DEPARTMENT OF DEFENSE

PHYSICAL SECURITY ENTERPRISE & ANALYSIS GROUP

PSEAG

2014 RDT&E

RESEARCH, DEVELOPMENT, TEST & EVALUATION

PROGRAM SUMMARY

PHYSICAL SECURITY ENTERPRISE & ANALYSIS GROUP ★ 2014 RDT&E PROGRAM SUMMARY

Dr. Vahid Majidi, Deputy Assistant Secretary of Defense for Nuclear Matters (DASD(NM))

The Washington Navy Yard shooting on September 16, 2013 is a tragic reminder that the Department of Defense must remain vigilant to internal and external threats. The success of the United States' policy to address terrorism at home and abroad depends on the steady development and deployment of technologies that meet the specific requirements of our Armed Forces. In 2014, the Department of Defense (DoD) Physical Security Enterprise & Analysis Group (PSEAG) played an important role in addressing this need and this summary highlights the physical security Research, Development, Test & Evaluation (RDT&E) efforts that are underway.

As the Deputy Assistant Secretary of Defense for Nuclear Matters, my office is responsible for overseeing the development of Department-wide physical security RDT&E solutions. The PSEAG will continue to pursue equipment and systems that leverage commonalities in physical security requirements that closely balance and integrate the needs of the Department of Defense.

Vahid Majidi, Ph.D.
Deputy Assistant Secretary of Defense
(Nuclear Matters)

Dr. Majidi became the Deputy Assistant Secretary of Defense for Nuclear Matters in December 2013. In this position, he is responsible for all aspects of nuclear weapon surety and the management, integration, and coordination of activities relating to the acquisition and modernization of the nuclear weapons stockpile. His office approves procedures and requirements relating to all facets of the nuclear weapons logistics and establishes procedures for review, approval, and transmittal to the Department of Energy on nuclear weapons matters.

2014 RDT&E

RESEARCH, DEVELOPMENT, TEST & EVALUATION

PROGRAM SUMMARY

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

In 2014, the Physical Security Enterprise & Analysis Group (PSEAG) continues its mission in the research and development of joint physical security solutions for the Services, while maximizing limited Department of Defense resources. The year was an important one for

the PSEAG that realized multiple significant events. They included the success of the Defense Installation Access Control Joint Capability Technology Demonstration proving for the first time that multiple Service installations and agencies can share real-time data across disparate secure systems improving physical access control; the ongoing efforts to thwart insider threats through the Continuous Evaluation Concept Demonstration; the PSEAG addressed information sharing requirements through the Mission Assurance, Threat Alert, Resiliency and Response project, and demonstrated an integrated set of new capabilities to address identified gaps in waterside security architecture through the Integrated Waterside Security Concept Demonstration. Lastly, the PSEAG oversaw the development of a backbone and data mediation capability through the Defense Security Enterprise Architecture project.

The PSEAG 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)), the Military Services and the Defense Threat Reduction Agency (DTRA). The mission of the PSEAG is to "provide enterprise-level physical security solutions to reduce risk, address prioritized capability gaps and serve as the catalyst for analyzing, developing, demonstrating and evaluating interoperable systems for DoD-wide requirements." This PSEAG summary provides a snapshot of 29 physical security-related research and development requirements identified by the Services and approved and vetted by the Office of the Secretary of Defense and the Joint Staff. These physical security requirements are identified through findings and recommendations reported by Department policy and security reviews. Prior to portfolio development and initiation of any RDT&E project, each requirement is scrutinized based on specific criteria including; a Joint-Service review, a capability gap review and match, and a return on investment analysis for the program.

Reflecting the mission of the program, joint initiatives make up the largest portion of the 2014 PSEAG portfolio. The following projects are examples of capabilities led by shared requirements from the Services, driven by policy directives, and in response to issues of national importance. The following projects emphasize capabilities in the areas of access control, decision support, and integrated approaches to physical security.

The Defense Installation Access Control (DIAC) effort played a significant role in addressing Washington Navy Yard investigation recommendations. The Secretary of Defense's

memorandum, "Final Recommendations of the Washington Navy Yard Shooting Internal and Independent Reviews" includes the DIAC's Identity Management Engine for Security & Analysis (IMESA) as one of the four key recommendations to address access control shortfalls noted during the internal and independent reviews. During the recent DIAC Joint Capability Technology Demonstration, this capability proved the Department could access and vet against federal authoritative data sources including the National Crime Information Center database.

The Continuous Evaluation Concept Demonstration utilizes software and business rules developed by the Defense Manpower Data Center (DMDC) to process automatic records checks of DoD, FBI, and commercial data sources to allow the DoD to conduct continuous evaluation (CE) of its cleared personnel. This RDT&E initiative continues to develop a CE capability to be able to identify cleared individuals in near real-time who may no longer meet the criteria for retaining a clearance and have become a potential security risk.

The Defense Security Enterprise Architecture serves to protect forces, mitigate threats, close protection gaps, and provides increased situational awareness by linking disparate physical, personnel, informational, industrial and operations security capabilities across the DoD while leveraging other government agencies' information. This capability develops a backbone and data mediation capability to share security domain information on a near real-time basis.

The Integrated Waterside Security Concept Demonstration was held in September 2014. This demonstration, composed of a select set of technologies/systems deployed ashore and afloat, that when integrated together at both the organizational and systems level, demonstrated a high potential to address specific gaps and shortfalls in the waterside security architecture and to improve the security posture and effectiveness in both the conventional and nuclear forces of the U.S. Navy.

Mission Assurance, Threat Alert, Disaster Resiliency and Response is another joint initiative established to automate information sharing interfaces across stove-piped emergency management and force protection applications to improve situational awareness and decision making. Due to the success of this demonstrated capability in CONUS; a similar need was also identified to eliminate information sharing gaps within the United States European Command area of responsibility.

The projects highlighted in this summary showcase the collaborative efforts of the PSEAG program to meet its mission of harmonizing requirements of the Services to combat the evolving threats within the physical security community. In the near term the PSEAG will continue to collaborate with other government agencies such as the science & technology community to transition concepts into developmental efforts that can be turned over to the Services for transition to programs of record. The PSEAG expects to address capabilities required to combat evolving threats in the areas of maritime and airborne threats, maritime force protection, cyber threats, standoff weapons detection and defeat, the establishment of a joint explosive detection program, and addressing weapons of mass destruction security requirements with the goal of ultimately creating a safer Nation for us all.

Roderick E. Gillis
Chairman,
Physical Security Enterprise & Analysis Group

Contents

INTRODUCTION 8

Department of Defense Physical Security Research, Development, Test and Evaluation (RDT&E) Program Overview 9

PSEAG Program Funding 10

PSEAG Program by Capability Area 11

ACCESS CONTROL 13

Continuous Evaluation Concept Demo 15

Defense Installation Access Control Working Group 16

Intermodal Security Devices 17

ANALYTICAL SUPPORT 19

PSEAG Top 5 Project Review 21

DECISION SUPPORT 23

Defense Security Enterprise Architecture 25

Emergency Responder Common Operating Picture 26

Identification of Friend or Foe 27

Integrated Waterside Security Concept Demonstration 28

Integrated Ground Security Surveillance Response – Capability 29

Joint Interface Group for Security Application Workspaces 30

Keystone United States European Command Technical Demonstration 31

Missile Field Defense Force Command, Control, Communications and Situational Awareness 32

Mission Assurance, Threat Alert, Disaster Resiliency and Response 33

Near-shore Unified Tactical Response 34

Video Management System 35

DETECTION & ASSESSMENT 37
Comparative Test and Evaluation:
HazMatID ELITE and HazMatID 360 39
Explosive Detection Equipment for Maritime Environment 40
Ground-Based Operational Surveillance System (Expeditionary) 41
Hailing Acoustic, Laser and Light Tactical System 42
Interceptor 43
Long Range Threat Identification Sonar 44
Marine Mammal Vigilance Localization 45
Radar Assisted Area Protection 46
Radar Processing Dynamic Structure Filter 47
Radiological Detection System 48
Comparative Test and Evaluation: Sensor Fusion Prototype Units 49
U.S. Navy Spike Weapon System Electro-Optical Seeker Upgrade 50

PREVENTION 53
Marine Mammal Enhanced Interdiction 54
Foliage Penetration Technology Evaluation 55

STORAGE & SAFEGUARDS 57
Radio Frequency Identification Tagging for Items in Extreme Cold Storage 59

APPENDICES 60
Administrative Points of Contact 61
List of Acronyms 62
PSEAG Sharepoint Site 66
DoD Physical Security Enterprise & Analysis Group 67

INTRODUCTION

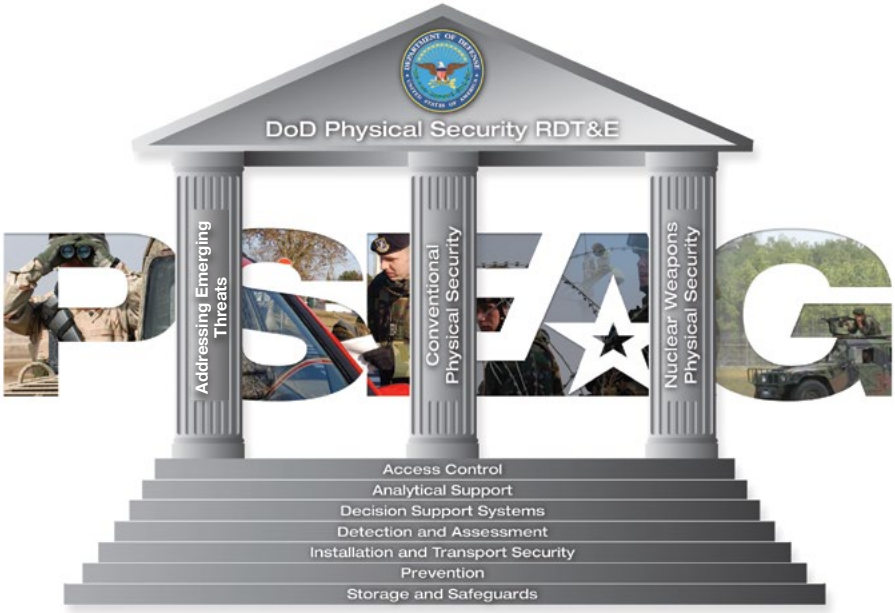
Department of Defense Physical Security Research, Development, Test and Evaluation (RDT&E) Program Overview

The Department of Defense (DoD) Physical Security 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. 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.

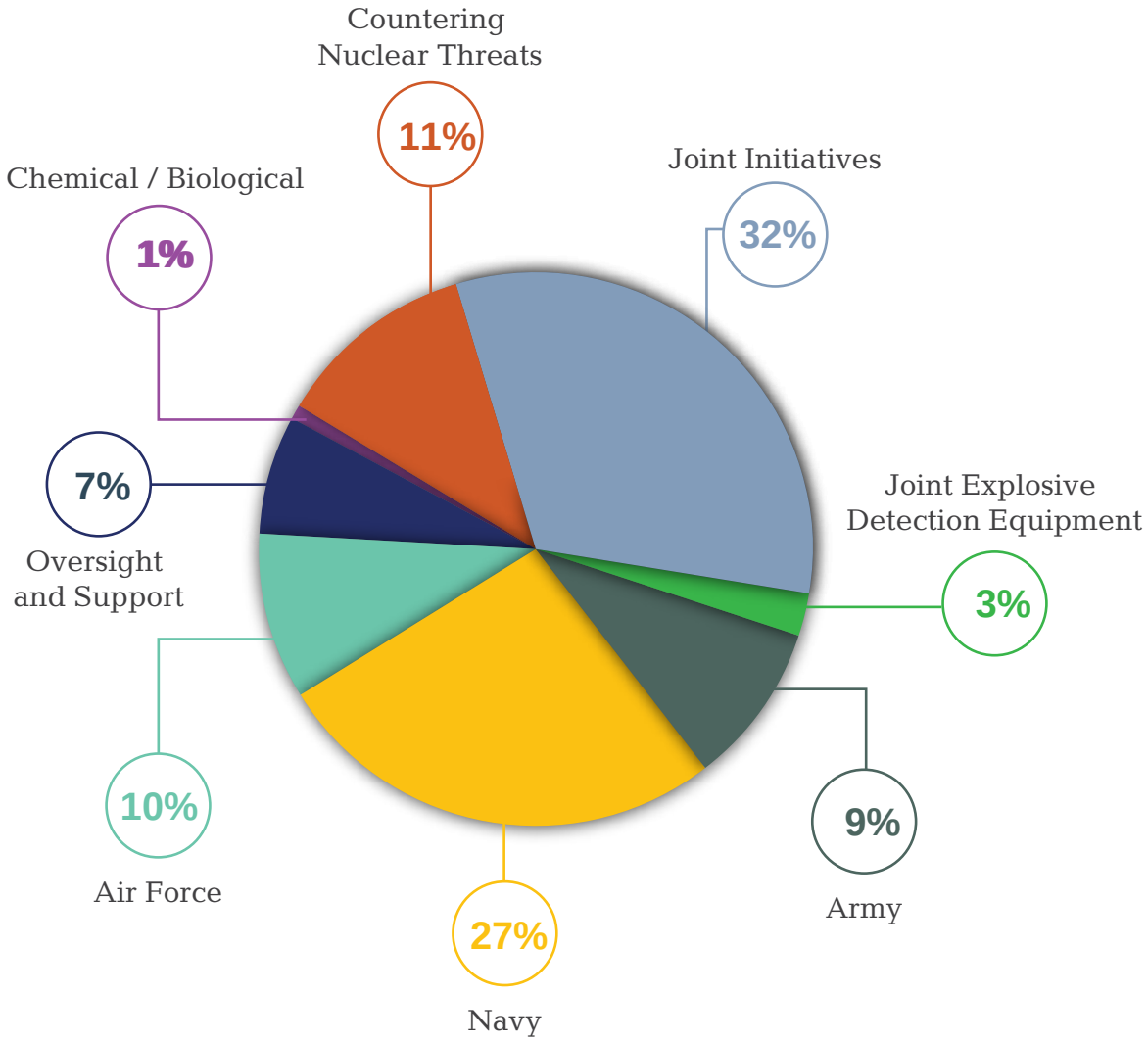
Underpinning this entire structure is a foundation of physical security activities, which are now organized into capability areas, centered on key physical security requirements. These capability areas bring together formerly disparate physical security projects into more cohesive and synergistic physical security 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



