

DEPARTMENT OF DEFENSE  
PHYSICAL SECURITY ENTERPRISE & ANALYSIS GROUP

**PSEAG**



# STRATEGIC PLAN SUMMARY

2016-2021

# Physical Security is Global in Scope

## National Security Strategy

"No threat poses as grave a danger to our security and well-being as the potential use of nuclear weapons and materials by irresponsible states or terrorists."

"...include efforts to better fuse and share information and technology..."

**President Barack Obama**

February 2015

## DoD QDR 2014

"We will actively seek innovative approaches to how we fight, how we posture our force, and how we leverage our asymmetric strengths and technological advantages. Innovation is paramount given the increasingly complex warfighting environment we expect to encounter."

**Mr. Chuck Hagel**  
**Secretary of Defense**

2014

## Defense Security Enterprise Strategic Plan

"The DSE must have an effective arsenal of enterprise-level security policy and capabilities in order to protect DoD personnel, information, operations, resources, technologies, and facilities. Security practitioners must balance information sharing requirements with the need to protect and foster efficient use of DoD resources."

**Mr. Michael G. Vickers**  
**Under Secretary of Defense for Intelligence**

2013

## 2015 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT)

"The IAEA is very active in preventing the spread of nuclear weapons. In using nuclear technology, it is very important to ensure safety. Another very important area is the fight against nuclear terrorism. Nuclear terrorism is a real issue. The IAEA is functioning as a global platform to strengthen nuclear security efforts."

**Mr. Yukiya Amano**

**Director General, International Atomic Energy Agency (IAEA)**

May 2015



## DEPUTY SECRETARY'S MESSAGE



As the Deputy Assistant Secretary of Defense for Nuclear Matters, I oversee the development of Department-wide enterprise-level physical security solutions. My office is responsible for the DoD Physical Security Research, Development, Test and Evaluation (RDT&E) Program, governed by DoD Instruction 3224.03. The Physical Security Enterprise and Analysis Group (PSEAG) is the executing arm of the program.

The PSEAG proactively seeks to introduce new technologies, enhance legacy systems and evaluate selected commercial solutions to improve capabilities against asymmetrical, conventional and weapons of mass destruction threats. RDT&E dollars are scarce: we must ensure PSEAG-sponsored initiatives yield a positive return on investment by positioning technologies for transition to warfighters.

Mr. Rod Gillis, my Director of Nuclear Surety, Security, and Response and the PSEAG Chairman, manages daily PSEAG operations. Any organization must understand its current vision, mission, goals and priorities to guide its pathway into the future. Rod recently reviewed the PSEAG Strategic Plan for 2011-2015 to assess currency and relevancy to constantly changing domestic and international physical security environments and corresponding threats.



A summary of the PSEAG Strategic Plan for the years 2016-2021 is shown on the following pages. We have refreshed our vision, mission, goals, priorities and capability areas in view of the rapidly changing world landscape. Our objective is to deter, detect, delay, deny, and defeat (the five "D's") any foreign or domestic threat to our overall security, whether simplistic or technologically advanced. Not only are we concerned with the five "D's", but we are working in parallel with our partners to advance priorities for sharing information across multiple security pillars.

We seek to improve DoD physical security capabilities by collaborating with other government agencies and international partners to develop collective RDT&E solutions. New technology can reduce capability gaps, increase efficiencies and overall effectiveness, and influence policy modifications. Identifying and developing new solutions requires aggressive action. My professional goal is to ensure the PSEAG is the RDT&E organization of choice to strategically lead DoD physical security initiatives proactively through future decades.

