DEPARTMENT OF DEFENSE

PSEAG

PHYSICAL SECURITY ENTERPRISE & ANALYSIS GROUP

2018 PROGRAM SUMMARY

CONTENTS

INTRODUCTION

Physical Security Enterprise & Analysis Group Overview 1

Fiscal Year 2018 PSEAG Program Funding By Capability Area 2

PSEAG Centers of Excellence 3

Organization and Structure 4

PSEAG Successes 5

ACCESS CONTROL

Biometrically Enabled Access Control – Husbanding 8

Defense Installation Access Control 9

Gatekeeper on the Move-Biometrics 10

ANALYTICAL SUPPORT

Requirements Development 12

DECISION SUPPORT

Command and Control Enhanced Capability Suite 14

Flexible Fire Control System 15

Force Protection Cross Domain Solutions 16

Interoperability Bridge 17

Joint Interoperable Gateway for Security, Antiterrorism, and Warfighting — System Operations Audit & Recording 18

Joint Risk Decision Support Tool 19

Security Equipment Integration Working Group 20

Video Analytics Assessment 21

DETECTION & ASSESSMENT

Aerial Physical Security Assessment 23

Comparative Evaluation of Colorimetric Explosive Detection Systems 24

Enhancing Biosecurity Surveillance using Radio Frequency Identification Technology 25

Explosive Vapor Detection Test & Evaluation 26

Force Protection Pre-Shot Sniper Detection Capability 27

Foliage Penetration Wide-Area Surveillance 28

Harbor and Restricted Waterway Counter-UUV/AUV System 29

Indoor Gunshot Detection System 30

Joint Interoperable Gateway for Security, Antiterrorism, and Warfighting — Integration Testing 31

Linear Sensor System Development for Maritime Threats 32

Linear Sensor System for Multi-Threat Detection 33

Multi-Sensor Detection and Discrimination 34

Portable Intrusion Detection System 35

Raman Comparative 36

Trace Explosive Detection System Improvement 37

Wide Area Infrared System for Persistent Surveillance 2.0 38

INSTALLATION & TRANSPORT SECURITY

GunnAR for Waterside Security 40

Integrating MANTAS USV with NUTR COP 41

Joint Active Shooter Protection & Response 42

M2HB/M2A1 Weapon Sight 43

Navy Stabilized Crew-Served Heavy Machine Gun Mount 44

Tactical Radio Interface Console 45

Virtual Reality Synthetic Boat and Warning Shot Simulator 46

PREVENTION

Standoff Weapons Defeat Joint Integrated Product Team 48

STORAGE & SAFEGUARDS

APPENDICES

PSEAG New Seal 52

PSEAG Sharepoint Site 53

List of Acronyms 54

INTRODUCTION

PHYSICAL SECURITY ENTERPRISE & ANALYSIS GROUP OVERVIEW

The Physical Security Enterprise and Analysis Group (PSEAG), with history going back to December 1976, continues to address evolving threats facing Department of Defense personnel, their families, and critical infrastructure.

The physical security materiel solutions summarized in this document represent the culmination of identified requirements from the Combatant Commands and Services and coordinated with appropriate Office of the Secretary of Defense and Joint Staff organizations, as well as identified findings and recommendations reported by ongoing Department policy and security reviews. Before initiating each Research, Development, Test and Evaluation (RDT&E) investment, the projects are processed through a Joint Service review to ensure 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.

PSEAG PROGRAM CAPABILITY AREAS

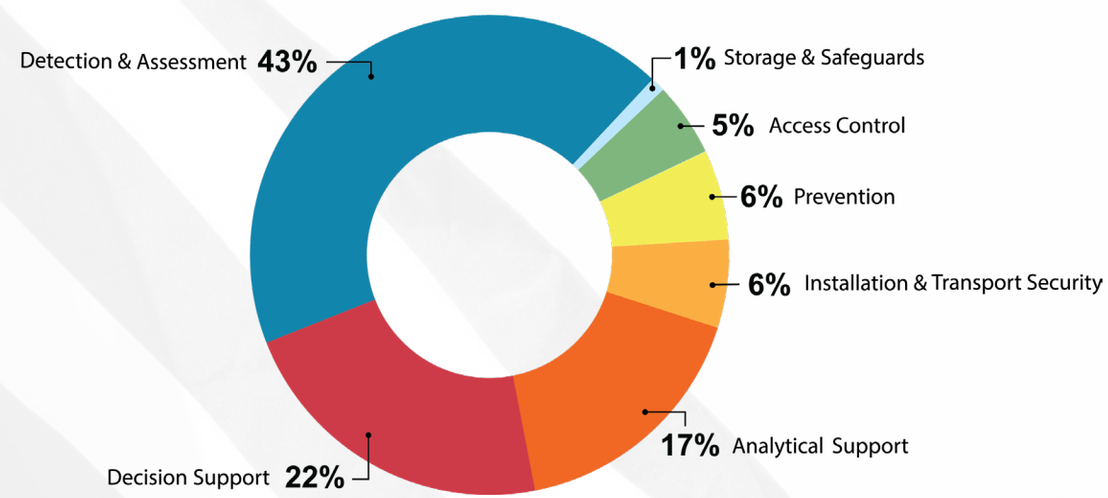
VISION

DoD's premier physical security RDT&E innovator for enterprise-level solutions to protect against asymmetrical, conventional, and weapons of mass destruction threats.

MISSION

Advance enterprise-level physical security RDT&E solutions to reduce risk created by current and emerging threats. Analyze, research, develop, demonstrate, and evaluate interoperable systems to transition capabilities to warfighters. Collaborate with DoD components, other government agencies, and the international community to prioritize and close capability gaps.

FISCAL YEAR 2018 PSEAG PROGRAM FUNDING BY CAPABILITY AREA ($40M)



PSEAG: CENTERS of EXCELLENCE

The PSEAG is composed of primary members from the Services with a complement of advisory personnel from the Joint Staff, other Office of Secretary of Defense staffs, the Defense Intelligence Agency, the Department of Energy, and other government 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)).

[ARMY]

- Tactical security equipment
- Lighting systems
- Personnel alerting systems
- Command and control systems
- Video assessment and recording (camera) systems
- Robotics
- Barriers

[USMC]

- Expeditionary physical security systems

[NAVY]

- Locks, safes, vaults, seals, containers, and delay systems
- Shipboard and waterfront security systems
- Anti-compromise evaluations
- Explosive detection systems

[USAF]

- Access control systems
- Active denial technology

PSEAG Policy (DoDI 3224.03)
- Minimize RDT&E duplication
- Ensure interoperability
- Ensure acquisition compliance

ORGANIZATION & STRUCTURE

EXECUTION ORGANIZATIONS**

DTRA Defense Threat Reduction Agency
NAVSEA NAVAL SEA SYSTEMS COMMAND
Sandia National Laboratories
Naval Information Warfare Center
AFRL
NAVFAC
Lawrence Livermore National Laboratory

* Primary Members: GS15–level representatives responsible for project oversight/execution. Ad hoc working groups as needed.
** Partial Listing

PSEAG SUCCESSES

In 2018, the PSEAG invested in access control by enhancing the Identity Matching Engine for Security & Analysis capability to compare cardholders against additional person files at the National Crime Information Center and the Interstate Identification Index. This project will enhance an already powerful tool to protect people and resources.

To address an active shooter scenario, the PSEAG invested in an Indoor Gunshot Detection System (IGDS) test and evaluation effort. Using commercial off-the-shelf technology, the PSEAG tested the applicability of an IGDS within DoD facilities, with a focus on common office work environments such as work spaces containing many office cubicles. Testing proved that an IGDS can help pinpoint the location of an active shooter event.

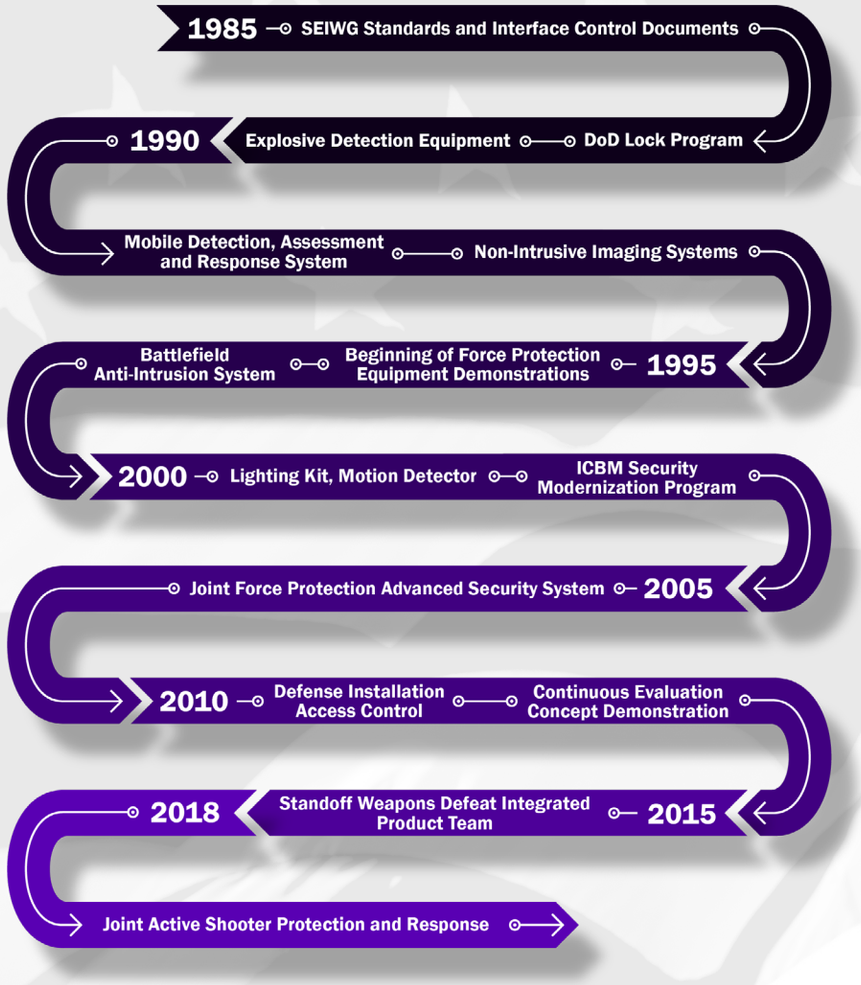
Explosive Detection Equipment testing and evaluation (T&E) remains an important part of the PSEAG's overall portfolio. In 2018, the focus turned to comparing new commercial off-the-shelf (COTS) colorimetric kits capable of explosives and precursor detection. The results of the T&E will help users better understand the capabilities of the kits prior to purchasing. The PSEAG also sponsored a project to determine the suitability of COTS vapor detection systems for real-world applications and to provide a baseline for testing of future vapor detection systems. Testing revealed this technology needs to mature to be effective.