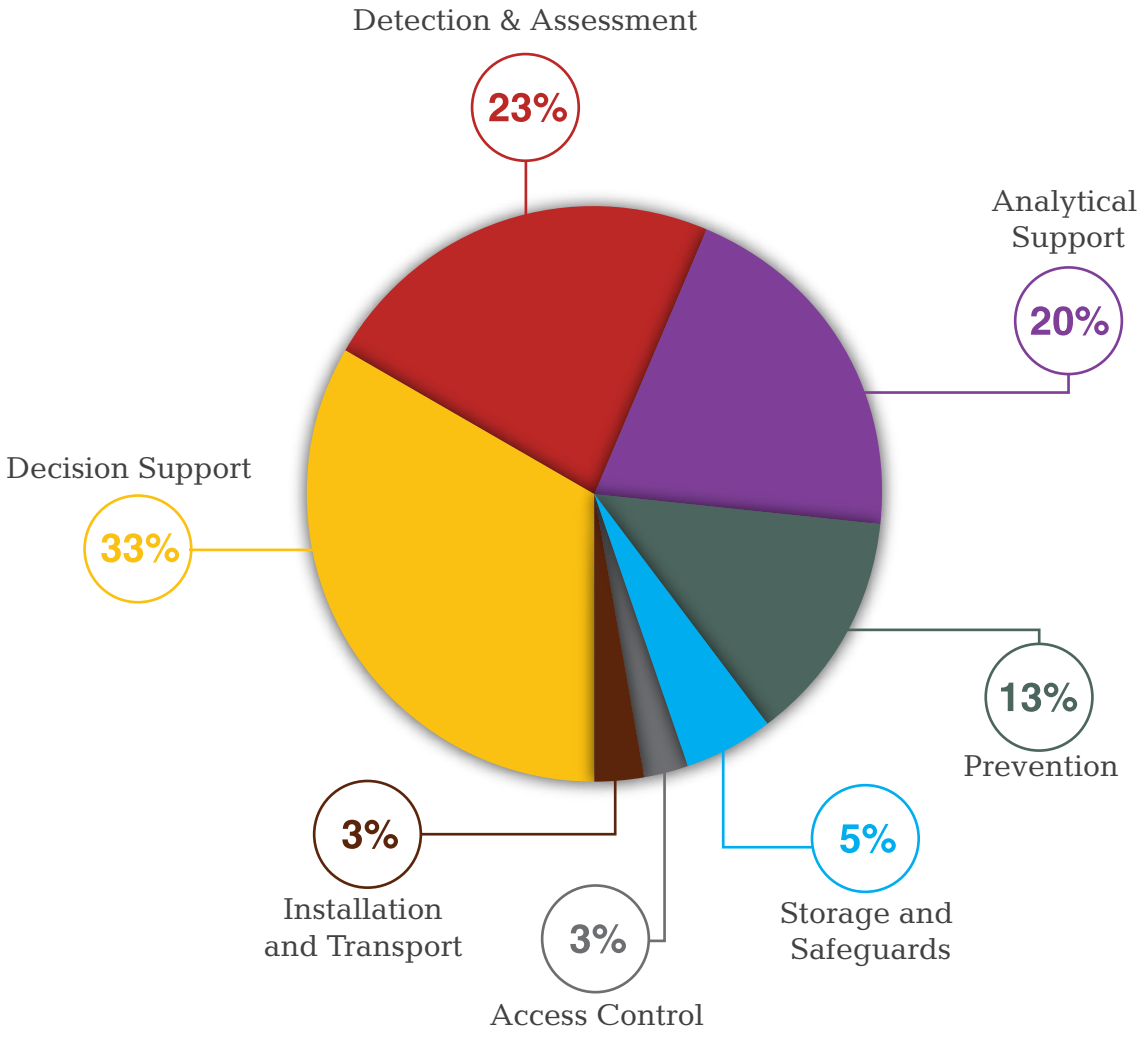
PSEAG Program Funding

This year's funding of over $30 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.



PSEAG Program by Capability Area

Decision Support, Detection & Assessment, Analytical Support, and Prevention were the largest capability areas for research and development in 2014. These capability areas reflect the Services priorities and requirements for the year.



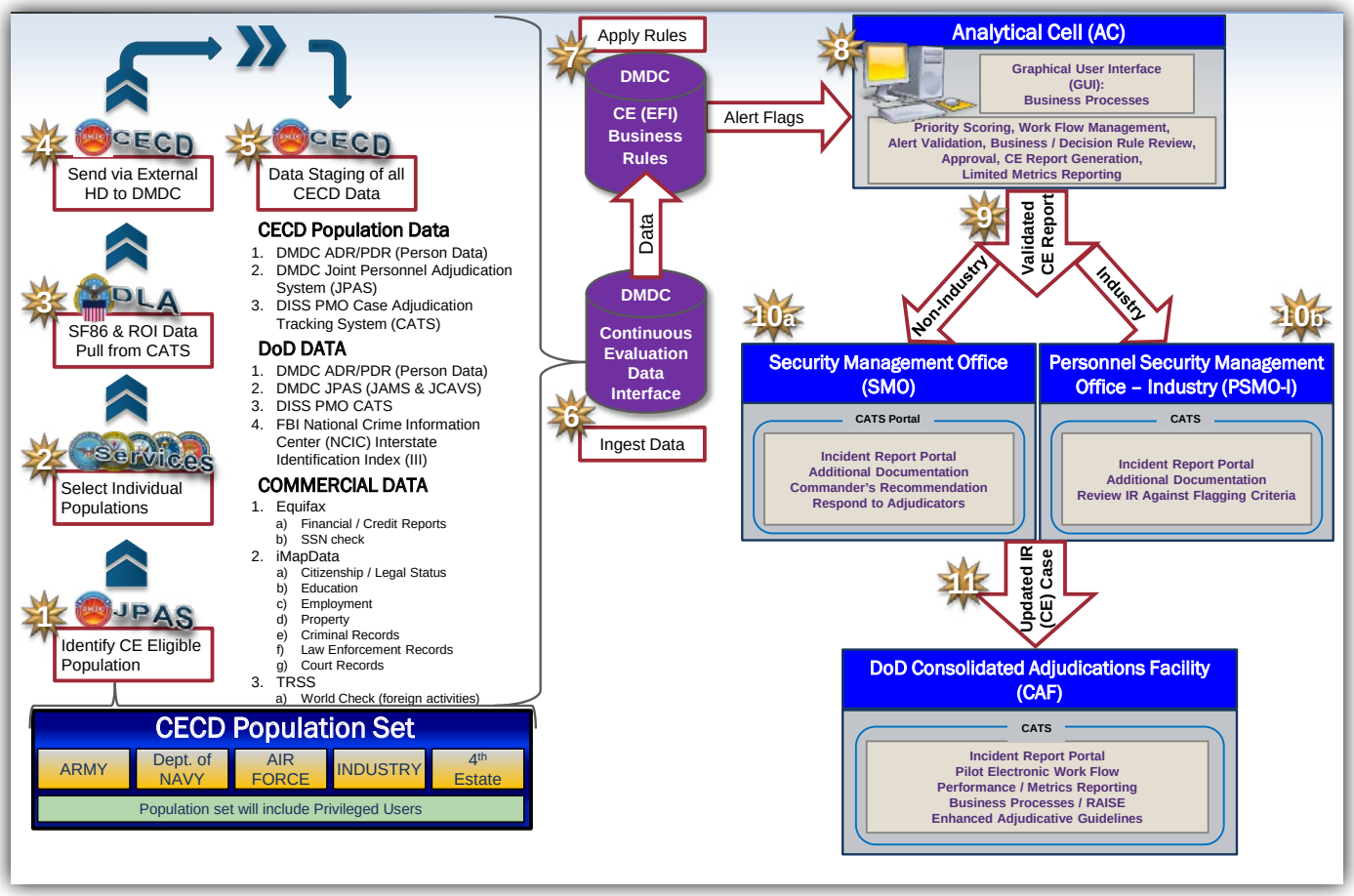
ACCESS CONTROL

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

Photo Credit: US Department of Defense. 2013

Continuous Evaluation Concept Demo

This project utilizes software and business rules developed by the Defense Manpower Data Center (DMDC) to process DoD, FBI, and commercial data sources to allow the DoD to conduct continuous evaluation (CE) of its cleared personnel. This RDT&E initiative continues to develop a CE capability to be able to identify cleared individuals in near real-time who may no longer meet the criteria for retaining a clearance and have become a potential security risk.

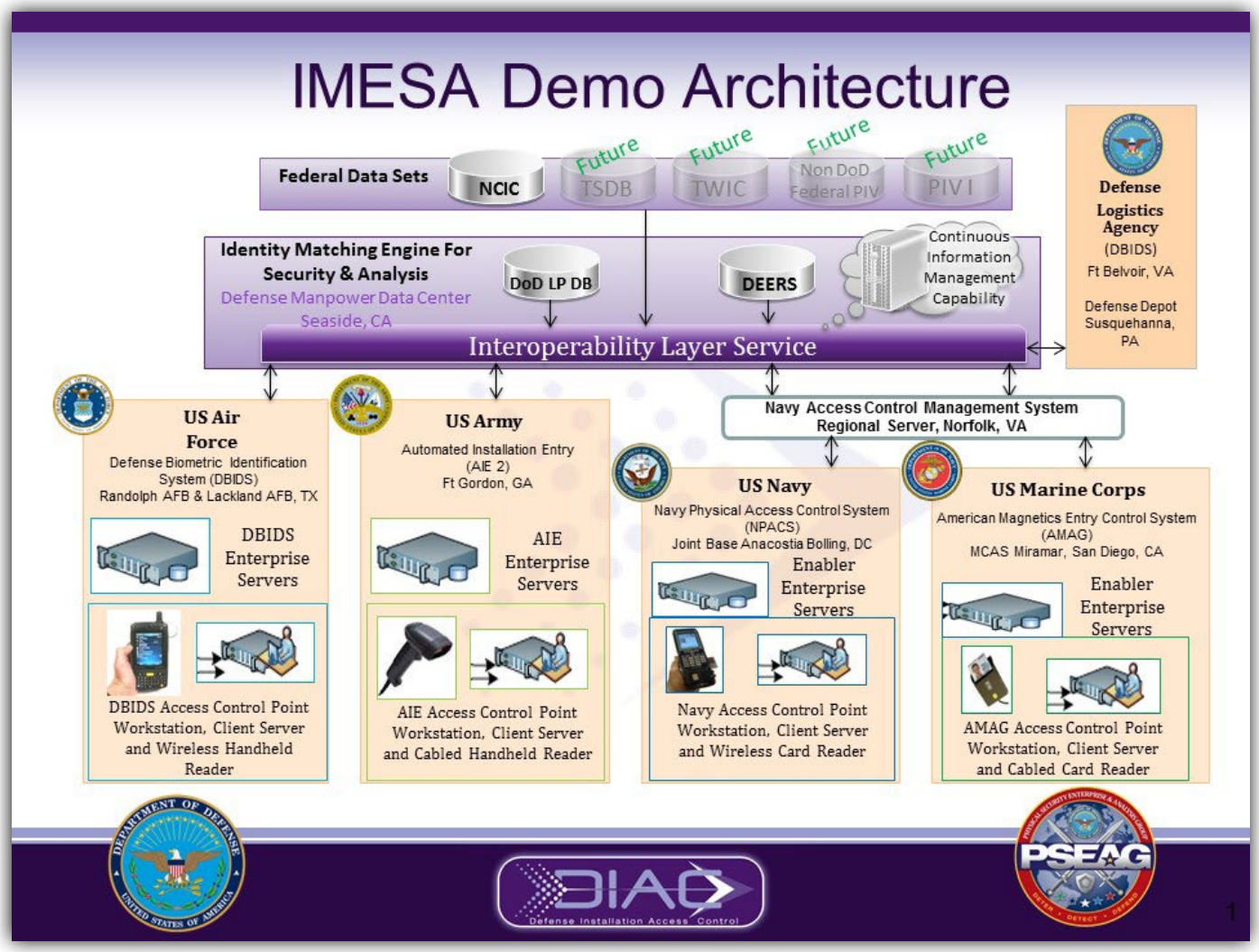


Requirements

- CENTCOM 2013 IPL 7 (STIPL 6.a and 6.d)
  Joint Service Explosive Ordnance Disposal ICD 1 June 2005
- Fleet Forces Command 2011 IPCL 1 & 6
  Navy Expeditionary Combat Command S&T Strategic Plan November 2011
- Integrated Unit, Base Installation Protection ICD January 2008
- DoD 2000.16 October 2006

Defense Installation Access Control Working Group

Defense Installation Access Control Working Group's goal is to develop an Identity Management Enterprise Services Architecture. The project team successfully demonstrated this capability during a recent Joint Capability Technology Demonstration.