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

# THE THREAT IS REAL



**Khobar Towers Bombing**  
Saudia Arabia  
June 26, 1996



**USS Cole Incident**  
Port of Aden, Yemen  
October 12, 2000



**Terrorist Attacks**  
Multiple Locations  
September 11, 2001



**Critical Nuclear Weapons Design Information Loss**  
Dr. A. Q. Khan Confession  
February 4, 2004



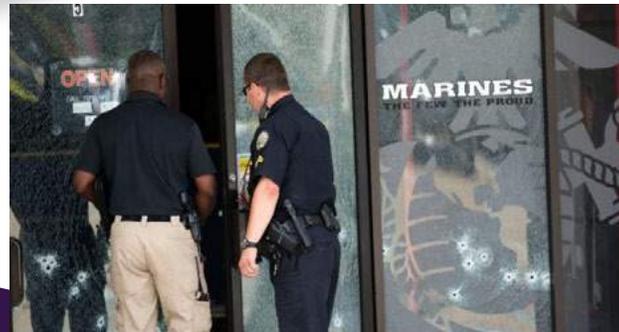
**Loss of Custody Incident**  
Minot AFB, ND  
August 29, 2007



**Mass Shooting**  
Fort Hood, TX  
November 5, 2009



**Mass Shooting**  
Washington, DC  
September 16, 2013



**Military Facilities Shooting**  
Chattanooga, TN  
July 16, 2015

# CHAIRMAN'S MESSAGE



In memory of  
**COL (RET) RODERICK E. GILLIS**  
 May 26, 1958 -  
 January 3, 2016



Since assuming my responsibilities as PSEAG Chairman in October 2014, I have gained a profound appreciation for the PSEAG's role in leading RDT&E innovations to improve physical security capabilities for warfighters.

I am privileged to work with security professionals representing the military Services and DoD agencies as part of daily PSEAG operations. Collectively, we execute ongoing technology projects to improve capabilities while planning RDT&E investments for future challenges at an enterprise-level. Upon assuming my role, I reviewed the 2011-2015 PSEAG Strategic Plan, focusing on strategic thoughts, future initiatives, investment priorities and improvements to PSEAG infrastructure. Over the past five years, the PSEAG achieved internal program goals by improving our management approach, streamlining governance structure, creating an automated internal database and public facing website, and modifying requirements review and approval processes.

Looking ahead to 2016-2021, we plan to continue the momentum created by broad and joint projects during the first half of this decade such as the Defense Installation Access Control (DIAC); Continuous Evaluation (CE); Defense Security Enterprise Architecture (DSEA); Mission Assurance, Threat Alert, Disaster Resilience and Response (MATADRR); and Integrated Waterside Security (IWS). The PSEAG primarily focuses on physical security challenges. However, we also realize information sharing among the Defense Security Enterprise's multiple security pillars is critical to improving our capabilities against various threat types. Sharing timely information between physical security and personnel security operating environments could possibly prevent catastrophic events in the future. We can also share internal DoD information with other government agencies and our international partners to further improve our capabilities.

Our new priorities for 2016-2018, on pages 8-9 of this Strategic Plan Summary, reflect potential initiatives to counter current and emerging threats. One of the PSEAG's strengths is our flexibility to adapt to new priorities when faced with evolving challenges. Although new priorities may surface, the ones listed in this summary are the starting points for our current outlook.

I look forward to continue working with DoD, other government agencies, industrial and academic professionals to provide physical security RDT&E solutions to ensure warfighting initiatives are highly efficient and effective.

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



## VISION

DoD's premier physical security RDT&E innovator for enterprise-level solutions to protect against asymmetrical, conventional and WMD 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.

## GOALS

### Develop Synergistic RDT&E Solutions

- Leverage RDT&E investments to achieve Physical Security enterprise-level solutions to deter, detect, delay, deny and defeat adversaries threatening nuclear and non-nuclear environments.

### Expand Information Sharing Across the Physical Security RDT&E Enterprise

- Ensure awareness of physical security information and initiatives, both within and external to the DoD, to reduce duplication, harmonize requirements and increase programmatic efficiencies.