Virtual and augmented reality are powerful tools to help the warfighter. The PSEAG invested in testing and evaluating a capability that allows for effective visual communication between the waterside security officer and the security personnel manning defensive gun positions using augmented reality. The capability also includes a virtual reality training system that replicates the entire waterside security environment so that it can be used for training within virtually any available space or schoolhouse environment.

The PSEAG and the Army's Product Manager Biometrics partnered to provide a contactless, multi-modal biometrics (fingerprint, face, and iris), forensics, and threat detection system fully integrated into and interoperable with the entry control point for the warfighter. The technology is being tested in an operational environment with very promising results.

Wide area threat detection for force protection is another area where the PSEAG is investing time and resources. This effort focused on the development of a 360-degree horizontal, 100-degree vertical wide area detection sensor with configurable keep-out zones to enhance overall situational awareness. Additionally, the sensor will provide an ideal base layer for fusion with other sensor modalities and can enable false alarm reduction compared to existing sensors.

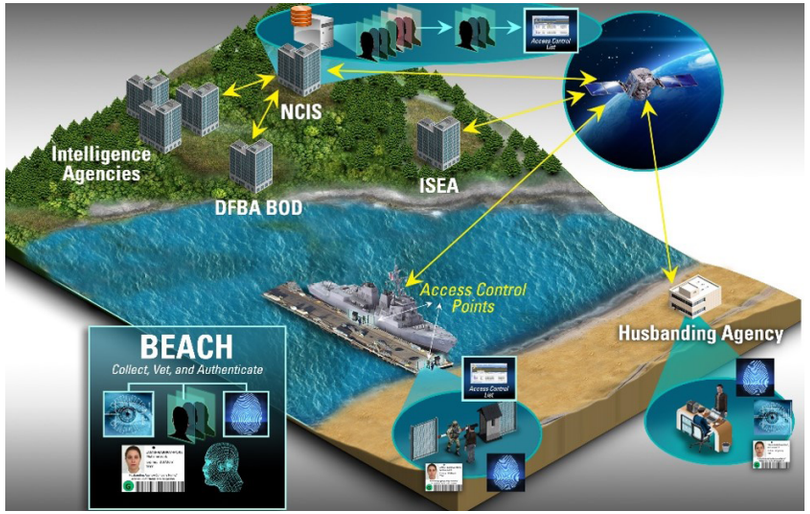
The PSEAG continues to successfully transition capability to the warfighter. Since its inception, the PSEAG has influenced over $2B in technology solutions for the Combatant Commanders and the Military Services. As examples, the PSEAG developed industry standards for physical security equipment interoperability, helped establish the DoD Lock and Joint Explosive Detection Equipment Programs, and assisted the Air Force develop a Remote Visual Assessment capability that is deployed at 450 remote launch facilities securing our Nation's Intercontinental Ballistic Missile fleet.



ACCESS CONTROL

Controlling access to safeguard personnel and their families and preventing unauthorized access to critical infrastructure and materials is paramount. This capability area focuses on programs and processes related to the validity and verification of individuals entering into or already within a facility.

BIOMETRICALLY ENABLED ACCESS CONTROL – HUSBANDING



REQUIREMENTS

— National Security Presidential Directive (NSPD)-41/ Homeland Security Presidential Directive (HSPD)-13

— NSPD-59/HSPD-24

Biometrically Enabled Access Control - Husbanding provides a capability that will collect, store, and share biometric data with United States Government biometric databases for vetting and badging of individuals seeking access to U.S. assets. Husbanding involves managing the logistic affairs of a ship while in port, including such tasks as customs, fueling, supplies, repairs and any requirements of the crew. This effort also integrates the biometric capabilities of the Identity Dominance System with husbanding operations to verify the identity of individuals on the approved access list.

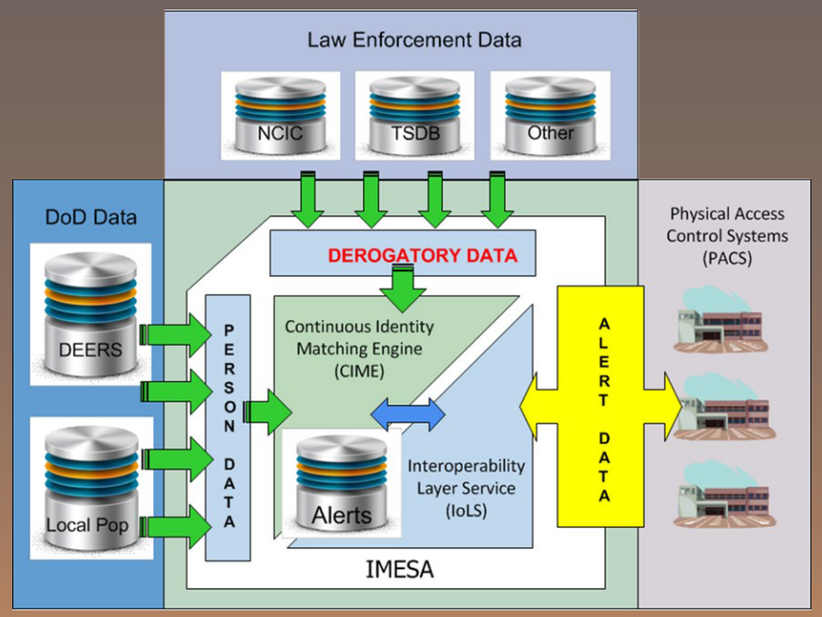
DEFENSE INSTALLATION ACCESS CONTROL

REQUIREMENTS

— National Defense Authorization Act for Fiscal Year 2016

— National Defense Authorization Act for Fiscal Year 2017

The Defense Installation Access Control project is a continuation of the PSEAG-funded project for the Identity Matching Engine for Security & Analysis (IMESA). The previous effort developed an underlying matching engine that compares DoD registered cardholders against the FBI's Wanted Persons File and against the Terrorist Screening Database. In 2018, Congress tasked DoD to plan for the expansion of IMESA, to include additional sources of derogatory information. The current project responds to the tasking to enhance the matching engine to compare cardholders against additional person files at the National Crime Information Center and the Interstate Identification Index databases. Additionally, this effort will improve the reporting capabilities of the matching engine by providing finer-grained accounting of the results.



GATEKEEPER ON THE MOVE – BIOMETRICS

REQUIREMENTS

— Joint Urgent Operational Needs Statement 0548

Gatekeeper on the Move - Biometrics (GOTM-B) is a contactless, multi-modal biometrics (fingerprint, face, and iris), forensics, and threat detection system fully integrated into and interoperable with the Entry Control Point (ECP). GOTM-B will be capable of near real-time identification and matching of personnel entering/ exiting the ECP with high accuracy, and will provide critical identity intelligence/ threat Information to decision makers generated from the transaction manager/fusion engine. GOTM-B was developed in partnership with the National Institute of Standards and Technology, Project Manager Terrestrial Sensors, and U.S. Central Command, GOTM-B will be an "open system" architecture based, government owned system, and "cooperative effort."

ANALYTICAL SUPPORT

Properly securing critical assets to prevent access by unauthorized persons and implementing control measures that ensure access is limited to authorized persons is the foundation of physical security. This capability area addresses equipment (e.g., locks, doors, etc.) designed to delay or stop unauthorized entry/access to a specified area.

REQUIREMENTS DEVELOPMENT

The Headquarters Department of the Army Office of the Provost Marshal General and the Army Physical Security Enterprise and Analysis Group facilitated the rapid advancement of technology through the Army Business Initiative and Defense Business System processes to produce requirements necessary to field emerging technology more efficiently. The development and implementation of these requirements will identify clear paths of transition and funding for needed systems to fill an enterprise capability gap and further secure Army and DoD installations.

DECISION SUPPORT

Decision support systems serve the management, operations, and planning levels of the DoD physical security enterprise to help make decisions, which may be rapidly changing with little advanced warning. This capability area focuses on command and control equipment and projects related to the creation and enhancement of common operating pictures and the establishment of common architectures and interface standards.