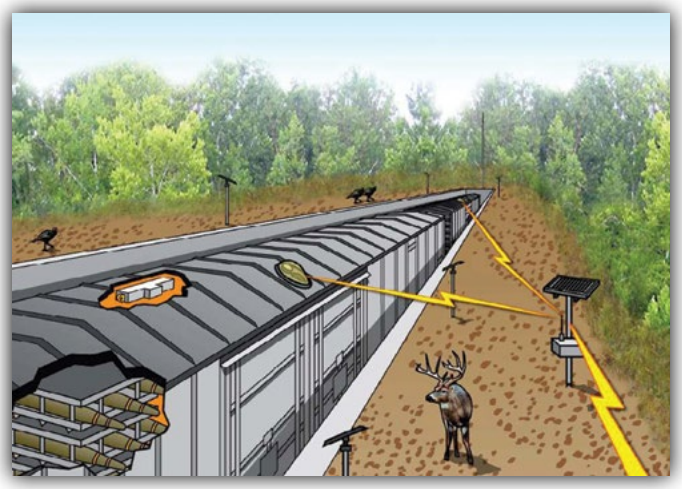


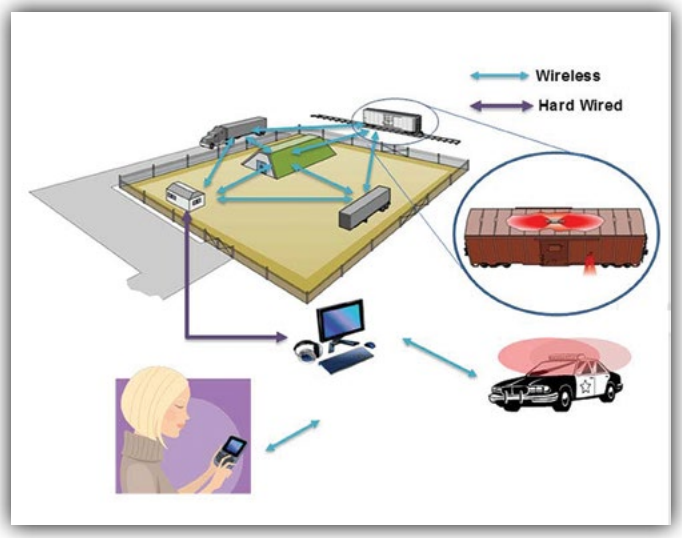
Requirements

- 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

Intermodal Security Devices

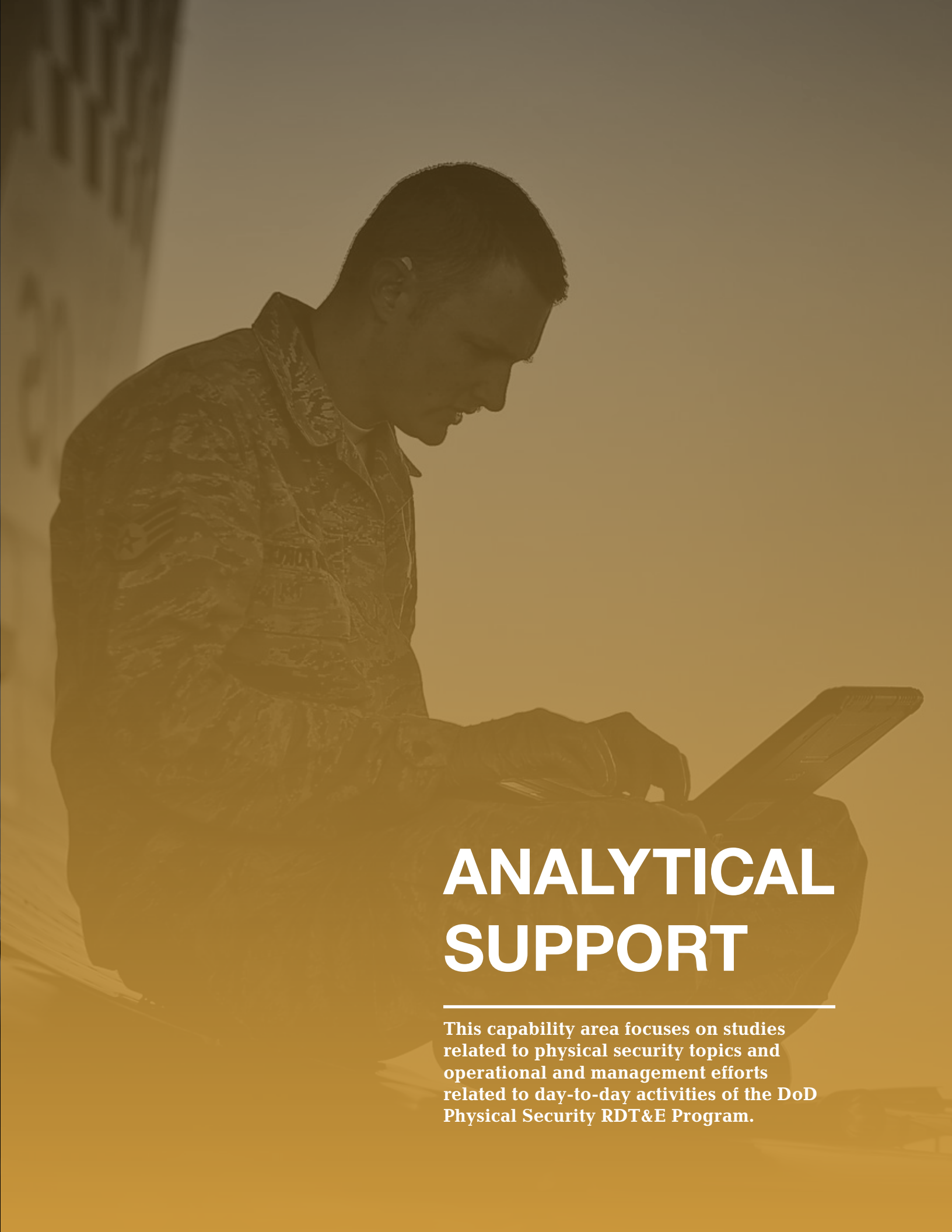
The Intermodal Security Devices project provides a wireless sensor network and web-based interface capability that detects breaches, door openings and environmental condition alarms. The System provides capability to integrate with services' existing Command, Control, Communications, Computer, and Intelligence architecture, or to operate as a standalone system.





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



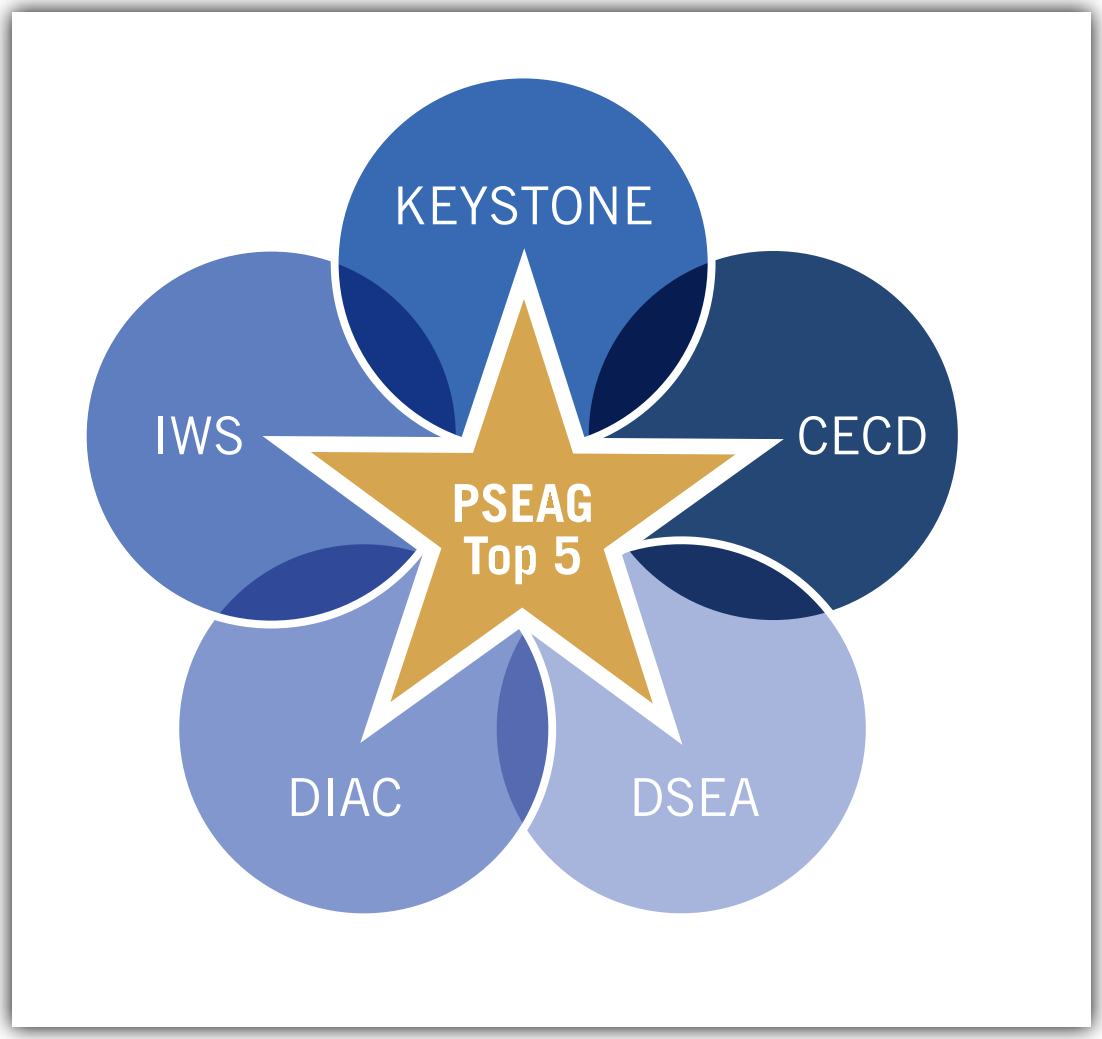
ANALYTICAL SUPPORT

This capability area focuses on studies related to physical security topics and operational and management efforts related to day-to-day activities of the DoD Physical Security RDT&E Program.

Photo Credit: US Department of Defense. 2012

PSEAG Top 5 Project Review

For this project the team conducted a technical characterization of the top five PSEAG projects to provide leadership with a standardized technical understanding of each project. This characterization will be used to determine possible efficiencies and augment strategic engagements with PSEAG leadership for increased awareness and support.