### Achieve Interoperability for Physical Security Solutions

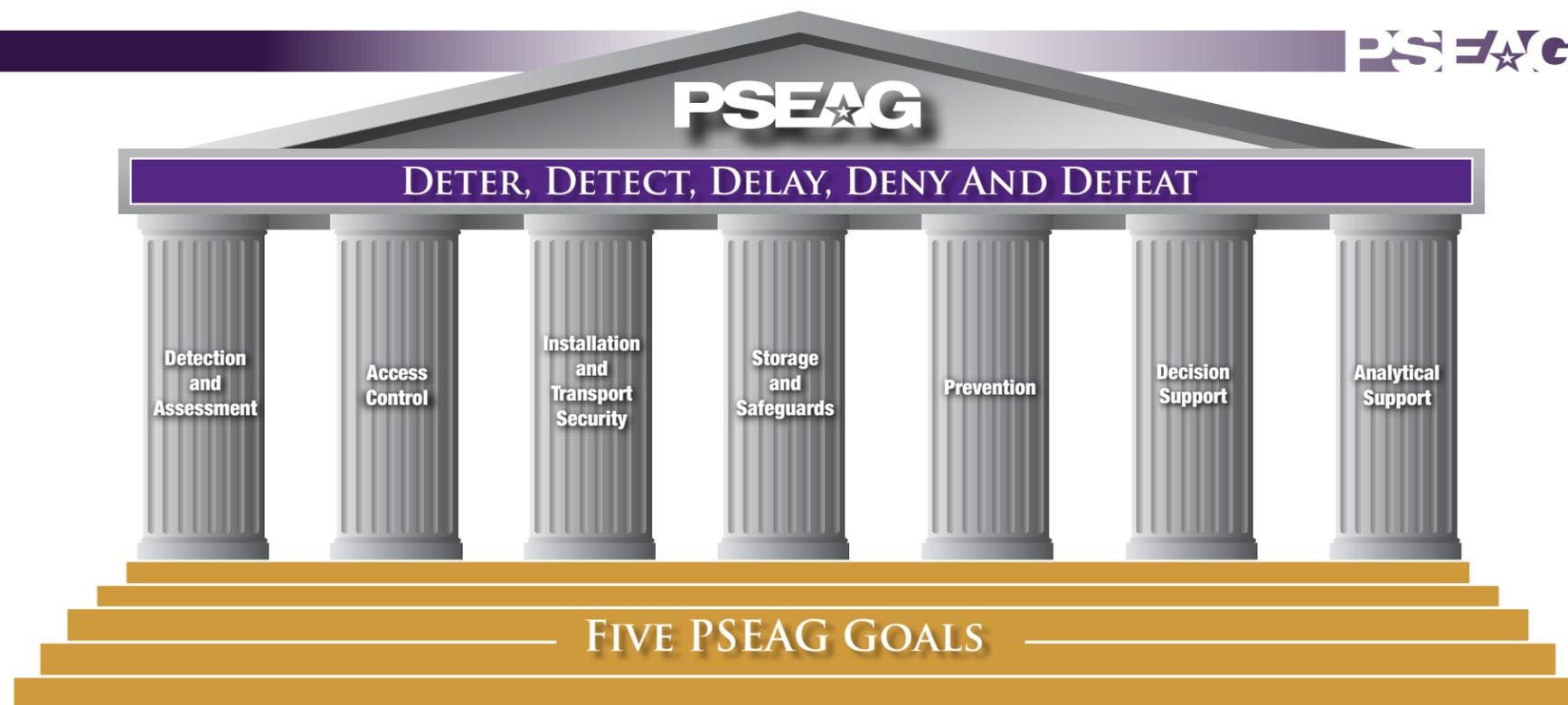
- Lead innovative Physical Security RDT&E to achieve cohesive architectures and systems of systems, adhering to government and appropriate industry standards for interoperability.

### Position RDT&E Solutions for Transition to Warfighters

- Improve transition of successful RDT&E innovations to DoD Acquisition agencies to provide improved warfighter capabilities against asymmetrical, conventional and WMD threats.

### Reduce Broad and Joint Capability Gaps

- Pursue DoD-wide Physical Security RDT&E initiatives to close broad Component and Joint capability gaps.



## Overview

The DoD Physical Security RDT&E Program, captured in the pictorial above and to the right, is built from the program's Vision, Mission, Goals and Capability Areas. Because of the RDT&E Appropriation Budget Activity types of annual funding the PSEAG receives, our Vision Statement looks 10 – 15 years into the future. The PSEAG Mission Statement sets forth what the PSEAG does today for physical security initiatives. Our five Goals reflect the core principles governing our approach and are likely to remain unchanged during the next five to ten years – in essence, our foundation. The seven Capability Areas compose our central organizing architecture - in essence, the columns - enabling us to better analyze, prioritize and fund our solutions. The updated Vision, Mission, Goals and Capability Areas work in parallel to ensure the PSEAG is postured to transition RDT&E successes into warfighter capabilities. Our Priorities, shown on pages 8 and 9, describe our anticipated investments over the next 2-3 years.