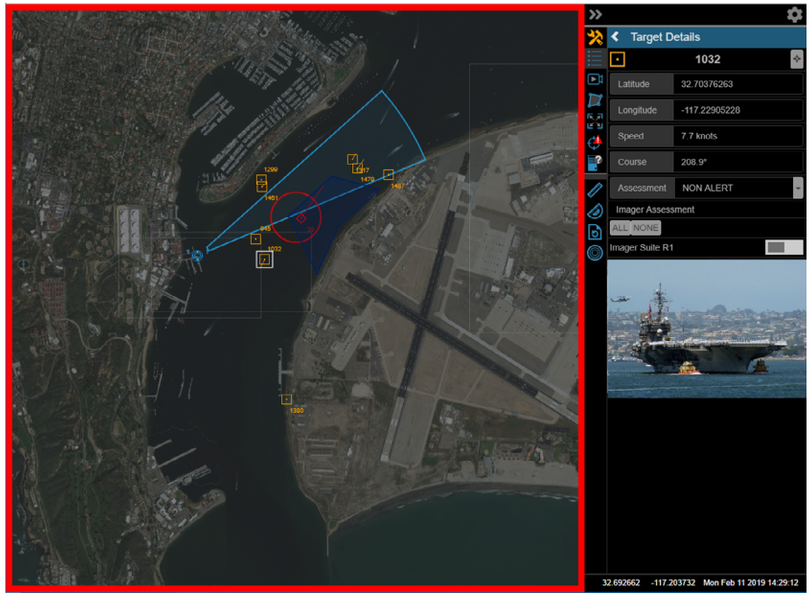
COMMAND AND CONTROL ENHANCED CAPABILITY SUITE

REQUIREMENTS

— DoD Manual S-5210.41, "(U) Nuclear Weapon Security Manual: The DoD Nuclear Weapon Security Program"

— Naval Facilities Engineering Command letter dated 27 February 2012, Electronic Harbor Security System Follow-on Test and Evaluation OT-IIIB

The Command and Control (C2) Enhanced Capability Suite draws upon lessons learned from evaluating other Physical Security Information Management Systems including the Joint Interoperable Gateway for Security, Antiterrorism, and Warfighting, Near-shore Unified Tactical Response, Cameleon 360 Surveillance, and the Electronic Harbor Security System Command, Control, and Communication and Display. Current efforts extend the capabilities of the C2 Enhanced Capability Suite project by supporting Joint Task Force, Naval Base Guantanamo Bay, Cuba, requirements.



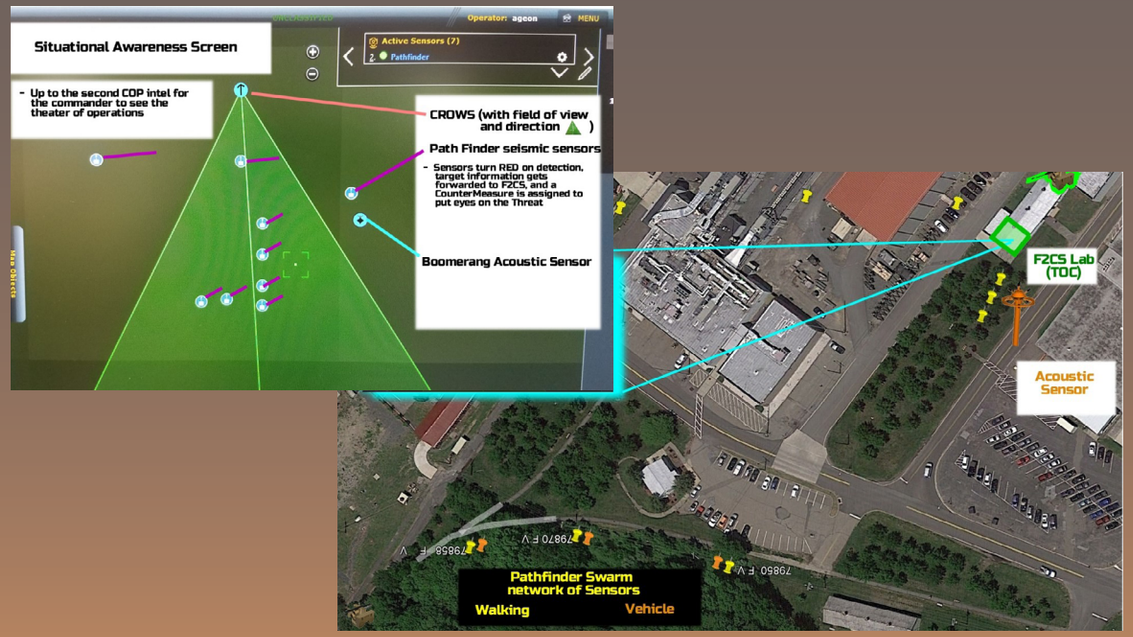
FLEXIBLE FIRE CONTROL SYSTEM

REQUIREMENTS

— Integrated Base Defense Security System Capability Development Document

— Base Defense and Response System Capability Development Document

The Flexible Fire Control System (F2CS) is a base defense and response system used to network various sensors and weapons, such as the Common Remotely Operated Weapon Station, for the protection of installations. The F2CS is designed to work between sensors and weapon systems to provide networking capability to the Army and other Services, which will serve as an added capability to the Army's existing Integrated Sensor Architecture. F2CS is capable of monitoring all of the system state messages and subscriptions that external systems are capable of handling, including: heartbeats, register requests, faults, acknowledgements, homing and angular positions, and threat messages.



FORCE PROTECTION CROSS DOMAIN SOLUTION

REQUIREMENTS

— Integrated Ground Security, Surveillance and Response -Capability (IGSSR-C), Capability Development Document (CDD), April 2013

— Tactical Security System, CDD, November 2014

— Ground-Based Operational Surveillance System (Expeditionary) CDD, May 2014

The Cross Domain Solution (CDS) initiative was established to enable command and control systems managing unclassified sensors to provide a common operating picture to combatant commanders from multiple sensors outside of the current accreditation boundaries. The CDS efforts will enable current disparate systems to share cursor-on-target messaging and full motion video across multiple enclaves in different security domains. Product Manager Force Protection Systems fully anticipates multiple services and Program Executive Officers to gain increased information sharing from this initiative.

INTEROPERABILITY BRIDGE

The Interoperability Bridge project will demonstrate the ability to connect different physical security equipment systems developed using different interoperability standards. The Security Equipment Integration Working Group (SEIWG) and a U.S. Army Program Office provided the support necessary to research, develop, and test an interoperability bridge for the SEIWG and the Integrated Sensor Architecture (ISA) based data models. The team used a phased approach and included development, testing, and demonstrations leveraging the existing interoperability standard and existing standard content, guidance, and tools. The PSEAG continues to promote the widest use of existing sensor solutions with a goal of not requiring the manufacturers or product team to re-develop their sensor product and/or command & control display equipment platform to support differing interface standards.

REQUIREMENTS

— Integrated Ground Security, Surveillance and Response -Capability (IGSSR-C), Capability Development Document (CDD), April 2013

— Tactical Security System, CDD, November 2014

— In addition, these CDDs have identified Human Systems Integration requirements to minimize workload and enhance mission performance

JOINT INTEROPERABLE GATEWAY FOR SECURITY, ANTITERRORISM, AND WARFIGHTING — SYSTEM OPERATIONS AUDIT & RECORDING

The Joint Interoperable Gateway for Security, Antiterrorism and Warfighting (JIGSAW) System Operations Audit & Recording (SOAR) project will provide an auditing, training, and forensic evidence capability for the JIGSAW platform. JIGSAW SOAR is an invaluable tool for system operators and stakeholders to rapidly reconstruct incidents, eliminating virtually all questions or uncertainties associated with human interpretation and reporting surrounding system operator activities and actions while providing critical auditing and forensic evidence. Additionally, any incident that is deemed to be of value in terms of lessons learned may be rapidly replayed, analyzed, and assessed to provide a defense in-depth capability that feeds the engineering life-cycle improvement process, concept of operations and tactics, techniques, and procedures to significantly benefit the training and exercise missions.

REQUIREMENTS

— DoD Instruction 3224.03, "Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E)"

— DOD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L))"

— DOD Directive 5000.1, "The Defense Acquisition System"

— DOD Manual 5200.08-R, "Physical Security Program"