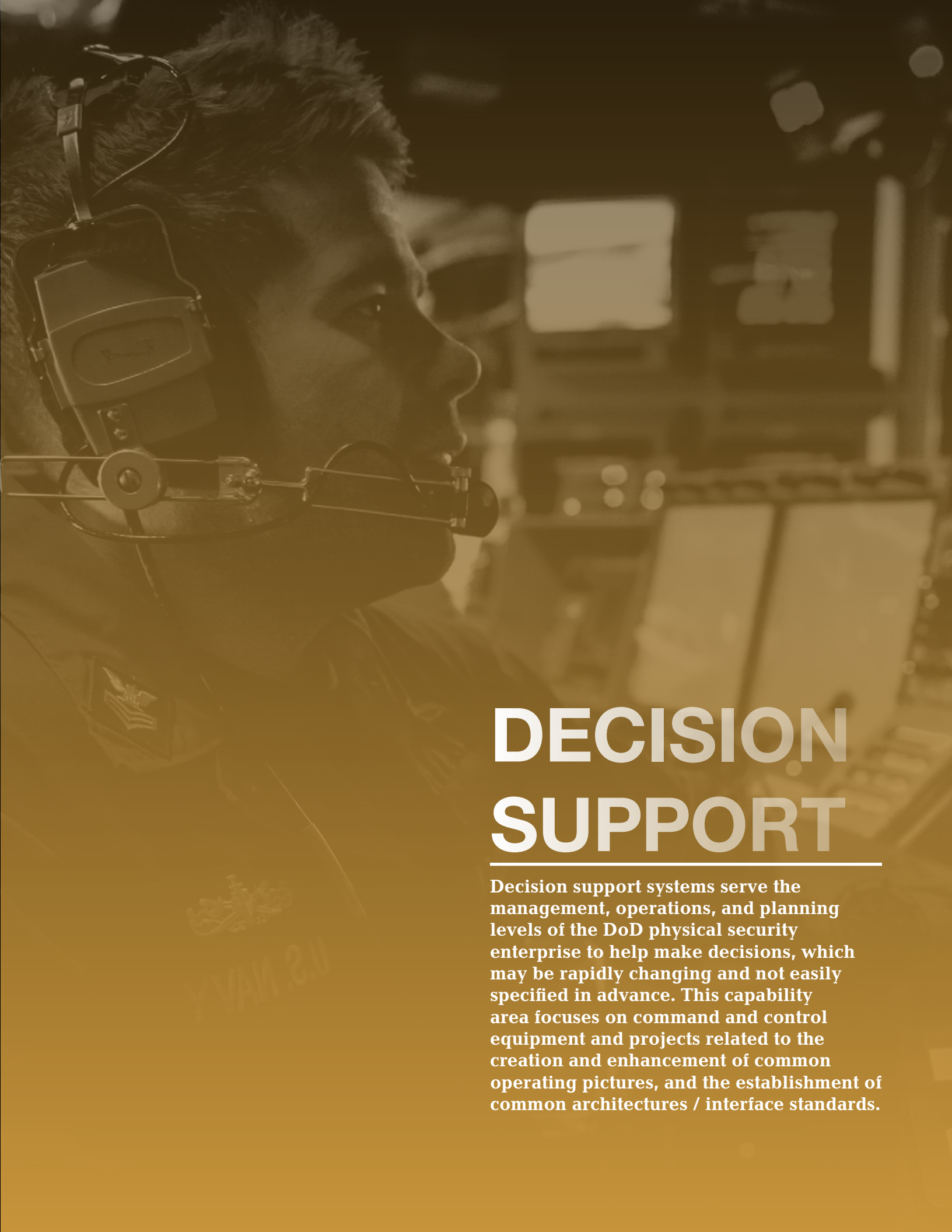
DIAC Defense Installation Access Control

CECD Continuous Evaluation Concept Demonstration

DSEA DEFENSE SECURITY ENTERPRISE ARCHITECTURE

INTEGRATED WATERSIDE SECURITY NPSEAG

KEYSTONE



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 and not easily specified in advance. 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 / interface standards.

Photo Credit: US Department of Defense. 2014

Defense Security Enterprise Architecture

This project will develop shared and automated content across the security domains and functional areas, enabling more efficient and accurate personnel vetting, access controls, insider threat prevention and enhanced security operating environments.

Requirements

- HSPD 5, HSPD12, Ft Hood Report Findings and Recommendations, DoDD 5200.43, Management of the Defense Security Enterprise

Emergency Responder Common Operating Picture

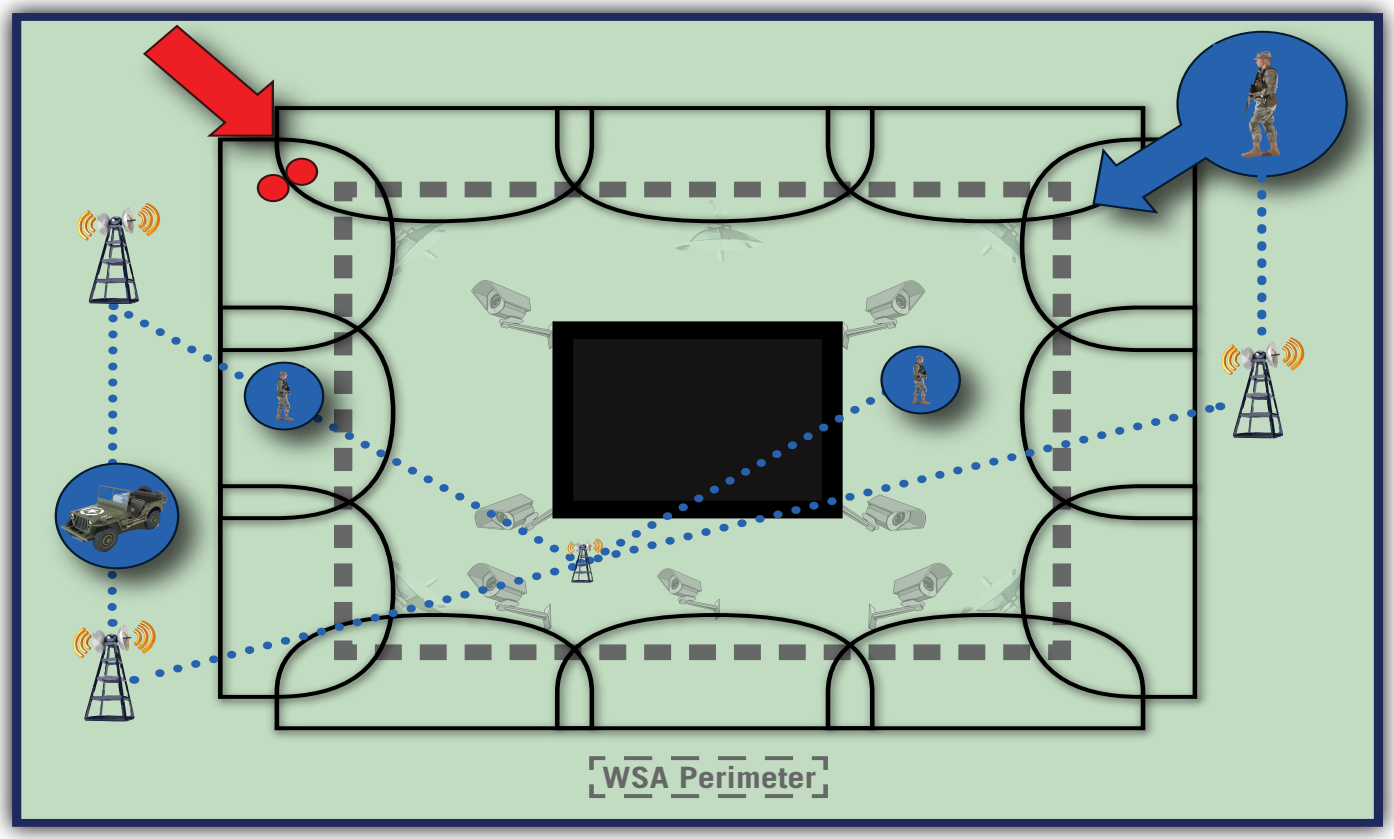
This project is an emergency notification system capability that will leverage existing AtHoc commercial-off-the-shelf (COTS) software to test and evaluate a fully integrated, COTS-ready common operating picture and shared situational awareness capability. The capability will be implemented and tested at one to several installations and support the day-to-day operational needs of the First Responder community, including, but not limited to; the Emergency Operations Center, Security Forces, Fire, Medical, Emergency Management operations and the installation Command Post.

Requirements

- SECDEF Hood Memo and DoDI 6055.17

Identification of Friend or Foe

Develops a capability to display Identification "Friend or Foe" information in two phases. Phase I – Develop and test correlation capability that integrates with wide area sensor and Command and Control Display Equipment Phase II – Specify, procure and evaluate Position Location Identification Tags for authorized personnel.



Requirements

- CDD for IBDSS, 17 Feb 05
- DoD S-5210.41M, 13 Jul 09, Volume 1, Encls 3 & 5
- AFMAN 31-108, 01 Feb 10, Volume 3, Encl 3

Integrated Waterside Security Concept Demonstration

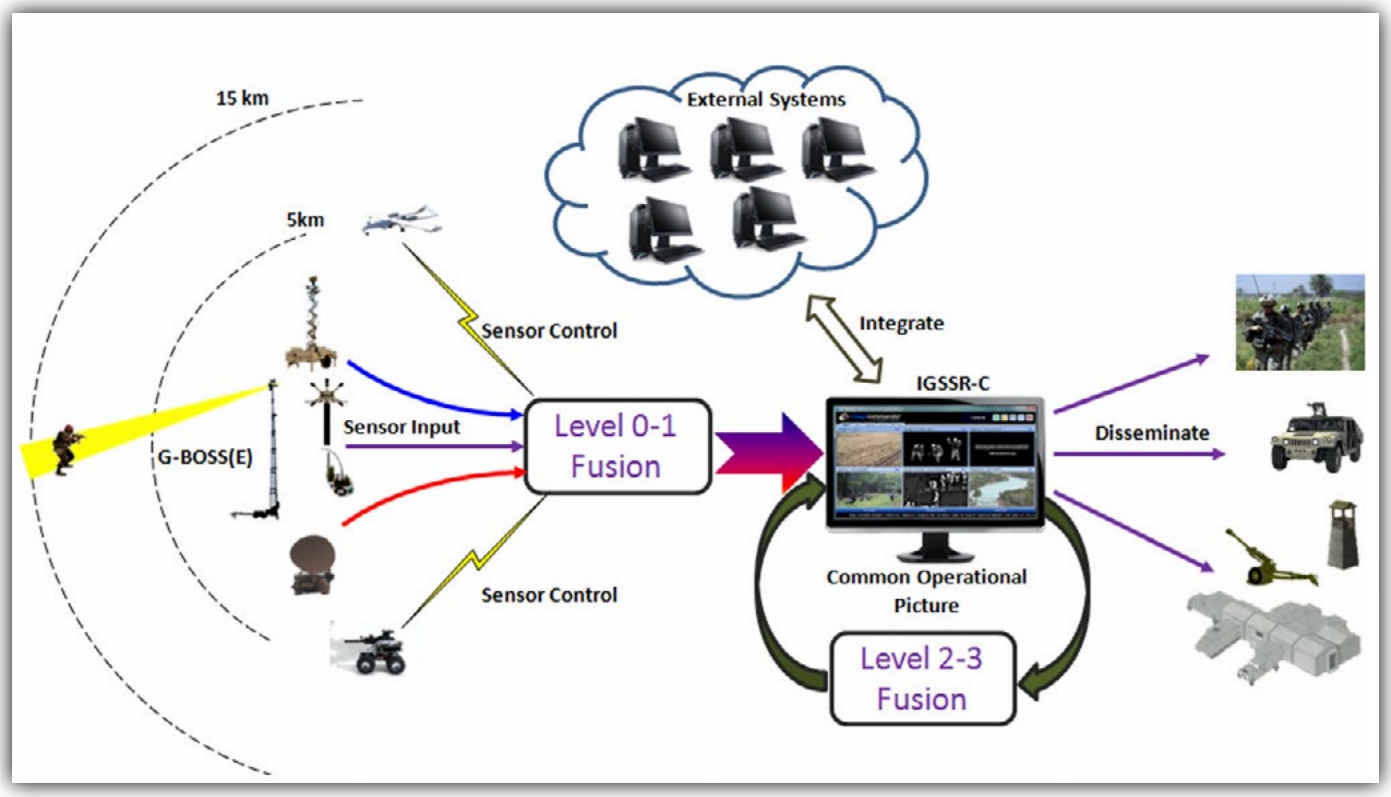
In September 2014, the DoD PSEAG, with support from USFFC, NWDC and CNIC, completed a first-of-its-kind Integrated Waterside Security Concept Demonstration (IWS-CD) at Naval Base San Diego, CA. This five-day IWS demonstration focused on the integration of Navy security forces ashore and afloat at both the organizational-and-systems level at a CONUS fleet concentration area. Ten different technologies were employed during the demonstration to address existing force protection capability gaps. These technologies ranged from non-lethal weapons designed to determine hostile intent, precision fire weapons well suited for close- quarters combat within a busy port, as well as advanced situational awareness tools and underwater detection systems to detect and interdict subsurface threats. The IWS-CD successfully showed the value of integrated technologies for Navy security forces ashore and afloat, and of identifying candidate technologies that show promise as new systems that can improve the efficiency and effectiveness of the Navy waterside security architecture.

Requirements

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

Integrated Ground Security Surveillance Response – Capability

This project provides a layered approach to integrate sensors, sensor systems and unmanned systems and to obtain automated fusion to create an in-depth security, surveillance and response Force Protection Common Operational Picture capability for fixed, semi-fixed or expeditionary elements in all operating environments. IGSSR-C's key component is a suite of software that achieves integration, fusion and interoperability.