## CAPABILITY AREAS

### Detection & Assessment

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

### Access Control

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

### Installation & Transport Security

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

### Storage & Safeguards

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

### Prevention

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

### Decision Support

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

### Analytical Support

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

# PRIORITIES

## COUNTER CURRENT AND EMERGING THREATS

Today’s asymmetric and WMD threats do not respect geographical boundaries – they strike anywhere and at any time. These threats endanger personnel, installations and equipment protected by physical security systems. The ever-evolving threats shown below challenge the ability of physical security systems to achieve Mission Assurance goals and objectives.



During FY 16-18, the PSEAG will focus on countering these current and emerging threats:

- **Unmanned Aerial Systems (UAS)** – advance countermeasures to evolving UAS threats, including sensor, weapon, WMD or explosive-based payloads, to holistically defend protected areas
- **Insider Threat** – provide innovative solutions to increasingly demanding challenges generated by malicious insiders
- **Cyber** – sponsor RDT&E initiatives to ensure physical security systems cyber-resiliency
- **Chemical, Biological, Radiological, and Nuclear (CBRN)** – continue to expand CBRN detection and situational awareness into physical security functioning domains
- **Stand Off Platforms** – ensure physical security against threats operating beyond traditional defended area engagement zones
- **Low-level threats** – explore unique physical security scenarios that can challenge public confidence in physical security systems’ ability to achieve Mission Assurance

## CLOSE CAPABILITIES GAPS

The PSEAG focuses its RDT&E resources on improving capabilities across the entirety of the physical security spectrum. Challenges run the gamut from fence lines, to gates, to lighting, to common operating pictures, to integrating ashore and afloat security, to unique nuclear weapon storage and safeguard procedures, and to sharing information across the Defense Security Enterprise. The PSEAG is using Integrated Project Team (IPT) initiatives to close capability gaps. IPT’s create multiple Service collaboration early in the requirements process, increasing the probability of eventual Joint requirements.



During FY 16-18, the PSEAG will improve these critical capability areas:

- **Detection and Assessment** – improve the defense of protected areas through enhanced target recognition
- **Improved Personal Identity Reliability for Access Control** – integrate technologies to increase credential validation accuracy
- **Fusing of Information** – synchronize information from disparate sources across multiple mission areas to improve situational awareness

DEPARTMENT OF DEFENSE  
PHYSICAL SECURITY ENTERPRISE & ANALYSIS GROUP



## OPERATE IN NON-TRADITIONAL ENVIRONMENTS

Joint Publication 1-02 defines Physical Security (PS) as "...that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft." The PSEAG traditionally invests in large-scale projects for protecting major installations, nuclear and non-nuclear assets, infrastructure and platforms, including land combat systems, aircraft and ships. DoD components increasingly operate in atypical environments: PS personnel, systems and architectures need to adapt accordingly to provide Mission Assurance in varied environments.



During FY 16-18, the PSEAG will improve PS operations in nontraditional environments:

- **Expeditionary environments** – develop RDT&E technologies to meet dynamic physical security demands of bare base environments
- **Non-Standard Installations** – balance PS equipment, systems and practices to meet challenges unique to usually smaller and unique installations
- **Strategic Transportation** – pursue RDT&E initiatives to assure protection during movement phases of high value assets

## SHARE INFORMATION

The PSEAG facilitates increased information sharing across physical security communities of interest by leveraging recurring security meetings and program management reviews into opportunities to exchange relevant updates. Periodic PSEAG and external organization discussions assist to synchronize information across DoD, other US government agencies (OGA) and international partners, minimizing duplication and creating synergistic opportunities.