— SEIWG 0101 series Interoperability Standard

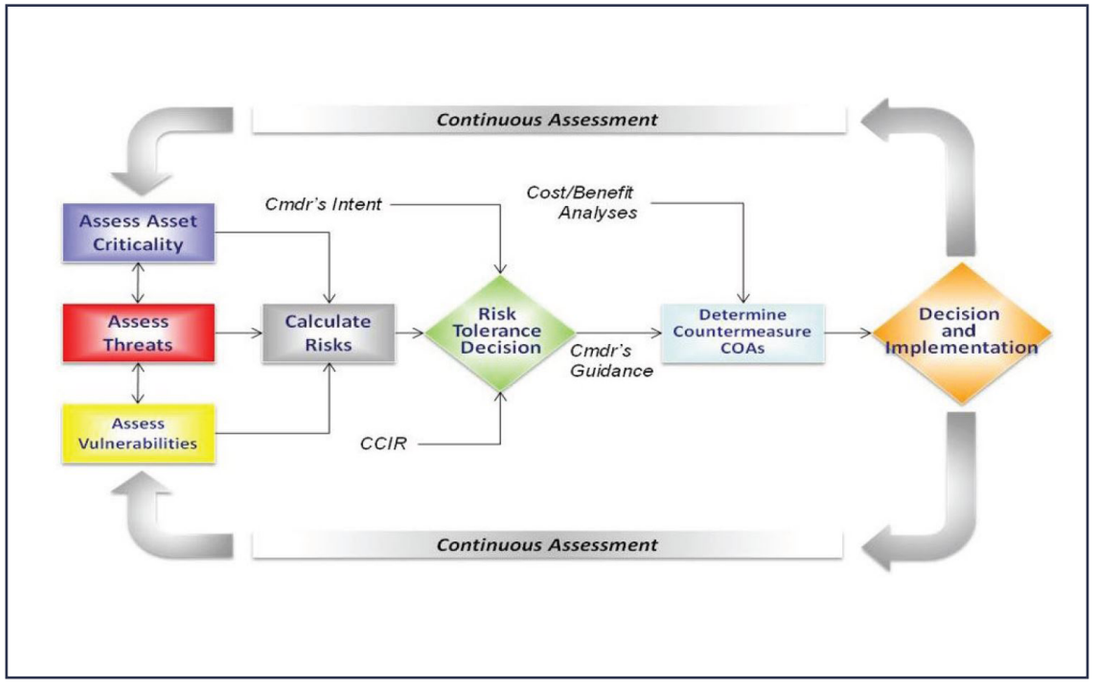
JOINT RISK DECISION SUPPORT TOOL

REQUIREMENTS

—2015 DoD Mission Assurance Assessment Benchmarks

—DoD Mission Assurance Strategy, May 2012

The Joint Risk Decision Support Tool effort developed an enterprise installation decision support application providing risk analysis and risk mitigation in a secure, web-enabled architecture to be hosted on one of DoD's classified networks. Adapting the capabilities of the Air Force and Army's ForcePRO software tool, this new application supports all services. This tool is a standardized Service and Major Command roll-up for expanded visibility of the risk picture and will enable more fiscally-efficient procurement of necessary resources.



SECURITY EQUIPMENT INTEGRATION WORKING GROUP

The Security Equipment Integration Working Group (SEIWG) is tasked to support Defense Security Enterprise efforts to achieve integrated physical security systems. To do this, the SEIWG develops interface standards between physical security equipment (PSE) so that these items may be assembled into seamlessly-integrated physical security systems, and establishes concepts for follow-on integrated PSE so that it is unconstrained by present PSE developments.

In 2015, the SEIWG commenced efforts to align the SEIWG Interoperability Standard with National Information Exchange Model (NIEM); this effort was completed in 2017. In 2018, the SEIWG won the "Best of NIEM" award for its Information Exchange Package Documentation. The SEIWG's work to encourage interoperability has had tremendous effects on the NIEM community, including the NIEM Military Operations (MilOps) domain content.

REQUIREMENTS

— DoD Instruction 3224.03, "Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E)"

— DoD Instruction 8320.07, "Implementing the Sharing of Data, Information Technology (IT) Services in the Department of Defense"

VIDEO ANALYTICS ASSESSMENT

REQUIREMENTS

— Integrated Ground Security, Surveillance and Response -Capability (IGSSR-C), Capability Development Document (CDD), April 2013

— Tactical Security System, CDD, November 2014

— In addition, these CDDs have identified Human Systems Integration requirements to minimize workload and enhance mission performance

Video Analytics (VA) is the capability to automatically analyze video to detect and determine temporal and spatial events. VA ultimately reduces the workload of an operator for a system that is video monitoring intense. Current Army force protection systems are heavily dependent on video sensors requiring 24 hour/7 days per week monitoring by personnel. System operators are required to detect and classify personnel and vehicles on numerous video sensors substantially increasing operator workload substantially. Software detects and classifies personnel and vehicles, while providing information related to the events occurring in real time. Effective video analytics can significantly reduce operator workload and provide a new, cost effective detection sensor capability.

DETECTION & ASSESSMENT

The ability to detect an adversary and assess their intentions is a basic physical security tenet. This capability area addresses the design of equipment to identify and warn of unauthorized access to a specified area or installation as well as equipment related to the notification and identification of explosive threats or hazards.

AERIAL PHYSICAL SECURITY ASSESSMENT

REQUIREMENTS

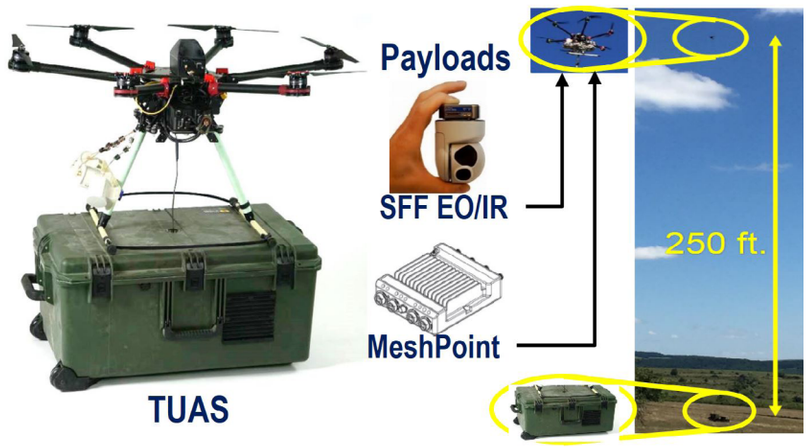
— DoD Instruction 3224.03, "Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E)"

— DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, 1. Technology, and Logistics (USD (AT&L))"

— DoD Directive 5000.1, "The Defense Acquisition System"

— DoD Manual 5200.08-R, "Physical Security Program"

The Naval Information Warfare Systems Command (formerly Space and Naval Warfare Systems Center Atlantic) assessed and demonstrated the application of small unmanned aerial systems in performing aerial physical security of intrusions in remote areas such as perimeters and enclaves. These areas are protected by an intrusion detection system, but are not equipped with co-located physical security assessment capabilities (e.g. electro-optical/infrared equipment).

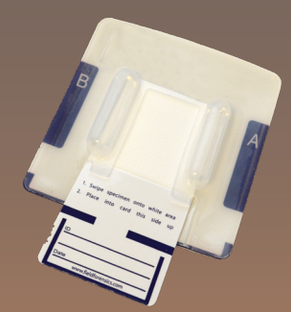


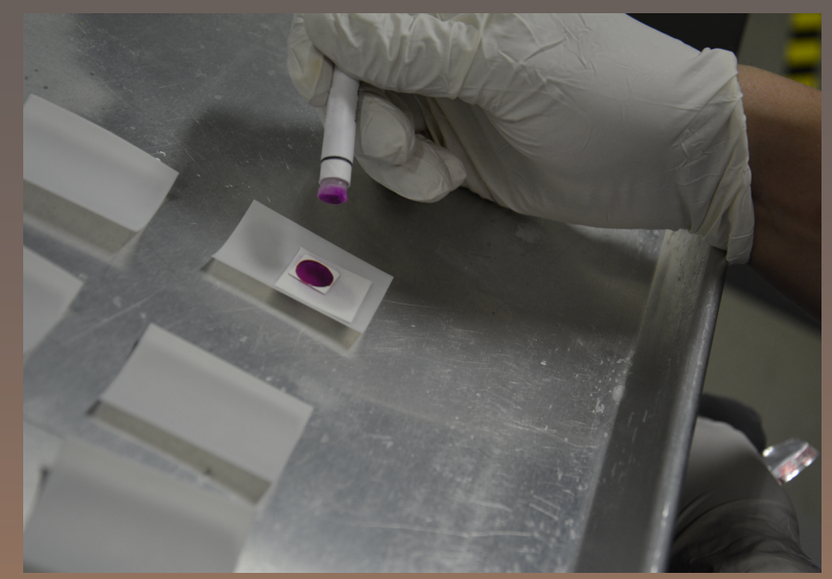
COMPARATIVE EVALUATION OF COLORIMETRIC EXPLOSIVE DETECTION SYSTEMS

REQUIREMENTS

— PSEAG Capability Gap 6

The Explosive Detection Equipment Program at the Naval Surface Warfare Center, Indian Head Explosive Ordnance Technology Division, will survey the capabilities of commercially available colorimetric detection systems for the purposes of explosive and precursor detection. Based on market research, systems will be selected for inclusion in the evaluation. The evaluation will include test series that assess the detection capability (bulk vs. trace), overall consistency, and false alarm rates for each of the systems. The final report will assist the warfighter in identifying the capabilities of these systems and their applicability to field use.





ENHANCING BIOSECURITY SURVEILLANCE USING RADIO FREQUENCY IDENTIFICATION TECHNOLOGY

REQUIREMENTS

— Inventory and accountability requirements 42 Code of Federal Regulations (CFR) Part 73, 9 CFR Part 121, 7 CFR Part 331

— DoD Instruction 5210.88, "Security Standards for Safeguarding Biological Select Agents and Toxins"

In an ongoing effort to enhance biosecurity surveillance of Biological Select Agents and Toxins (BSAT), the study evaluated the application of Radio Frequency Identification (RFID) technology to detect RFID-labeled samples concealed in shipping containers exiting through the entry control point without having to open the containers. The study demonstrated that RFID technology is capable of providing longer reading distance thus reducing time to inventory, and automatically detects RFID labeled samples concealed in various types of shipping containers. Implementing this technology will reduce the reliance on paper-based information, prevent erroneous or deliberate loss of BSAT, and eliminate the safety and security risks. Security personnel will be able to scan or receive alerts when the shipping box or BSAT sample is being transported to and through the exit control point, thus enhancing security surveillance.