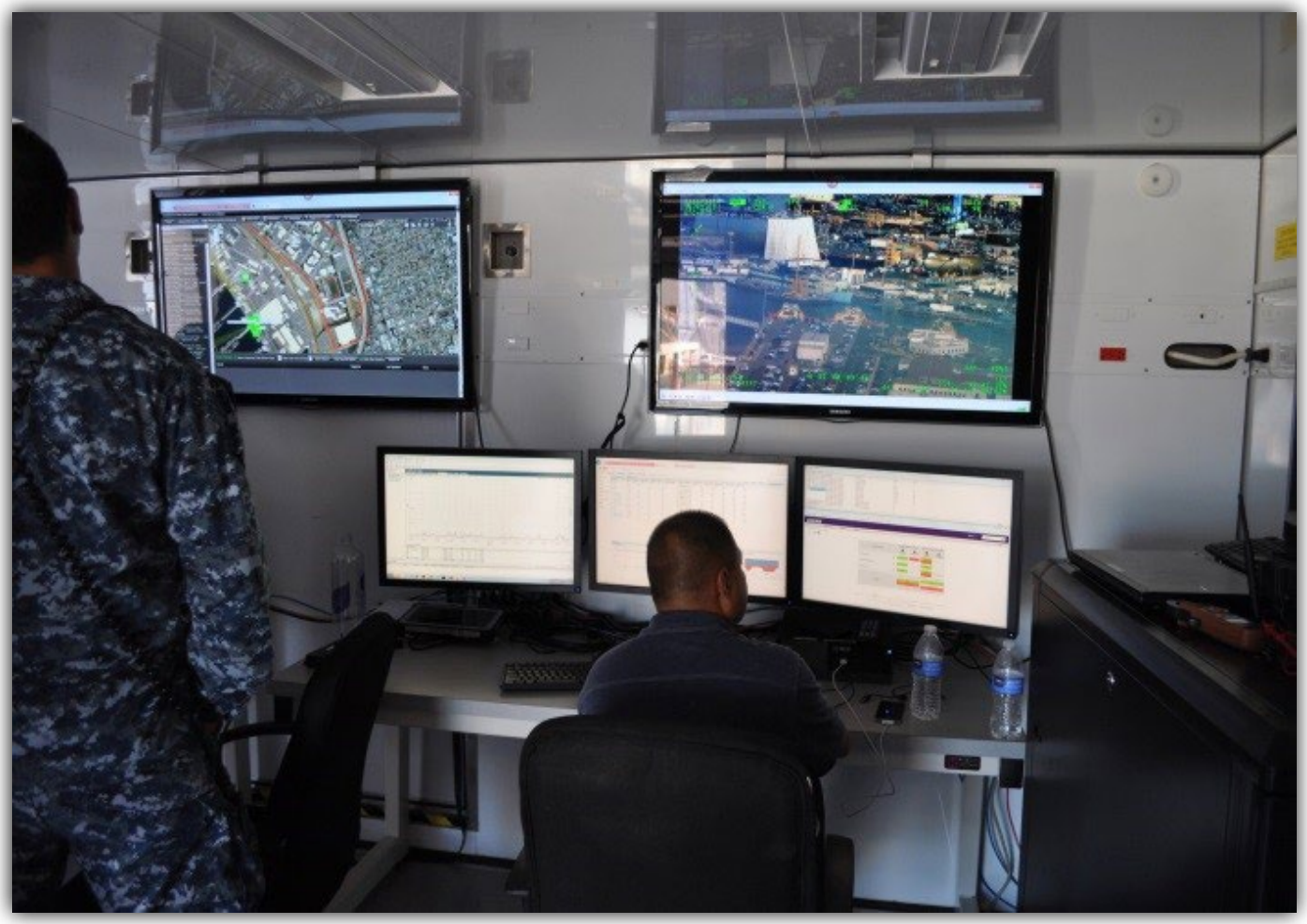


Requirements

- Interoperability ICD Approved (CARDS 1052) - MAR 2010; IGSSR-C CDD Approved (CARDS 6093) - SEP 2013

Joint Interface Group for Security Application Workspaces

Service Oriented Architecture framework for the collection and consolidation of data from disparate small to large security systems.



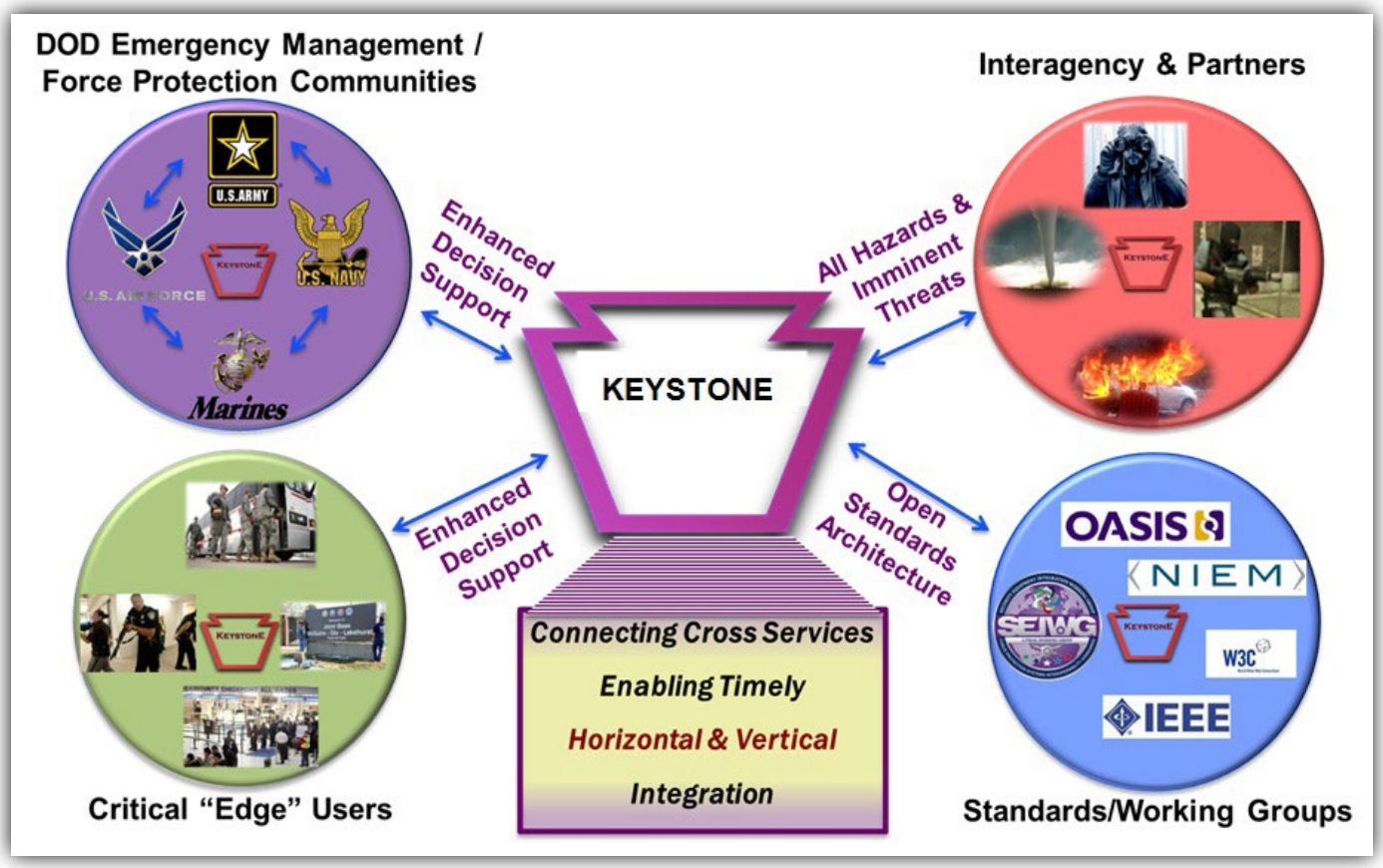
Requirements

- Integrated Unit, Base Installation Protection ICD, 13 July 07
- Integrated Base Defense Security System CDD, 17 Feb 2005, IGSSR-C CDD, JIGSAW SRD

JIGSAW
JOINT INTERFACE GROUP FOR SECURITY APPLICATION WORKSPACES

Keystone United States European Command Technical Demonstration

The Keystone EUCOM demonstration includes identifying applications from both the German Host Nation first responders and United States Army Garrison (USAG) Stuttgart to form an allied capability to integrate and correlate collection, analysis, reporting, and processing of OCONUS emergency management, force protection and threat information from existing systems. The integration software and user-level equipment will demonstrate information sharing; a proof of concept integration of German Host Nation systems, and software/cloud hosting to avoid creating a new stovepipe or need for new equipment.

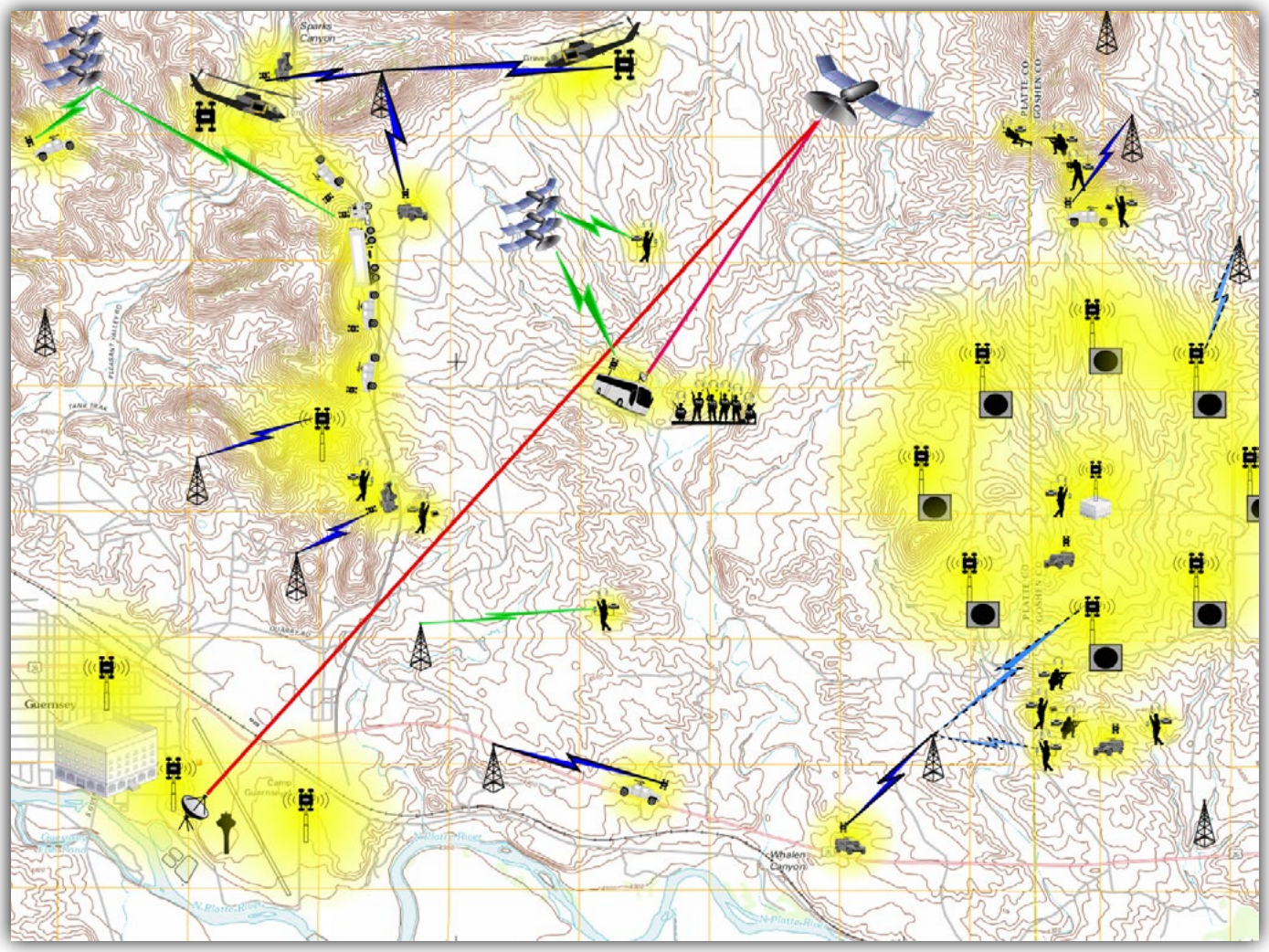


Requirements

- Final Recommendations of the Fort Hood Follow on Review" dated 18 August 2010; Washington Navy Yard Shooting Findings

Missile Field Defense Force Command, Control, Communications and Situational Awareness

Provides a redundant combination of physical layer and software application layers to provide a fail safe communications capability for stationary and on the move assets in the missile field (including blue force tracking).

