
CIRT	Controlled Impact Rescue Tool
CONUS	Continental United States
COP	Common Operating Picture
COTS	Commercial Off-The-Shelf

Acronym	Defenition
COTS Qual	Commercial-off-the-Shelf Equipment Qualification
CTF	Combined Test Force
DHS	Department of Homeland Security
DMS	Diminishing manufacturing sources
DoD	Department of Defense
DoE	Department of Energy
DT&E	Development Test and Evaluation
DTEDE	Desktop Explosive Detection Equipment
DTRA	Defense Threat Reduction Agency
EDE	Explosive Detection Equipment
ERDC	Engineer Research and Development Center
ESQD	Explosive Safety Quantity Distance
FLIR	Forward Looking Infrared (Camera)
FP	Force Protection
FPED	Force Protection Equipment Demonstration
FPS2	Force Protection Security Systems
FSD-ZBV	Forward Scatter Z-Backscatter Van
FUE	First Unit Equipped
FY	Fiscal Year
GaRDS	Gamma Ray Detection System
G-BOSS(E)	Ground Base Operational Security System (Expeditionary)
GCTS	Ground Combat Training Squadron
GIS	Geographic Information System

Acronym	Defenition
GPS	Global Positioning System
GSA	General Services Administration
HAL2TS	Hailing Acoustic Laser & Light Tactical System
HERO	Hazards of Electromagnetic Radiation to Ordnance
HHEDE	Handheld Explosive Detection Equipment
HVA	High Value Assets
IATO	Interim Authority to Operate
IBDSS	Integrated Base Defense Security System
ICD	Initial Capabilities Document
IDC2COP	Integrated Defense Command and Control Common Operating Picture
IDS	Intrusion Detection System
IED	Improvised explosive device
IFF	Identify Friend or Foe
IGSSR-C	Integrated Ground Security Surveillance Response- Capability
I-IBD	Interim Integrated Base Defense
IIMS	Installation Incident Management System
ILD	Internal Locking Device
IMS	Ion Mobility Spectrometry
IR	Information Retrieval
IUBIP	Integrated Unit, Base, Installation Protection
JDOC	Joint Defense Operations Center

Acronym	Defenition
JEFX	Joint Expeditionary Forces Experiment
JIGSAW	Joint Interface Group for Security Application Workspaces
JPEO	Joint Program Executive Office
JPMG	Joint Political Military Group
JUONS	Joint Urgent Operational Needs Statement
KRD	Kachemak Research Development
LAN	Local Area Network
LED	Light-emitting diode
LKMD	Lighting Kit, Motion Detector
MAJCOMs	Major Commands
MESF	Maritime Expeditionary Security Force
MIPs	Molecularly Imprinted Polymers
MUC	Mobile Unified Capabilities
MVEDEX	Mobile Vehicle Explosive Detection Equipment
NAR/FAR	Nuisance Alarm Rates and False Alarm Rates
NAVEODTECHDIV	Naval Explosive Ordnance Disposal Technical Division
NAVFAC	Naval Facilities Engineering Command
NDIA	National Defense Industrial Association
NECC	Naval Expeditionary Combat Command
NGWC	Next Generation Wireless Communications

Acronym	Defenition
NIE	Network Integration Evaluation
NSWCDD	Naval Surface Warfare Center, Dahlgren Division
NUWC	Naval Undersea Warfare Center
OCONUS	Outside the Continental United States
ONS	Operational Needs Statement
OPNAVINST	Office of the Chief of Naval Operations Instruction
PCC	Probability of Correct Classification
POR	Program of Record
PSEAG	Physical Security Equipment Action Group
QRC	Quick Response Checklist
QRF	Quick Reaction Force
R&D	Research and Development
R/SEDS	Remote/Standoff Explosive Detection System
RDT&E	Research, Development, Test and Evaluation
RFI	Request for Information
SA	Seismic-Acoustic
SaaS	Software as a Service
SC	Single Crystal
SEIWG	Security Equipment Integration Working Group
SIMs	Software Interface Modules
SLiMS	Shore-Line Monitoring Systems
SME	Subject-Matter-Expert

Acronym	Defenition
SOA	Service Oriented Architecture
SPO	System Program Office
SSN	Source's Sought Notice
STANAG	Standardization Agreement
STUAS	National Air Space Integration Demonstrator for Small Tactical UAS
TCP	Transmission Control Protocol
T-MMV	Trailer-Mounted Military Mobile VACIS
TRL	Technology Readiness Level
TSD-IMS	Temperature Step Desorption - Ion Mobility Spectrometry
TSS	Tactical Video Surveillance System
UAS	Unmanned Aerial (Air) Vehicle System
UC	Unified Capabilities
USAF	United States Air Force
USN	United States Navy
UVIS	AutoScan Under-Vehicle Inspection System
UWB	Ultra-Wide Band
VBIED	Vehicle Borne Improvised Explosive Device
VMD	Video Motion Detection