EXPLOSIVE VAPOR DETECTION TEST & EVALUATION

REQUIREMENTS

— PSEAG Capability Gap 6

The Explosive Detection Equipment Program conducted a small, qualitative-type vapor test several years ago and determined systems were unable to detect the vapor samples being produced. The objective of this effort was to conduct a more rigorous vapor study for commercial off-the-shelf (COTS) systems. The test determined the detection capabilities of the systems using a quantifiable source of vapor (the NRL TESTBed) and will provide a baseline for future testing of vapor detection systems.

FORCE PROTECTION PRE-SHOT SNIPER DETECTION CAPABILITY

REQUIREMENTS

— Ground-Based Operational Surveillance System (Expeditionary) Capability Development Document, May 2014

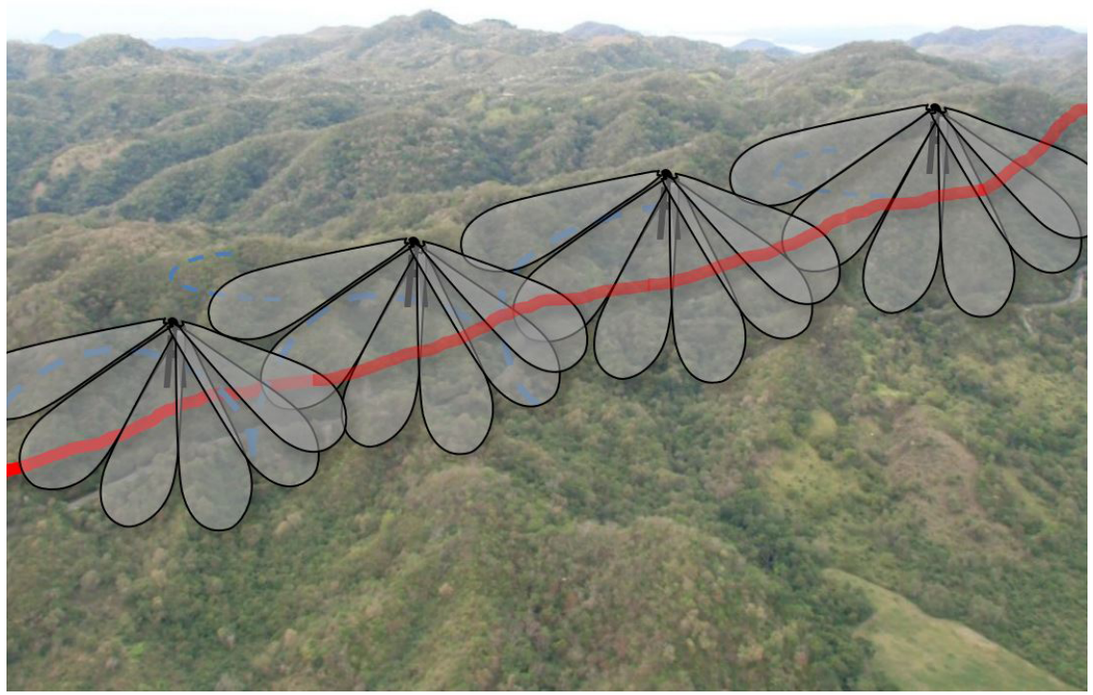
The Force Protection Pre-Shot Sniper Detection sensor provides a sniper detection capability via multi-modal detection processing including: glint, shape, and change detection. The mapping capabilities and glint detection will allow the sensor to identify potential threats indicative of sniper activity.

FOLIAGE PENETRATION WIDE-AREA SURVEILLANCE

REQUIREMENTS

— DoD Manual S-5210.41, "(U) Nuclear Weapon Security Manual: The DoD Nuclear Weapon Security Program"

The Foliage Penetration Area Surveillance program evaluated technologies that have the capability to detect, classify and track human activity in areas concealed by foliage. A market survey of industry was conducted and has determined that there are currently multiple vendors that have candidate prototype radars at the appropriate technical readiness level. The US Army has determined that several contractors have potential systems that could meet a portion of the Navy's requirements. These components have been integrated in the laboratory and have been tested in environments with characteristics similar to those expected at Navy's operational sites.

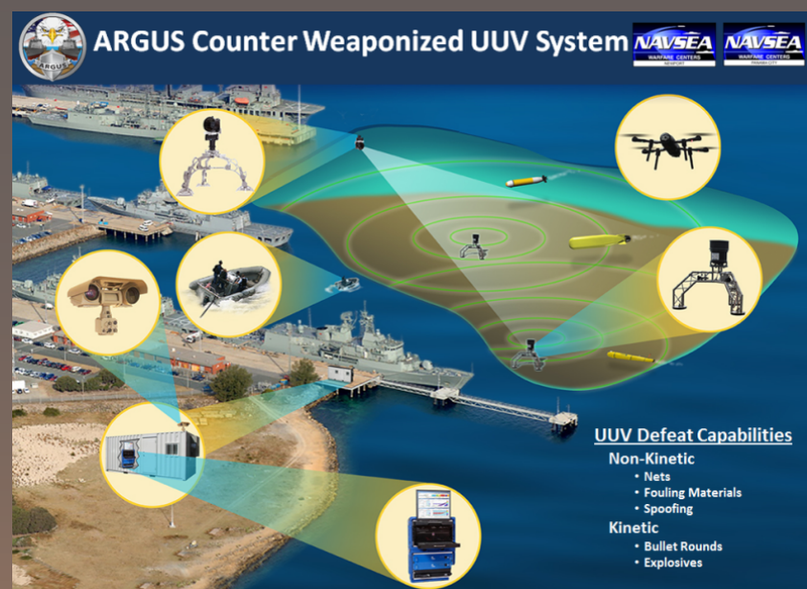


HARBOR AND RESTRICTED WATERWAY COUNTER-UUV/AUV SYSTEM

REQUIREMENTS

- United States Pacific Command Requirements for Counter-UUV
- Fleet Forces Command Requirements
- Army Physical Security Capability Gaps
- Army Interoperability / Integration Key Performance Parameters of IGSSR-C Capability Development Document

The Harbor and Restricted Waterway Counter-Unmanned Underwater Vehicle (UUV) / Autonomous Underwater Vehicle (AUV) System project provided a detect-to-defeat capability against small and mid-sized UUV threats in a harbor and restricted waterway environment. The project consisted of the capability to detect, track, alert, and respond with a defeat capability prior to the threat accomplishing its mission.

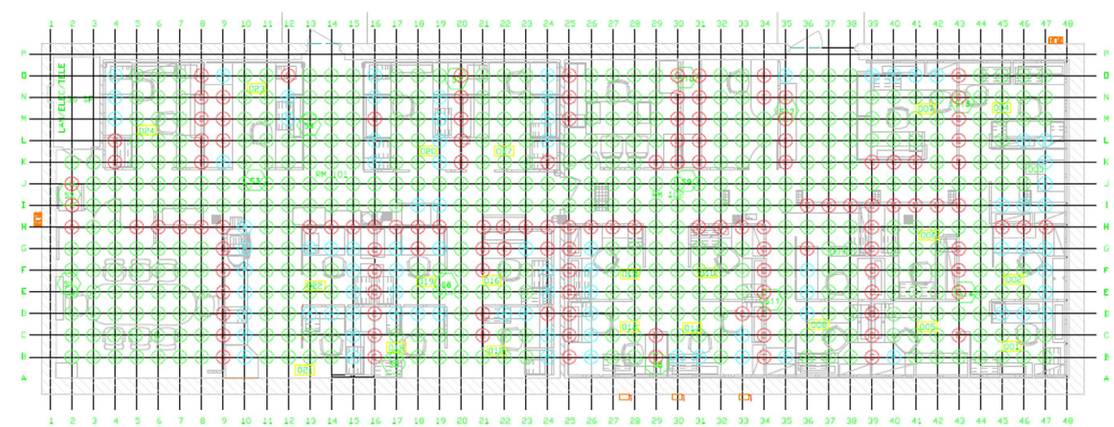


INDOOR GUNSHOT DETECTION SYSTEM

REQUIREMENTS

- DoD Directive 5000.01, "The Defense Acquisition System"
- DoD Instruction 3224.03, "Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E)"
- DoDI 5200.08-R, "Physical Security Program"
- DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L))"

The Indoor Gunshot Detection System (IGDS) project conducted test and evaluation of a commercial off-the-shelf sensors in applications within DoD facilities (i.e. indoors), with a focus on common DoD office space environments such as facility work spaces containing many cubicles. The project deliverable included a baseline guide for the DoD's use in planning, designing, and/or implementing IGDS. While this project focused on the materiel and facility aspects of IGDS, the project's results offer insight on the impact to tactics, techniques, and procedures resulting from the employment of IGDS and a determination if IGDS is a tangible materiel solution.



JOINT INTEROPERABLE GATEWAY FOR SECURITY, ANTITERRORISM, AND WARFIGHTING — INTEGRATION TESTING

The Joint Interoperable Gateway for Security, Antiterrorism, and Warfighting (JIGSAW) Integration Testing effort will determine if JIGSAW (a U.S. Marine Corps physical security command and control system) can perform with the U.S. Air Force Tactical Automated Security System components. JIGSAW will assist in providing real-time control and sensor status for physical security operators. The results of the Technical Evaluation will support a decision to go into Integrated Testing.