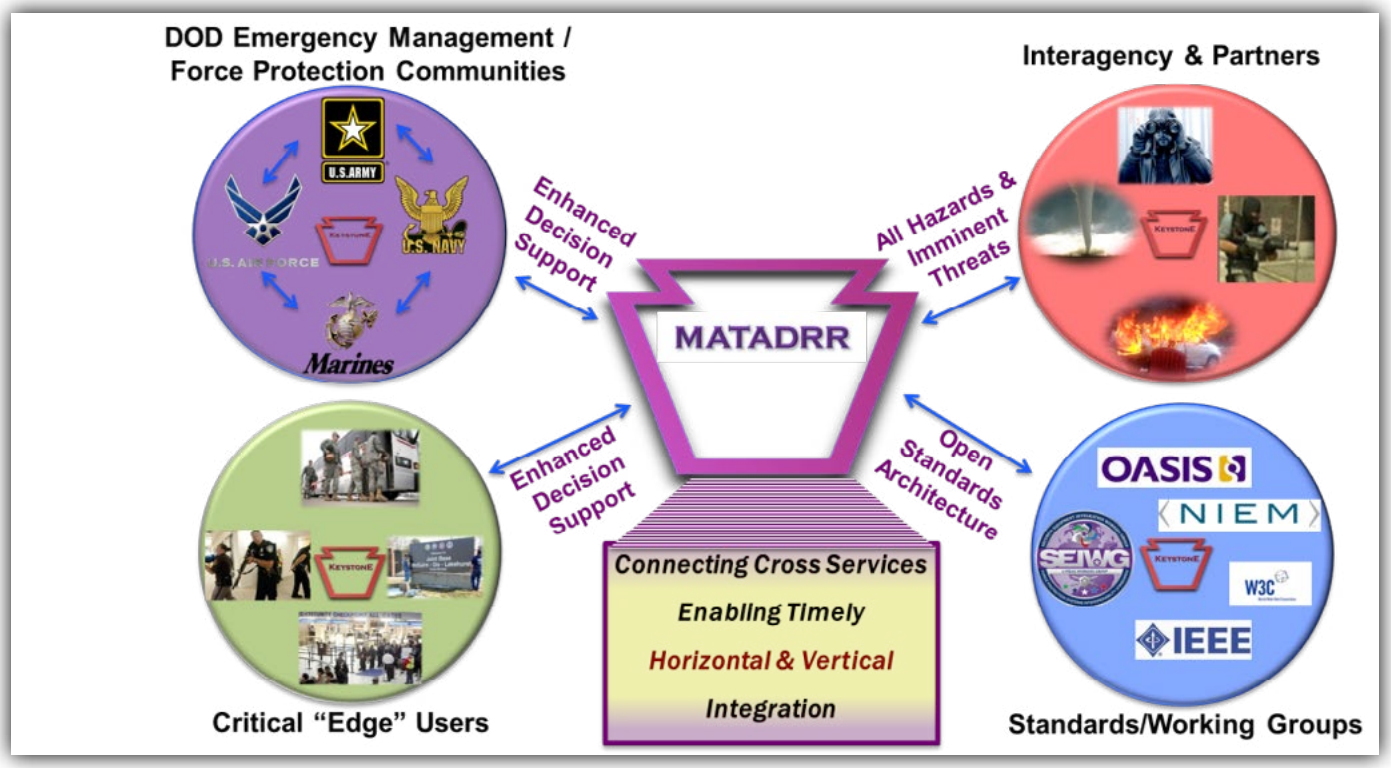


Requirements

- USAF Nuclear Security Roadmaps Needs; Mighty Guardian Results; Increase in security operations efficiencies

Mission Assurance, Threat Alert, Disaster Resiliency and Response

Information sharing across 'stove-piped' force protection and emergency management applications. Technical and operational demonstrations were conducted to validate the capabilities developed throughout the program.



Requirements

- JROCM– (VCJCS, 30 May 12) Capabilities Gap Assessment
- NC FY 13-17 IPL Priority 9: Information Sharing
- EC FY 13-17 IPL Priority 4: Information Sharing
- ARNORTH ONS - 11 November 2012

Near-shore Unified Tactical Response

An operational demonstration was conducted to improve common situational awareness by linking shipboard security teams, shore-based security and response boats.

Requirements

- Aligns to #3 Maritime Expeditionary Security Force (MESF) ICD gap, March 2008, MESF ROC & POE Jan 2010

Video Management System

The intent of this project is to evaluate available commercial-off-the-shelf Video Management System technology to meet Air Force requirements. If products successfully meet the requirements they will be recommended for inclusion on approved equipment lists. Qualification of a VMS provides an assessment capability to enhance response and provide increased situational awareness.

Requirements

- DoD Manual 5210.41M, Volume 2, Enclosure 3, paragraph 4.i. and subsequent paragraphs

DETECTION & ASSESSMENT

The ability to detect adversaries and assess their intentions is a basic physical security tenant. This capability area focuses on deficiencies in equipment used 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.

Photo Credit: US Department of Defense. 2013

Comparative Test and Evaluation: HazMatID ELITE and HazMatID 360

The objective of this effort is to complete a comparative test and evaluation of the Smiths Detection HazMatID ELITE and HazMatID 360. Once the capabilities of these systems are documented, they could be more accurately and effectively incorporated into a system of systems approach to security.

Requirements

- CENTCOM 2013 IPL 7 (STIPL 6.a and 6.d)
- Joint Service Explosive Ordnance Disposal ICD 1 June 2005
- Fleet Forces Command 2011 IPCL 1 & 6
- Navy Expeditionary Combat Command S&T Strategic Plan November 2011
- Integrated Unit, Base Installation Protection ICD January 2008
- DoD 2000.16 October 2006

Explosive Detection Equipment for Maritime Environment

The primary objective of this effort is to establish the capabilities and limitations of explosive detection systems and identify the system that most effectively meets the requirements set forth by Fleet Forces Command for use in maritime theaters of operation.

Seeker

XCAT

Fido X3

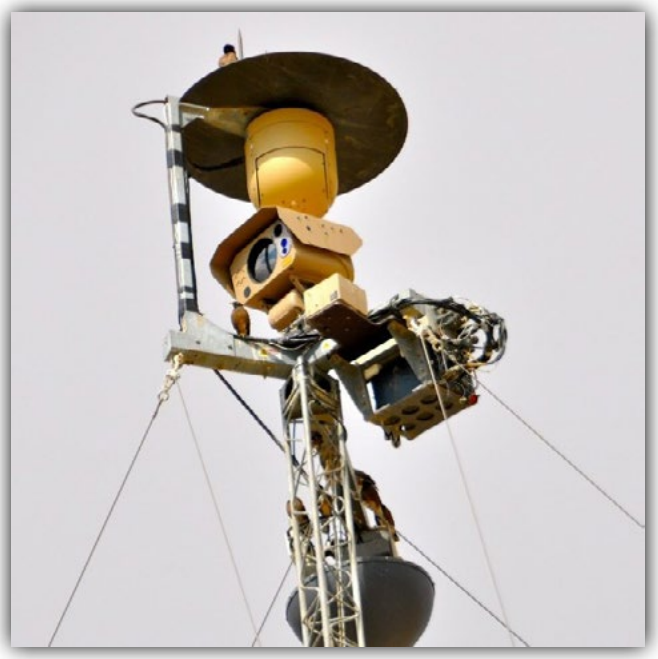
E3500

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

Ground-Based Operational Surveillance System (Expeditionary)

G-BOSS(E) is an expeditionary, ground-based, self-contained, multi-spectral sensor-oriented, persistent surveillance system used to greatly enhance situational awareness to counter physical security threats.

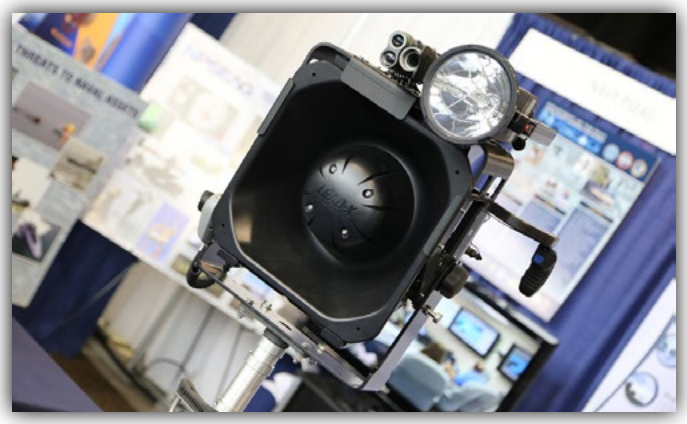


Requirements

- Capability Development Document for G-BOSS(E), Version 4.0, J8, 15 March 2012
- TRADOC validation of Army Annex to adopt USMC G-BOSS(E) CDD, 19 Aug 2013
- HQDA Deputy Chief of Staff G3/5/7 approved USMC G-BOSS(E) CDD adoption, designation as Joint Integration with CARD number is 06099, 6 May 2014

Hailing Acoustic, Laser and Light Tactical System

Provides a single operator with the ability to simultaneously control and operate multiple non-lethal deterrent devices to guard checkpoints, keep-out zones, and ship close-aboard areas.

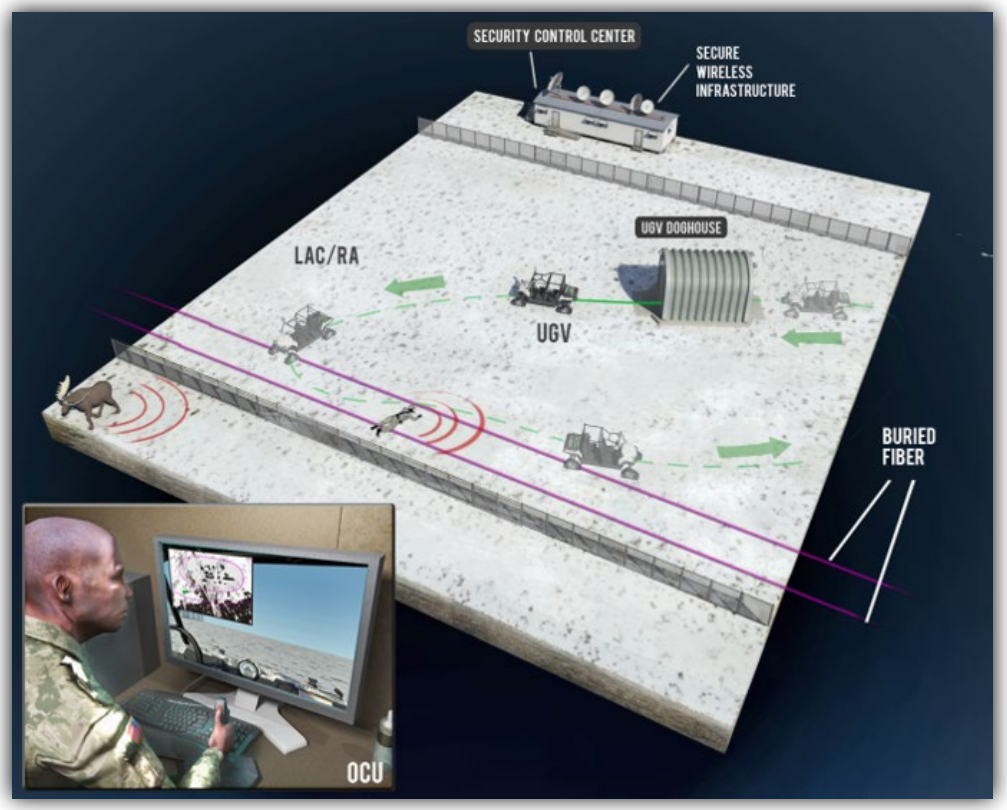


Requirements

- UONS #9309 [Counter Swarm]; UONS #9313 [Non-Lethal Weapons]; RFI N00178-11-Q-3900

Interceptor

The Interceptor capability consists of components that interoperate to enhance the detection and identification of threats to a secured area: the Linear Seismic Sensor, Broadband Acoustics Sensor, and Unmanned Ground Vehicle and addresses force protection capability gaps in the United States Northern Command and other Combatant Commands' areas of responsibility.

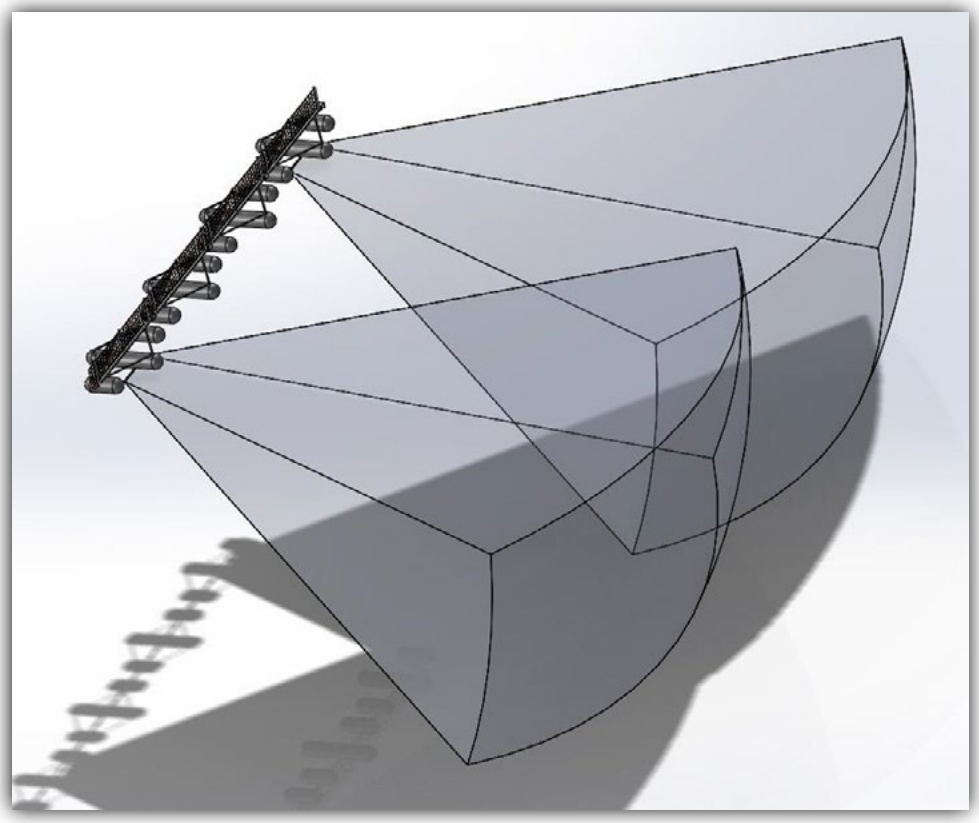


Requirements

- STRACOM Instruction 538-2

Long Range Threat Identification Sonar

Design, build, and demonstrate a sonar that can identify divers and nuisance targets at long range.