During FY 16-18, the PSEAG will increase these information sharing activities:

- **PSEAG All Hands Meetings** – sponsor quarterly to semi-annual sessions or management reviews to consistently share information
- **Force Protection Equipment Demonstrations** – explore the opportunity to reinstate a fourteen year tradition of hosting several hundred vendor demonstrations of commercial-off-the-shelf (COTS) products to government leaders
- **Technology Exchanges** – coordinate periodic meetings with OGA and international partners

## INCREASE PHYSICAL SECURITY EFFICIENCIES

As the envisioned DoD's premier RDT&E program for physical security, the PSEAG has a critical role to develop and monitor standards and interface control documents; test and evaluate new and legacy systems and COTS products; and research improvements to components common to physical security systems benefiting the entire community of interest. During FY 16-18, the PSEAG will:



- **Maintain currency of PSEAG standards** – incorporate evolving standards and best practices to ensure DoD compliance and increase efficiencies
- **Evaluate COTS products for selected threats** – support user requirements by evaluating products for quick turnaround solutions to meet high – profile threats
- **Reduce False and Nuisance Alarms** – seek common causes and solutions to these ever-present problems in physical security systems
- **Conduct Software Independent Verification & Validation (IV&V)** – ensure new and evolving software is reliable and meets user requirements
- **Review Legacy Systems** – conduct periodic evaluations of select existing capabilities to ensure performance standards are met relative to evolving threats