REQUIREMENTS

— Integrated Base Defense Security System Capability Development Document

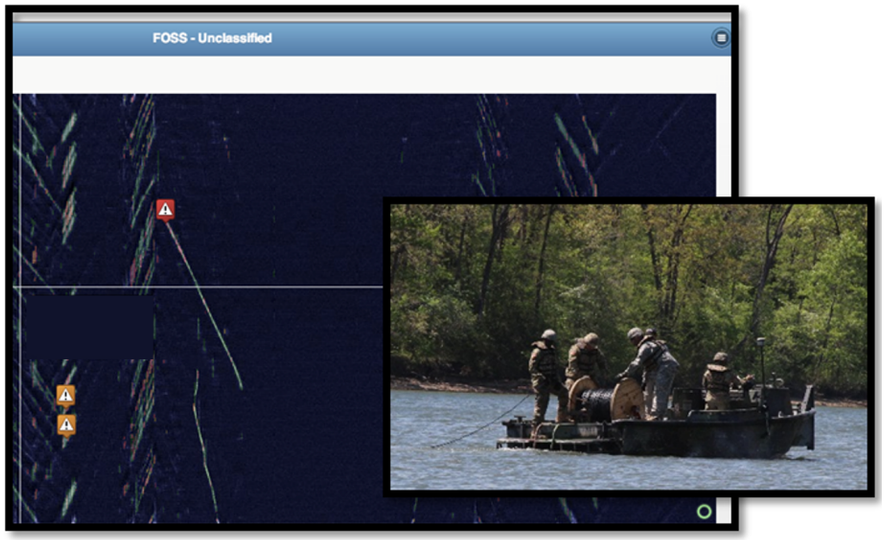
LINEAR SENSOR SYSTEM DEVELOPMENT FOR MARITIME THREATS

REQUIREMENTS

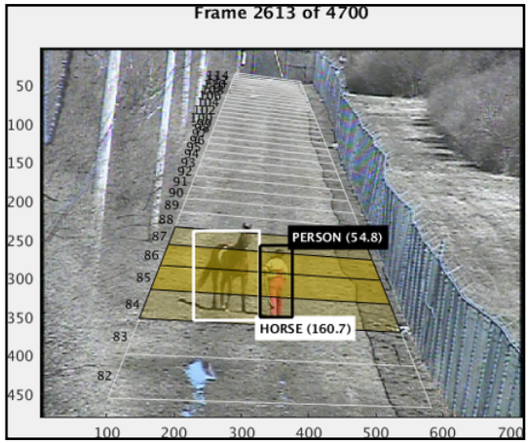
— Addresses technology gaps in force protection and physical security for U.S. Indo-Pacific Command and U.S. Special Operations Command.

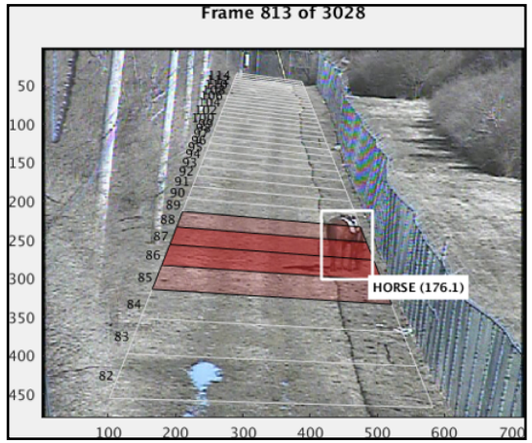
— Commander, Navy Installations Command (CNIC) Instruction 5530.14, "CNIC Ashore Protection Program"

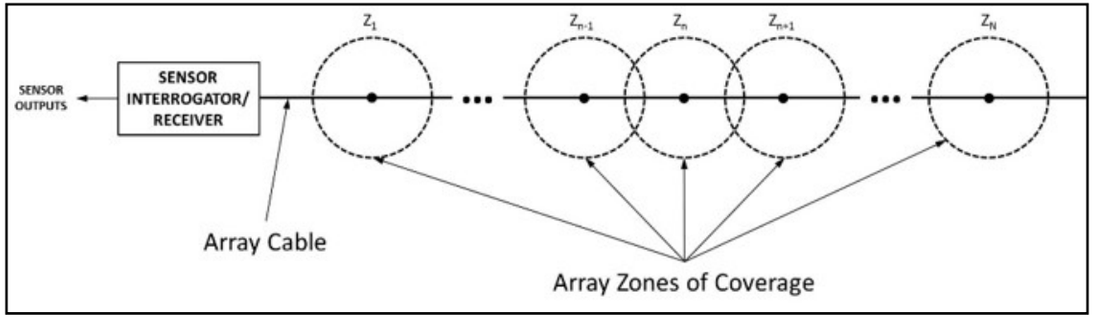
The Linear Sensor System (LSS) is a seismic sensor array that combines different systems within a single umbrella sensor system. The existing LSS will be augmented to detect and localize maritime threats. This includes development, tuning, implementation, and testing of narrowband signature discrimination capabilities for threats of interest for physical security of assets with land-water interfaces.



LINEAR SENSOR SYSTEM FOR MULTI-THREAT DETECTION







REQUIREMENTS

— Joint Urgent Operational Needs Statement United States Central Command - 0046

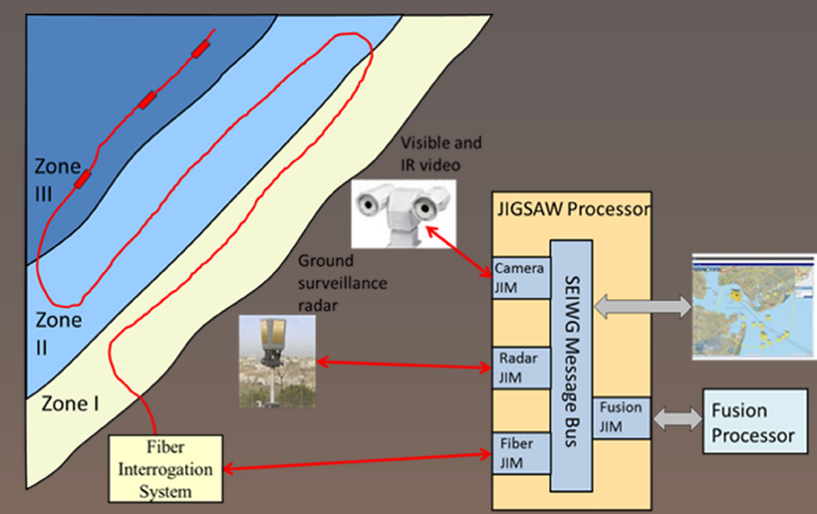
The Linear Sensor System (LSS) is a seismic sensor array that has the combined capabilities of the Border Tunneling Activity Detection System-Linear, Interceptor, Thunderware, and Glasswave systems within a single umbrella system. The proposed effort will enhance the performance of LSS for existing applications and augment the system for new application areas.

MULTI-SENSOR DETECTION AND DISCRIMINATION

REQUIREMENTS

— DoD Manual S-5210.41, "(U) Nuclear Weapon Security Manual: The DoD Nuclear Weapon Security Program"

The Multi-sensor Detection and Discrimination (MSDD) effort is a scalable multi-sensor wide area surveillance system deployed at the land-water interface for autonomous detection and discrimination of asymmetric threats. MSDD provides consistent threat detection and accurate threat assessment at the land/water interface.



PORTABLE INTRUSION DETECTION SYSTEM

REQUIREMENTS

— DoD Manual S-5210.41, "(U) Nuclear Weapon Security Manual: The DoD Nuclear Weapon Security Program"

— Integrated Base Defense Security System Capability Development Document

The Portable Intrusion Detection System (PIDS) project will develop a temporary system that can be deployed, set up, configured, and operational within a short time frame. The PIDS system will detect intrusions at the perimeter, provide location data (e.g. sector or zone) of intrusions along the perimeter, annunciate the alarms and the location to security forces, and provide a means of assessment of all alarms. PIDS will be scalable for varying perimeter sizes, environments, and locations, and will be capable of being transported rapidly to locations that require temporary perimeter detection.

RAMAN COMPARATIVE

REQUIREMENTS

— PSEAG Capability Gap 6

A number of Raman systems have joined the market and/or have been updated since the last comparative Raman evaluation completed by the Explosive Detection Equipment Program in 2016. The objective of this effort is to complete a comparative assessment of handheld Raman systems capable of detecting explosives and their precursors. The evaluation will include test series that assess the bulk identification capability and overall consistency for each of the systems. The final report will assist the warfighters in identifying capabilities and their applicability to use in the field.

TRACE EXPLOSIVE DETECTION SYSTEM IMPROVEMENT

REQUIREMENTS

— PSEAG Capability Gap 6

The Trace Explosive Detection System project will improve trace explosive detection systems to provide an enhanced solution and increase government competition for trace explosive detection capabilities. The systems will provide detection of energetic threats in a design that is more rugged, easier to operate, and easier to maintain. The primary objective of this effort is to develop up to two of the systems that have previously demonstrated effective detection but had deficiencies in either operation or design that hinder the ability to provide the optimal solution for trace explosive detection.