Marine Mammal Vigilance Localization

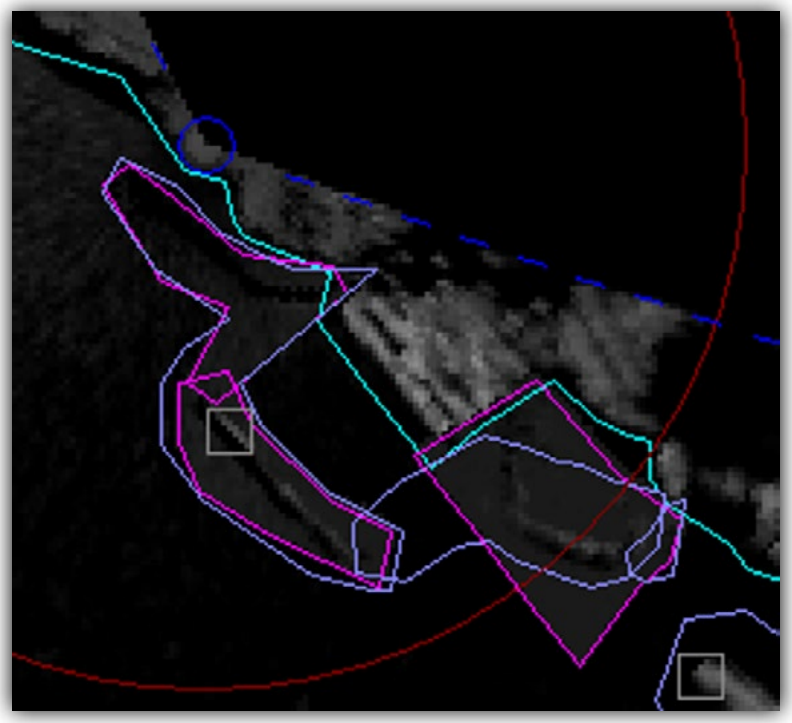
Develop a stand-alone, mobile, automated pen system to support 24/7 dolphin detection/localization operations that directly tie into existing Swimmer Interdiction Security Systems concept of operations.

Radar Assisted Area Protection

Testing and development of Interferometer radar technology to advance the capability to search, detect, track and identify Unmanned Aerial Systems (UAS) and direct-fire standoff threats for installation and asset defense.

Radar Processing Dynamic Structure Filter

This project will develop new techniques and algorithms using established processes (lower risk) to automate the filtering of permanent and/or semi-permanent floating structures detected by the Electronic Harbor.



Requirements

- EHSS CONOPS
- EHSS Key System Attributes
- EHSS Interface Control Documents

Radiological Detection System

The Radiological Detection System is intended to replace DoD's legacy Radiation Detection, Indication and Computation survey meters. This project provides a joint solution to increase capability and reduce life-cycle costs through the use of interoperable equipment with adequate sensitivity and common units of measure.

Requirements

- Capability Development Document (CDD) for the RDS, 3 July April 2014
- CBRN Sensors for Application on Unmanned (and Manned) Platforms Initial Capabilities Document (ICD), 3 October 2005
- CBRN Field Analytics ICD,12 January 2010. Countering Nuclear Threats (CNT) ICD, 25 April 2011
- Joint Publication 3-11. Operations in CBRN Environments, 26 August 2008
- DoD 3150.8-M, Nuclear Weapon Accident Response Procedures (NARP)
- Radiological Clearance Criteria Guidelines for Platforms and Materiel Memo, 16 December 2011

Comparative Test and Evaluation: Sensor Fusion Prototype Units

This effort selects the best performing Raman and infrared systems from a previous comparative testing for a systems integration effort.

Requirements

- JUONS CC-0255, IEDD ICD, NUONS CBRNE, IBDSS CDD, IUPBIP ICD, JSEOD ICD, NC 07-07

U.S. Navy Spike Weapon System Electro-Optical Seeker Upgrade

Develop and demonstrate an improved electro-optical seeker that will enable the Spike Weapon system to reliably track and engage AT/FP stationary and moving threat targets while operating in complex shorefront environments during day and low light conditions.

Requirements

- DEPSECDEF Memo of 23 Jan 2012 Subj: USCENTCOM/USPACOM Capability Enhancements
- COMUSFLTFORCOM NORFOLK VA 221715Z SEP 11 Subj: 2011 Fleet AT/FP IPCL
- CENTCOM JUONS CC-0506 Title: Smart Munitions for Aerostat Target Designation

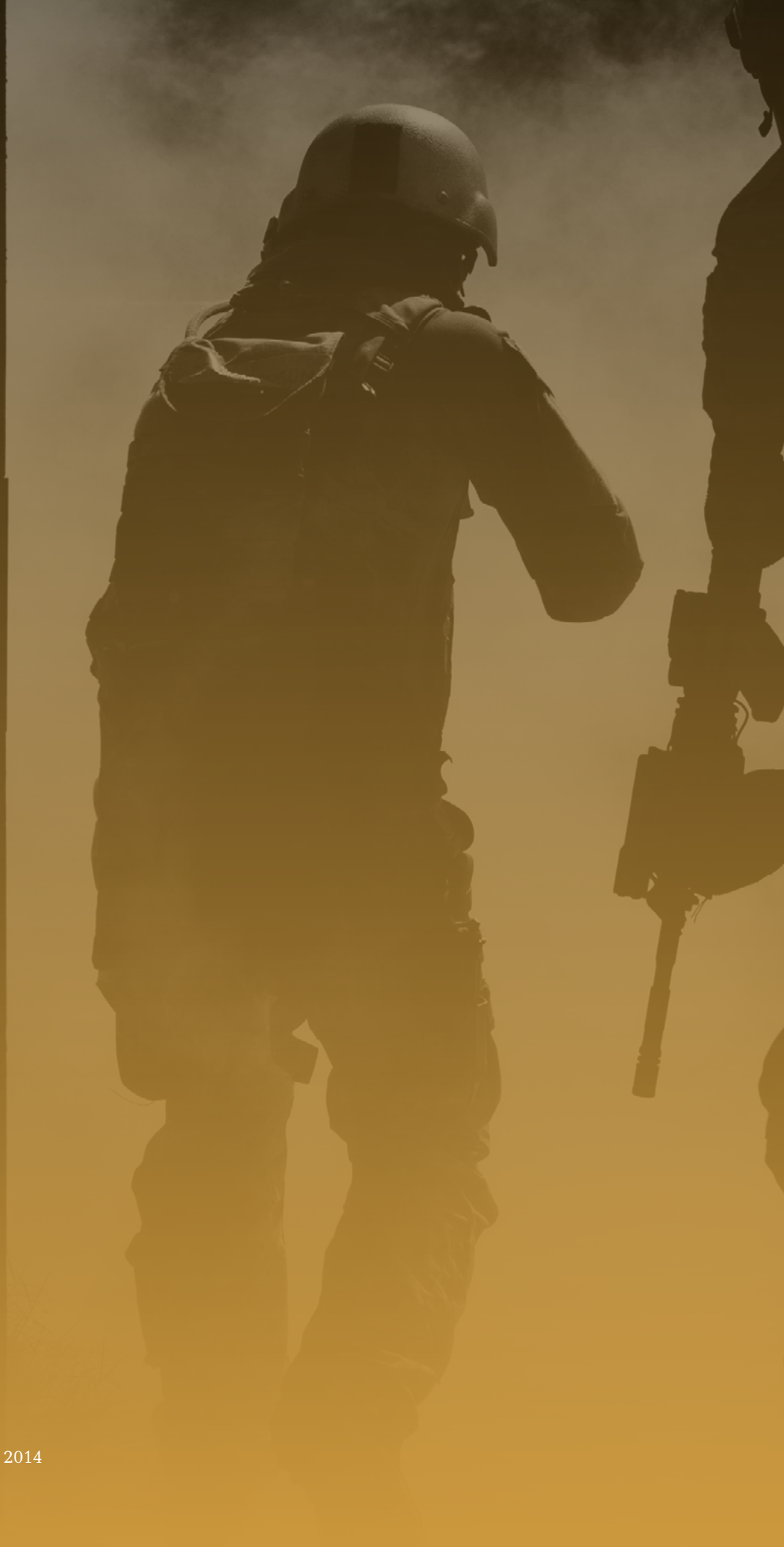


Photo Credit: US Department of Defense. 2014

PREVENTION

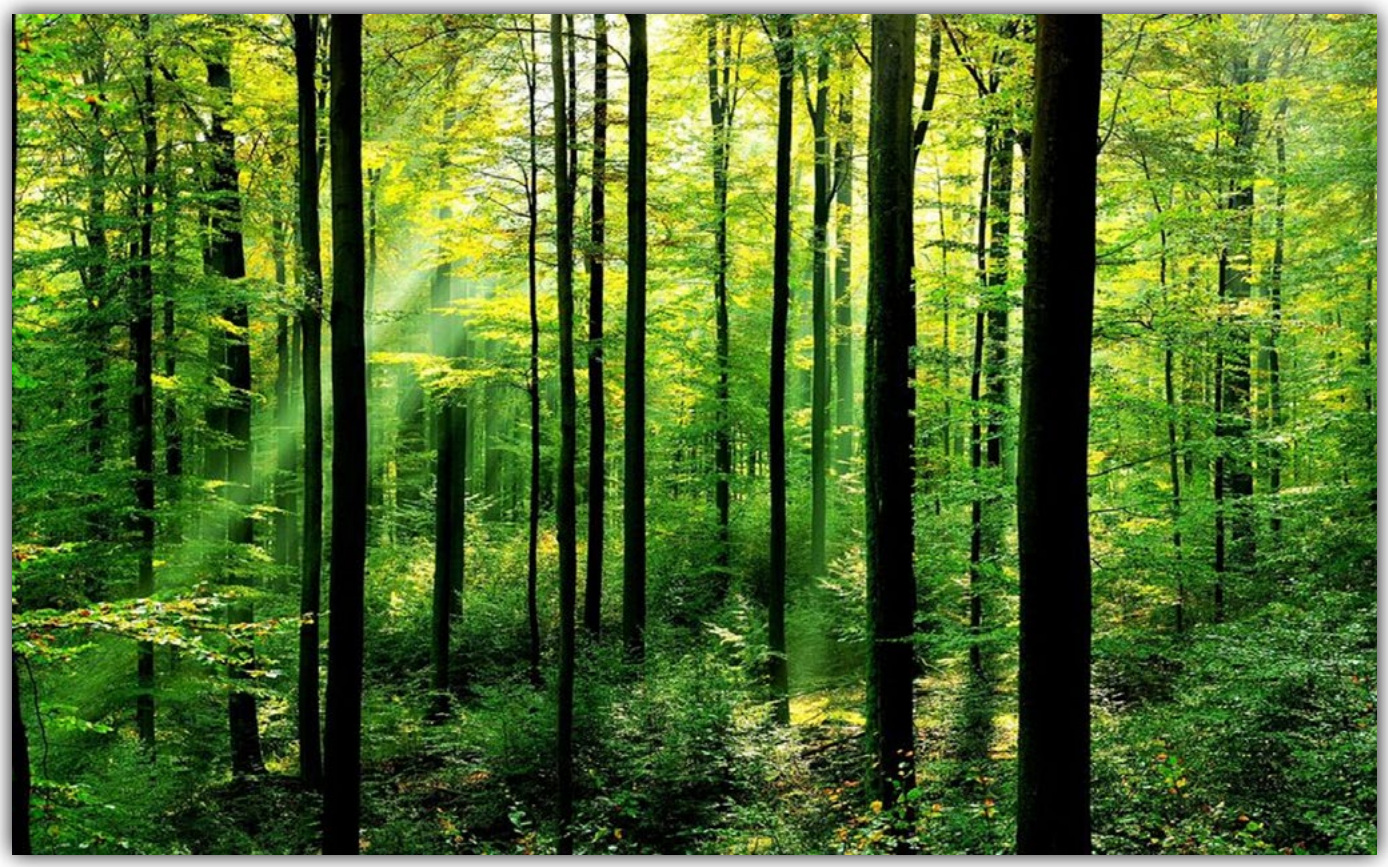
The security procedures taken to discourage an adversary from accessing weapons of mass destruction or gaining unauthorized access to critical assets are at the heart of prevention. This capability area focuses on broad spectrum, generic efforts that have the ability to influence multiple areas.