# PSEAG SUCCESS



Explosive  
Detection Equipment

DoD Lock  
Program

SEIWG Standards and  
Interface Control Documents

1990

1985

Mobile Detection, Assessment  
and Response System

Non-Intrusive  
Imaging Systems

Beginning of Force  
Protection Equipment  
Demonstrations

1995

2000

Battlefield  
Anti-Intrusion System

Lighting Kit,  
Motion Detector

ICBM Security  
Modernization Program

Defense Installation  
Access Control Working Group

2014

2005

Continuous Evaluation  
Concept Demonstration

Joint Force Protection  
Advanced Security System

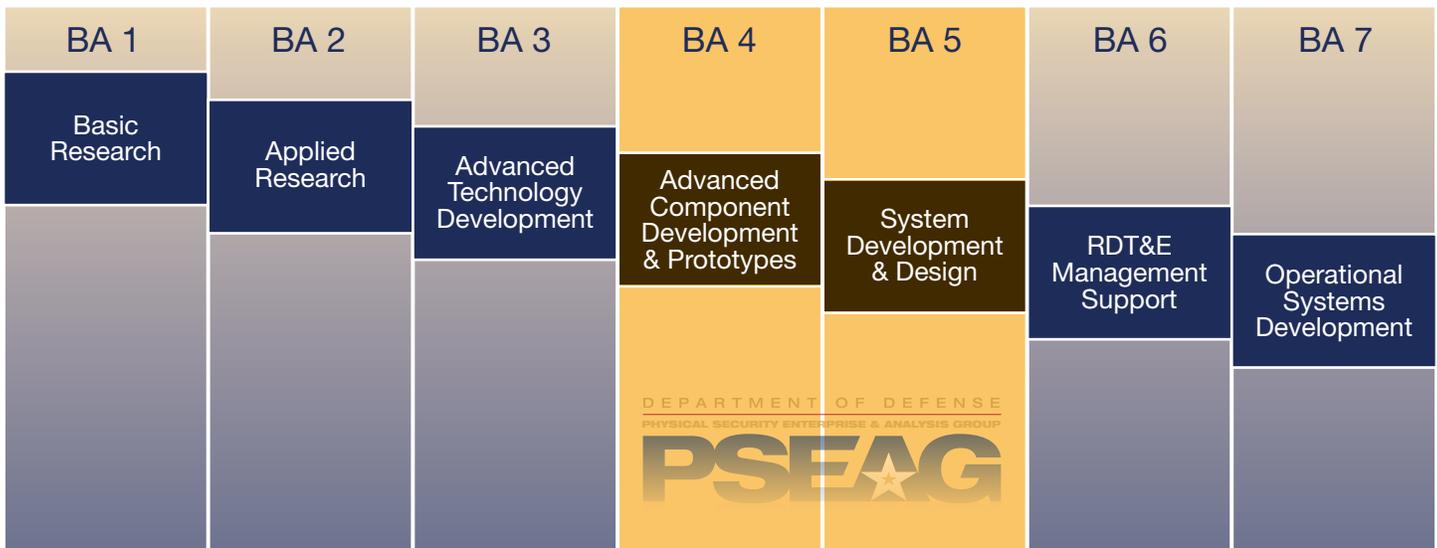
# PSEAG HISTORY

The Physical Security Enterprise and Analysis Group (PSEAG) is the DoD’s Research, Development, Testing and Evaluation (RDT&E) focal point for physical security solutions to broad and joint department-wide capability gaps. The PSEAG has managed over 400 projects, each typically ranging from one to three year periods of performance. Numerous PSEAG-led projects have successfully resulted in Programs of Record (PoR) or in some other way advanced physical security technology.

Formed in 1976 to pursue more effective solutions to DoD physical security challenges, the PSEAG originally executed its responsibilities under the Director of Defense Research and Engineering (DDR&E) in the Office of the Secretary of Defense (OSD). At that time, funding for physical security equipment remained with the Military Services. The PSEAG focused on finding physical security issues common to all of the Military Services, assisting the requirements harmonization process and reducing duplicate RDT&E initiatives among the Military Services.

The Fiscal Year 1989 Appropriations Act consolidated physical security funding for the Services at the OSD-level – substantially changing the role of the PSEAG – and the PSEAG moved to the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)) Land Warfare office. For two years (2003-2005), Headquarters, Air Force’s A7S office managed the PSEAG. In 2005, the PSEAG moved under the Office of the Assistant Secretary of Defense (Nuclear, Chemical, Biological)/Nuclear Matters (OASD(NCB/NM)).

Today, the PSEAG focuses on developing programs of record, maturing possible technology insertions, or evaluating and demonstrating commercial-off-the-shelf (COTS) products. DoD budget activities 4 (advanced component development and prototypes (ACD&P)) and 5 (system development and demonstration (SDD)) fund PSEAG projects as shown in the accompanying diagram.