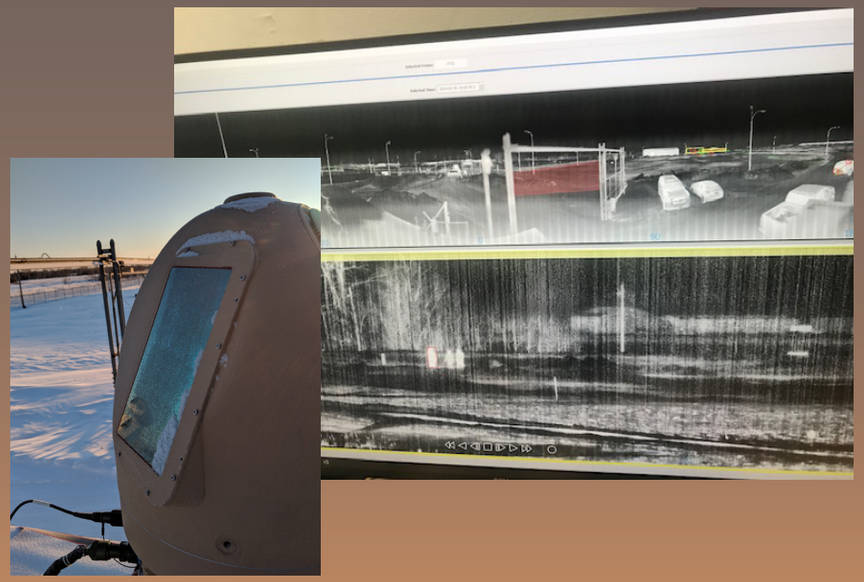
WIDE AREA INFRARED SYSTEM FOR PERSISTENT SURVEILLANCE 2.0

REQUIREMENTS

— Integrated Base Defense Security System Capability Development Document

The Wide Area Infrared System for Persistent (WISP) Surveillance project is a long-wave infrared system that was developed and successfully delivered to theater for forward operating base (FOB) protection on Persistent Ground Surveillance Towers. The deployed WISP 1.0 systems provide day/night (24/7/365) situational awareness and force protection for FOBs in harsh environments by providing persistent 360 degree motion imagery over a 20 degree vertical field of view. Advanced processing algorithms automatically adapt continuously to the scene and detect the presence of moving objects in the surroundings using only the passive infrared imagery.

The WISP 2.0 sensor will perform as a 360 degree horizontal, 110 degree vertical wide area detection sensor with configurable keep-out zones and upgraded overall situational awareness. Additionally, it will provide an ideal base layer for fusion with other sensor modalities and can enable false alarm reduction. The WISP 2.0 augments (or replaces, if resolution requirements allow) existing thermal imagers.



INSTALLATION & TRANSPORT SECURITY

Robust installation and transport security are vital to preventing a weapon of mass destruction attack or the unauthorized access to key assets such as nuclear weapons and special nuclear material. This capability area focuses on programs and equipment intended to improve the physical security profile of fixed sites, facilities, and critical items while in transit.

GUNNAR FOR WATERSIDE SECURITY

REQUIREMENTS

— US Fleet Forces Command Requirements

— Antiterrorism/ Force Protection Integrated Priority Capability List

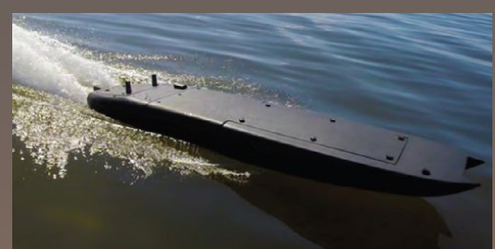
The Gunnery System with Augmented Reality (GunnAR) capability allows the antiterrorism tactical watch officer (ATTWO) or gunner's liaison officer to send visual firing commands via a command & control tablet to the Gunner's Augmented Reality Heads Up Display (AR HUD). The AR HUD also transmits video to the ATTWO along with data on where the gunner is looking and where the gun is pointing, which provides improved situational awareness to the ATTWO. The GunnAR for Waterside Security System also includes a virtual reality training system that replicates the entire AR HUD and command & control tablet functionality. The AR HUD also transmits video to the ATTWO along with data on where the gunner is looking and where the gun is pointing, which provides improved situational awareness to the ATTWO.

INTEGRATING MANTAS USV WITH NUTR COP

REQUIREMENTS

— Requirements for this effort are derived from the Maritime Expeditionary Security ICD March 2008

The Man-portable Tactical Autonomous System (MANTAS) Unmanned Surface Vehicle (USV) with Near-shore Unified Tactical Response (NUTR) Common Operating Picture (COP) project provides for enhanced USV control for operators of the NUTR terminals by integrating some basic vehicle/sensor package controls (e.g. manual control of vehicle speed and direction) and coordinated behavior commands (e.g. swarm control). The project will also incorporate NUTR technology into the MANTAS Mobile Command Center (MCC) software in order to display the current COP on the MCC operator's display. The MCC will also utilize NUTR technology to display the operator's position on the MCC's geographical display and report that location back to NUTR COP.

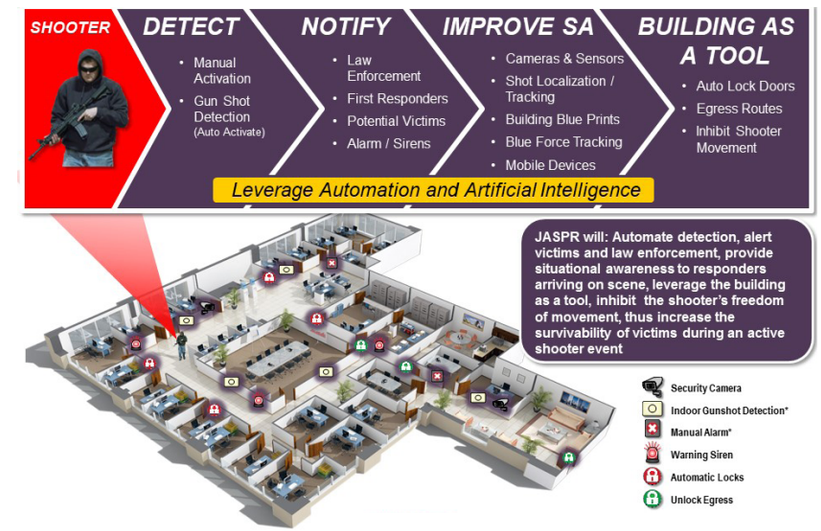


JOINT ACTIVE SHOOTER PROTECTION & RESPONSE

REQUIREMENTS

— Office of the Provost Marshal General, Physical Security Division is writing the deliberate requirement for JASPR leveraging the business initiative process to become a Defense Business System

The Joint Active Shooter Protection & Response (JASPR) effort will develop an integrated capability leveraging current and emerging technologies to automatically detect indoor gunshots, provide potential victims, responders, and authorized personnel with information for increased situational awareness, and enable automatic or manual control of the building. The goal is to inhibit the shooter, shorten the duration of an active shooter, and ultimately save lives.



M2HB/M2A1 WEAPON SIGHT

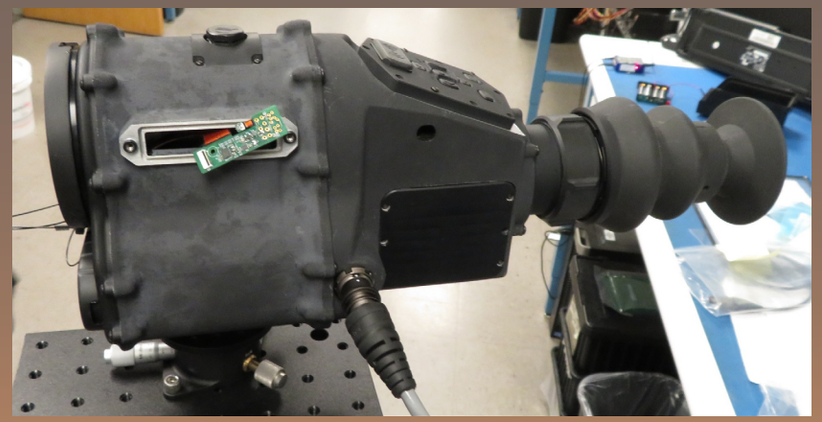
REQUIREMENTS

— Letter from Commander, Navy Expeditionary Combat Command titled "Visual Augmentation Systems (VAS) Capability Requirements and Associated Capability Gaps," October 2, 2014

— Navy Expeditionary Combat Command Expeditionary Warfare Improvement Program Integrated Priority Capability List priorities, July 10, 2015

— Visual Augmentation Systems Capability Development Document (draft)

The M2HB/M2A1 Weapon Sight effort is the development of an advanced thermal imaging sight for the M2HB/M2A1 crew-served weapon systems. This system will enable improved target acquisition capabilities. The system would include multiple target indicators, an integrated ballistics processer, video recording, and a data export functionality.



NAVY STABILIZED CREW-SERVED HEAVY MACHINE GUN MOUNT

REQUIREMENTS

— 2017 Integrated Prioritized Capabilities List for Surface Warfare and Joint Urgent Operational Needs for Antiterrorism/Force Protection

The Navy Stabilized Crew-Served Heavy Machine Gun Mount project is a review of requirements, procurement, suitability testing, design improvement, and a demonstration of a field-able stabilized crew-served heavy machine gun mount for naval applications. The stabilized crew-served heavy machine gun mount will be useful for antiterrorism/force protection missions including the fast attack craft/fast inshore attack craft role. The proposed stabilized crew-served mount would provide improvements to legacy systems without sacrificing deck space, situational awareness, or impacting training. At the end of this project, the stabilized crew-served weapon system will exhibit an increase in the probability of hit against stationary and moving surface targets.