Marine Mammal Enhanced Interdiction

Develop an Enhanced Interdiction Grabber that would immediately stop an underwater intruder and allow the Swimmer Interdiction Security System to interdict multiple targets and hand off the intruder to a Harbor Security Boat.

Foliage Penetration Technology Evaluation

Identify and evaluate the most promising technologies for accessing human activity within heavily forested areas from ground level.



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 focuses on equipment (e.g., locks, doors) designed to delay or stop unauthorized entry / access to a specified / localized area.

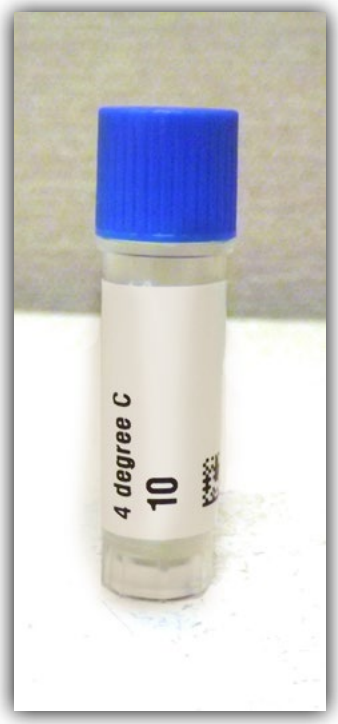
Photo Credit: US Department of Defense. 2014

Radio Frequency Identification Tagging for Items in Extreme Cold Storage

Radio-frequency identification is an automatic identification technology that combines inexpensive labels and radio infrastructure for tracking the identity and location of assets. This project improves physical security, inventory and accountability of infectious agents and toxins (IAT).

Requirements

- Inventory and accountability requirements from 42 CFR Part 73, 9 CFR Part 121, 7 CFR Part 331, DoD 5210.88/89, AR 50-1, and AR 190-17



APPENDICES

Administrative Points of Contact

PSEAG Chairman
Mr. Roderick Gillis
OASD(NCB/NM)
(703) 697-1124
roderick.e.gillis.civ@mail.mil

U.S. Army Representative
Mr. Eugene A. Smith
HQDA, OPMG
Phone: (703) 695-4210
eugene.a.smith4.civ@mail.mil

U.S. Navy Representative
Mr. Jeffrey Jones
ASN (E,I & E)
Phone: (703) 695-0461
jeffrey.r.jones2@navy.mil

U.S. Air Force Representative
Mr. John Salley
HQ AF/A4SX
Phone: (571) 256-0566
john.t.salley.civ@mail.mil

U.S. Marine Corps Representative
Mr. Charles "Tony" Pierce
HQ USMC (PS)
Phone: (703) 695-7203
Fax: (703) 614-6538
charles.a.pierce1@usmc.mil

DTRA Representative
Mr. Ernest (Rett) Sauls
HQ DTRA/OP-NSPS
Phone: (703) 767-7768
ernest.sauls@dtra.mil

Joint Explosive Detection Equipment Program Representative
Ms. Denice Lee
Naval Explosive Ordnance Disposal Technical Division
Phone: (301) 744-5143
denice.lee@navy.mil

SEIWG Chairman/PSEP T&E Coordinator
Mr. Rodney Rourk
USMC Systems Engineering
Phone: (843) 218-4375
rodney.rourk@navy.mil

List of Acronyms

Acronym	Definition
AEL	Approved Equipment List
AFMAN	Air Force Manual
AFNORTH	Air Force North
AR	Army Regulation
ASN (E,I & E)	Assistant Secretary of the Navy - Energy, Installations & Environment
AT/FP	Anti-Terrorism/Force Protection
CBRN	Chemical, Biological, Radiological and Nuclear
CBRNE	Chemical, Biological, Radiation, Nuclear, Explosive
CD	Concept Demonstration
CDD	Capability Development Document
CE	Continuous Evaluation
CECD	Continuous Evaluation Concept Demonstration
CFR	Code of Federal Regulations
CNIC	Commander, Navy Installations Command
CNT	Countering Nuclear Threats
COMUSFLTFORCOM	Commander, United States Fleet Forces Command
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial Off-The-Shelf
DEPSECDEF	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DIAC	Defense Installation Access Control
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	DoD Instructions
DSEA	Defense Security Enterprise Architecture
DTM	Directive Type Memorandum
DTRA	Defense Threat Reduction Agency
EDE	Explosive Detection Equipment
EHSS	Electronic Harbor Security Systems
ERCOP	Emergency Responder Common Operating Picture
FBI	Federal Bureau of Investigation

List of Acronyms

Acronym	Definition
FP	Force Protection
FY	Fiscal Year
G-BOSS(E)	Ground Base Operational Security System (Expeditionary)
HAF	Headquarters, Air Force
HALLTS	Hailing Acoustic Laser and Light Tactical System
HQ AF/A4SX	Headquarters, Air Force
HQDA	Headquarters, Department of the Army
HSPD	Homeland Security Presidential Directive
IA	Information Architecture
IATS	Infectious Agents and Toxins
IBD	Integrated Base Defense
IBDSS	Integrated Base Defense Security System
ICD	Initial Capabilities Document
IEDD	Improvised Explosive Device Defeat
IEEE	Institute of Electrical and Electronics Engineers
IFF	Identify Friend or Foe
IGSSR-C	Integrated Ground Security Surveillance Response- Capability
IMESA	Identity Management Engine for Security & Analysis
IPCL	Integrated Prioritized Capabilities List
IPL	Integrated Priority List
IUBIP	Integrated Unit, Base, Installation Protection
IWS	Integrated Waterside Security
JCTD	Joint Capability Technology Demonstration
JIGSAW	Joint Interface Group for Security Application Workspaces
JROCM	Joint Requirements Oversight Council Memorandum
JSEOD	Joint Service Explosive Ordnance Disposal
JUONS	Joint Urgent Operational Needs Statement
MATADRR	Mission Assurance Threat Alert Disaster Resiliency and Response
MESF	Maritime Expeditionary Security Force
NARP	Nuclear Weapon Accident Response Procedures
NIEM	National Information Exchange Model
NSWC IHEODTD	Naval Surface Warfare Center, Indian Head Explosive Ordnance Disposal Technology Division
NUONS	Navy Urgent Operational Needs Statement

List of Acronyms

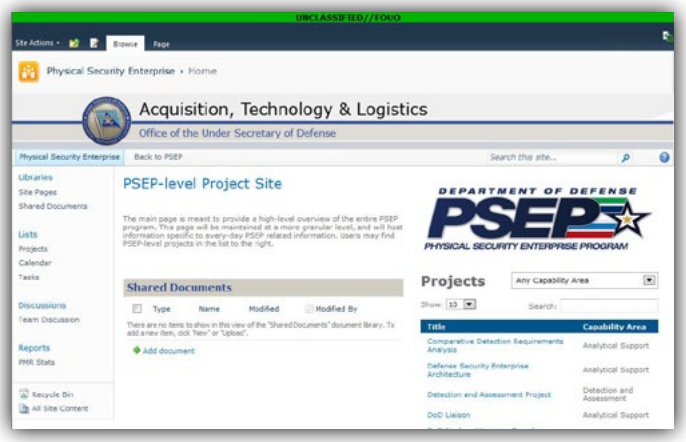
Acronym	Definition
NUTR	Near-shore Unified Tactical Response
NWDC	Navy Warfare Development Command
OASD(NCB/CB)	Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Chemical and Biological Defense
OASD(NCB/NM)	Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs/Nuclear Matters
OCONUS	Outside the Continental United States
ONS	Operational Needs Statement
OPMG	Office of the Provost Marshal General
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	Office of the Chief of Naval Operations Instruction
OPORDER	Operation Order
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
PMG	Provost Marshal General
POE	Projected Operational Environment
POR	Program of Record
PSE	Physical Security Equipment
PSEAG	Physical Security Enterprise & Analysis Group
RDT&E	Research, Development, Test and Evaluation
RFI	Request for Information
ROC	Regional Operations Center
S&T	Science & Technology
SECDEF	Secretary of Defense
SEIWG	Security Equipment Integration Working Group
SPAWAR	Space and Naval Warfare Systems Command
SSP	Strategic Systems Programs
UAS	Unmanned Aerial Systems
UONS	Urgent Operational Needs Statement
USAF	United States Air Force
USAG	United States Army Garrison
USCENTCOM	United States Central Command
USEUCOM	United States European Command
USFFC	United States Fleet Forces
USMC	United States Marine Corps

Acronym	Definition
USN	United States Navy
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
VCJS	Vice Chairman, Joint Chiefs of Staff
VMS	Video Management System

PSEAG Sharepoint Site

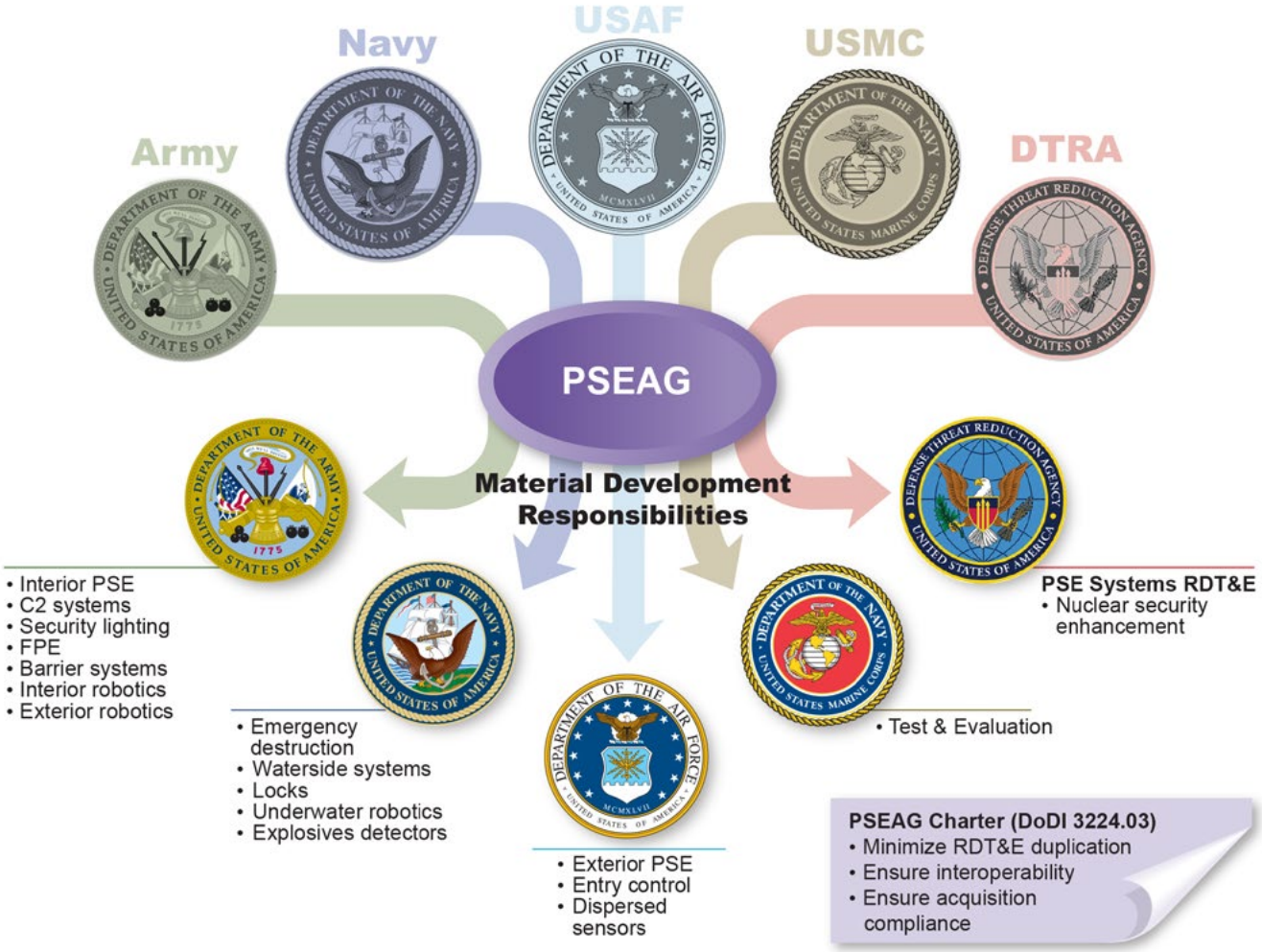
The Physical Security Enterprise & Analysis Group (PSEAG) developed a web portal (right) that will allow program managers, government representatives, support contractors and other approved users to access a wealth of Physical Security RDT&E-related information, upload reports, view PSEAG History projects 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.

This tool modernizes the once tedious paper process and standardizes the format for all future projects. The web portal also allows for users to enter monthly reporting and scheduling 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 system will also become an archive of project data and a useful tool for referencing old projects and reporting on historical data.



PSEAG Organization and Structure

The Physical Security Enterprise & Analysis Group (PSEAG) is composed 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)).



2014 RDT&E

RESEARCH, DEVELOPMENT, TEST & EVALUATION

PROGRAM SUMMARY