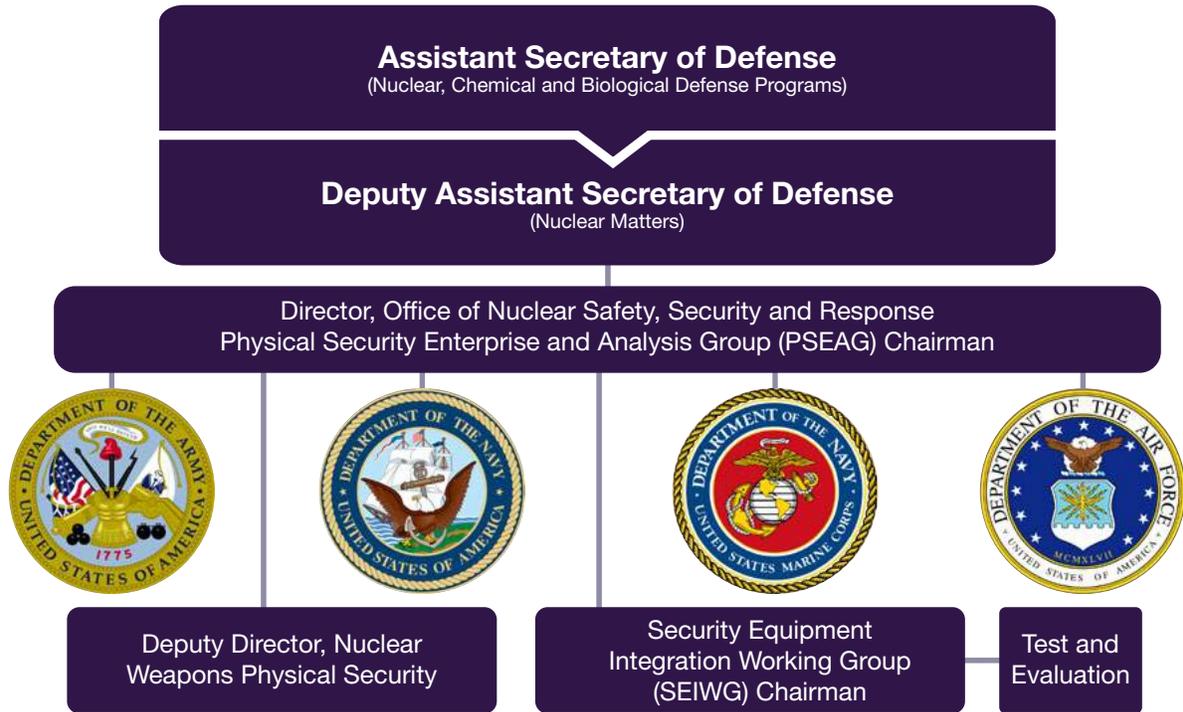


DoD Budget Activities

Today, PSEAG proactively engages at the enterprise level within DoD, with other government agencies, and international partners. This integrated and comprehensive approach includes both equipment solutions and necessary analytical underpinnings to solve capability gaps and improves performance-based technology assessments.

The PSEAG membership consists of the PSEAG Chairman, representatives from each Military Service and the Security Equipment Integration Working Group (SEIWG) Chairman. The PSEAG Chairman leads, monitors and evaluates overall PSEAG operations and provides oversight for all the Services, Agencies and organizations that execute these projects throughout the annual cycle.

# POINTS OF CONTACT



**PSEAG Chairman**

**MR. WAYNE P. HUDSON**

Principal Director, Deputy Assistant Secretary of Defense for Nuclear Matters  
Office of the Deputy Assistant Secretary of Defense for Nuclear Matters  
The Pentagon  
Room 3B884  
Washington DC 20301-3050  
Office: 703-697-2953  
[wayne.p.hudson.civ@mail.mil](mailto:wayne.p.hudson.civ@mail.mil)

**Deputy Director, Nuclear Safety, Security and Response**

**TROY A. ROBERTS, COL, USAF**

Office of the Deputy Assistant Secretary of Defense for Nuclear Matters  
The Pentagon  
Room 3B884  
Washington DC 20301-3050  
Office: 703-697-5393  
DSN 227-5393  
[troy.a.roberts1.mil@mail.mil](mailto:troy.a.roberts1.mil@mail.mil)

**U.S. Army PSEAG Representative**

**MR. GENE SMITH**

Chief, Physical Security  
Office of the Provost Marshal General  
2800 Army Pentagon  
Washington, DC 20310  
Office: 703-695-4210  
[eugene.a.smith4.civ@mail.mil](mailto:eugene.a.smith4.civ@mail.mil)

**U.S. Air Force PSEAG Representative**

**MR. JOHN SALLEY**

HQ AF/A7SX  
1800 Air Force Pentagon  
Washington, DC 20330-1800  
Office: 571-256-0566  
DSN 260-0566  
[john.t.salley.civ@mail.mil](mailto:john.t.salley.civ@mail.mil)

**SEIWG Chairman**

**MR. RODNEY ROURK**

SPAWAR Systems Center Atlantic  
USMC Systems Engineering Branch  
Office: 843-218-4375  
[rodney.rourk@navy.mil](mailto:rodney.rourk@navy.mil)

**U.S. Navy PSEAG Representative**

**DR. J. R. JONES (JEFF)**

Branch Chief, Physical Security  
DUSN(P) Security Directorate  
Department of the Navy  
Washington, DC 20350-1000  
Office: 703-601-0480  
DSN 225-0480  
[jeffrey.r.jones2@navy.mil](mailto:jeffrey.r.jones2@navy.mil)

**U.S. Marine Corps PSEAG Representative**

**MR. TONY PIERCE**

Head, Security Technologies Section  
Physical Security & Electronic Security Systems  
Headquarters Marine Corps  
Security Division, (PS)  
Security Branch (PSS)  
3000 Pentagon  
Room 4A324  
Washington, DC 20350-3000  
Office: 703-695-7202  
DSN 225-7202  
[charles.a.pierce@usmc.mil](mailto:charles.a.pierce@usmc.mil)