TACTICAL RADIO INTERFACE CONSOLE

REQUIREMENTS

— 2015 Antiterrorism/Force Protection Integrated Priority Capability List (paragraphs 2.D.6.C and 5.E.3) and Fleet requests

The Tactical Radio Interface Console (TRIC) project will demonstrate a communications interface device that enables force protection radios to associate and communicate with other ship's Land Mobile Radio systems effectively. TRIC would be agnostic of the manufacturer or frequency required. This capability would enable existing mobile radios to seamlessly communicate with each other as well as new radios that are introduced across all ships.

VIRTUAL REALITY SYNTHETIC BOAT AND WARNING SHOT SIMULATOR

REQUIREMENTS

— Navy Expeditionary Combat Command Capability Gap

— Gap derived from Universal Joint Task List, specifically OP 5.4.6 Conduct Operational Rehearsal

The Virtual Reality (VR) Synthetic Boat and Warning Shot Simulator effort will create a virtual version of the warning shot simulator that supplements existing training, and provides remote anytime-anywhere refresher training. The virtual trainer will consist of lightweight, low-cost equipment which can be rapidly deployed and quickly installed at multiple locations to support local training. This trainer will enhance current capabilities and likely decrease training/qualification time required for the current Warning Shot Simulator. This prototype simulator will serve as a stepping stone to later efforts to build a large-scale boat simulator and inform the formal defense acquisition process.

PREVENTION

The security procedures taken to discourage an adversary from accessing weapons of mass destruction or gaining unauthorized access to critical assets are at the heart of prevention. This capability area focuses on broad-spectrum, generic efforts that have the ability to influence multiple areas.

STANDOFF WEAPONS DEFEAT JOINT INTEGRATED PRODUCT TEAM

REQUIREMENTS

— DoD Manual S-5210.41, "(U) Nuclear Weapon Security Manual: The DoD Nuclear Weapon Security Program"

The Standoff Weapons Defeat Joint Integrated Product Team (JIPT) has supported the development of a Standoff Weapons (SOW) Defeat capability since 2014. The JIPT initially assessed the current state of the art in SOW defeat capabilities then addressed the requirements, architecture, technology roadmaps, and funding needed to develop those capabilities. The JIPT draws its membership from the joint nuclear weapon surety community, the conventional force requirements community, and government technical experts from Service laboratories. The FY18 IPT effort transitioned to the Counter-Unmanned Aircraft Systems (C-UAS) Capabilities Working Groups and continued assessing the current state-of-the-art in small UAS countermeasures and provided ad hoc technical subject matter experts support to the Services responding to U.S. Strategic Command's Joint Emergent Operational Needs Statement.

STORAGE & SAFEGUARDS

Properly securing critical assets to prevent access by unauthorized persons and implementing control measures that ensure access is limited to authorized persons is the foundation of physical security. This capability area addresses equipment (e.g., locks, doors, etc.) designed to delay or stop unauthorized entry/access to a specified/localized area.

APPENDICES

INTRODUCING THE NEW PSEAG SEAL

The Longitude and Latitude lines descending down from the point of the sword symbolize global protection.

The sword pointing upward symbolizes power, strength, and preparation for current and future defense.

The four horizontal colored stripes in the handle of the sword mirror the support branches of PSEAG:

- Army (green)
- Marine Corps (red)
- Navy (dark blue)
- Air Force (light blue)

The globe represents the breadth of our work, protecting and defending DoD assets and military personnel at home and abroad.

DETERRENCE is the first method of ensuring Physical Security on the home front.

Guidance from the DoD and the Pentagon not only help DETECT Physical Security threats, but the equipment/products produced as a result of these requirements help detect intruders in a secured area.

The third method of ensuring Physical Security is to DEFEND the secured area as represented by the sword. The Physical Security products produced through the PSEAG will help to do this.

PSEAG SHAREPOINT SITE

The PSEAG is managed using the web portal below that allows program managers, government representatives, support contractors and other approved users to access a wealth of Physical Security RDT&E related information, upload reports, view historical documents, and collaborate in a secured environment. The portal fosters collaboration between force protection (FP) communities and 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 policy documents that provide guidance on the development and use of physical security equipment.

This tool has modernized the once-tedious paper process, standardizes the format for all future projects, and serves as an archive of historical project data and reports. The web portal enables users to enter monthly reports and scheduling data for projects and events, generate aggregated reports, and display project health information for use by managers when conducting project reviews.

ACRONYMS

AFPSEAG	*Air Force PSEAG*
AFRL	*Air Force Research Laboratory*
APSEAG	*Army PSEAG*
AR HUD	*Augmented Reality Heads Up Display*
ASD(NCB)	*Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs*
***AT&L**	*Acquisition, Technology, and Logistics*
ATTWO	*Antiterrorism Tactical Watch Officer*
AUV	*Autonomous Underwater Vehicle*
BEACH	*Biometrically Enabled Access Control - Husbanding*
BSAT	*Biological Select Agents and Toxins*
C2	*Command and Control*
CCIR	*Commander's Critical Information Requirements*
CDD	*Capability Development Document*
CDS	*Cross Domain Solution*
CFR	*Code of Federal Regulations*
CIME	*Continuous Identity Matching Engine*
CNIC	*Commander, Navy Installations Command*
COA	*Courses of Action*
COP	*Common Operating Picture*
COTS	*Commercial Off-The-Shelf*
C-UAS	*Counter-Unmanned Aircraft System*
DASD(NM)	*Deputy Assistant Secretary of Defense for Nuclear Matters*
DEERS	*Defense Enrollment Eligibility Reporting System*
DFBA BOD	*Defense Forensics and Biometrics Agency Biometrics Operations Division*
DIA	*Defense Intelligence Agency*
DoD	*Department of Defense*
DoDD	*Department of Defense Directive*
DoDI	*Department of Defense Instruction*
DoDM	*Department of Defense Manual*
DTM	*Directive Type Memorandum*
DTRA	*Defense Threat Reduction Agency*
ECP	*Entry Control Point*
EDE	*Explosive Detection Equipment*
EO/IR	*Electro-Optical/Infrared*
FOB	*Forward Operating Base*
FOPEN	*Foliage Penetration*
F2CS	*Flexible Fire Control System*
FBI	*Federal Bureau of Investigation*
FP	*Force Protection*

ACRONYMS

FY	*Fiscal Year*
G-BOSS(E)	*Ground-Based Operational Security System (Expeditionary)*
GOTM-B	*Gatekeeper on the Move-Biometrics*
GunnAR	*Gunnery System with Augmented Reality*
HSPD	*Homeland Security Presidential Directive*
ICBM	*Intercontinental Ballistic Missile*
ICD	*Initial Capabilities Document*
IEPD	*Information Exchange Package Documentation*
IGDS	*Indoor Gunshot Detection System*
IGSSR-C	*Integrated Ground Security Surveillance and Response-Capability*
IMESA	*Identity Management Engine for Security & Analysis*
IoLS	*Interoperability Layer Service*
IPT	*Integrated Product Team*
IR	*Infrared*
ISA	*Integrated Sensor Architecture*
ISEA	*In-Service Engineering Agent*
IT	*Information Technology*
JASPR	*Joint Active Shooter Protection & Response*
JIGSAW	*Joint Interoperable Gateway for Security, Antiterrorism, and Warfighting*
JIPT	*Joint Integrated Product Team*
LSS	*Linear Sensor System*
MANTAS	*Man Portable Tactical Autonomous System*
MCC	*Mobil Command Center*
MCPSEAG	*Marine Corps PSEAG*
MilOps	*Military Operations*
MSDD	*Multi-Sensor Detection and Discrimination*
NAVFAC	*Naval Facilities Engineering Command*
NAVSEA	*Naval Sea Systems Command*
NCIC	*National Crime Information Center*
NCIS	*Naval Criminal Investigative Service*
NIEM	*National Information Exchange Model*
NPSEAG	*Navy PSEAG*
NSPD	*National Security Presidential Directive*
NUTR	*Near-Shore Unified Tactical Response*
OASD(NCB/NM)	*Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs / Nuclear Matters*
PACS	*Physical Access Control Systems*
PIDS	*Portable Intrusion Detection System*
PSE	*Physical Security Equipment*
PSEAG	*Physical Security Enterprise & Analysis Group*
PSIM	*Physical Security Information Management Systems*
RDT&E	*Research, Development, Test and Evaluation*
RFID	*Radio Frequency Identification*
SECDEF	*Secretary of Defense*
SEIWG	*Security Equipment Integration Working Group*
SFF	*Small Form Factor*
SOW	*Standoff Weapons*
SOAR	*System Operations Audit and Recording*
T&E	*Test & Evaluation*
TRIC	*Tactical Radio Interface Console*
TSDB	*Terrorist Screening Database*
TUAS	*Tethered Unmanned Aerial System*
UAS	*Unmanned Aircraft Systems*
USAF	*United States Air Force*
USD	*Under Secretary of Defense*
USD(A&S)	*Under Secretary of Defense for Acquisition & Sustainment*
***USD(AT&L)**	*Under Secretary of Defense for Acquisition, Technology, and Logistics*
USMC	*United States Marine Corps*
USV	*Unmanned Surface Vehicle*
UUV	*Unmanned Underwater Vehicle*
VA	*Video Analytics*
VAS	*Visual Augmentation System*
VR	*Virtual Reality*
VCJS	*Vice Chairman, Joint Chiefs of Staff*
WISP	*Wide Area Infrared System for Persistent Surveillance*

**Per the National Defense Authorization Act for Fiscal Year 2017 the Office the Under Secretary of Defense for Acquisition, Technology, and Logistics was disestablished and divided into the Office of the Undersecretary of Defense for Acquisition and Sustainment and the Office of the Undersecretary of Defense for Research and Engineering.*