

DEPARTMENT OF DEFENSE
PHYSICAL SECURITY EQUIPMENT ACTION GROUP

PSEAG

**STRATEGIC PLAN SUMMARY
2011 - 2015**



TRANSITIONING TO THE FUTURE



The Department of Defense has the responsibility to protect its personnel, installations, and resources from various threats throughout the world. A critical component for that responsibility is the development of physical security technologies advancing capabilities that the Services and DoD Agencies deploy to protect assets in both conventional and nuclear asset environments. The Physical Security Equipment Action Group, known as the “PSEAG”, has accomplished the mission of developing physical security technologies since 1976.

In FY89, the Services’ Physical Security Equipment (PSE) Research Development Test and Evaluation (RDT&E) funding was consolidated under a single entity in the Office of the Secretary of Defense (OSD) to better achieve the objectives of harmonized requirements, interoperability, and prevention of technology duplication. Since 2005 the PSEAG mission has been led by the Office of the Assistant Secretary of Defense for Nuclear, Chemical and Biological Programs/ Nuclear Matters (OASD (NCB/NM)).

The PSEAG leverages the natural synergy that resides in common technology solutions, when applicable, for both conventional and nuclear physical security requirements. In essence, we are leveraging important and scarce RDT&E dollars to ensure our best return on investment. Looking to the future, the PSEAG will continue to be a leader in developing security technologies. We are actively engaged in a security technology Outreach Program that intersects with DoD organizations, such as the Technical Support Working Group (TSWG), Joint Improvised Explosive Device Defeat Organization (JIEDDO), and Joint Non-Lethal Weapons Directorate (JNLWD) as well as other organizations external to DoD, to include the Department of Energy (DOE), National Nuclear



Security Administration (NNSA), Department of Homeland Security (DHS), and national laboratories. Sharing lessons learned, best practices, and collaborating on a continuous basis with partners will increase mission effectiveness and efficiency.

An emerging physical security technologies mission we are also engaged in is Countering Nuclear Threats (CNT). The PSEAG will focus on synergies from the two mission areas of physical security and CNT to improve performance and make more efficient use of resources.

As we look to the future, the PSEAG will continue to be a leader of physical security RDT&E as it has for the past two decades. We will continue to accomplish our mission while serving as excellent stewards of resources. As you read this summary, I am confident you will learn more about the PSEAG and what our plans are to meet future physical security challenges.

Thomas J. Whittle, PE
PSEAG Acting Chairman
May 3, 2011



VISION

To be DoD's premier RDT&E provider to warfighter organizations to mitigate physical security vulnerabilities and close identified capability gaps; serve as the catalyst for developing, demonstrating and evaluating interoperable solutions for DoD-wide capability requirements; and work in close collaboration with other government agencies to achieve and sustain interoperability.

“Employing Technology to Protect our Nation: Our renewed commitment to science and technology – and our ability to apply the ingenuity of our public and private sectors toward the most difficult foreign policy and security challenges of our time – will help us protect our citizens and advance U.S. national security priorities. These include, for example, protecting U.S. and allied forces from asymmetric attacks...”

– National Security Strategy (May 2010)

OUR FOCUS:

- Deter, detect, delay, deny and defeat our adversaries
- Protect our forces and supporting infrastructure
- Leverage technology to out-pace the threat
- Partner and progress in order to maintain supremacy

MISSION

Harmonize physical security material requirements to develop, demonstrate and evaluate emerging interoperable RDT&E solutions. Focus on closing DoD-wide capability gaps through investments resulting in programs of record, technology insertions, or commercial off-the-shelf solutions. Leverage solutions across nuclear and conventional physical security environments as well as counter nuclear threats.

CURRENT PSEAG THRUST AREAS:

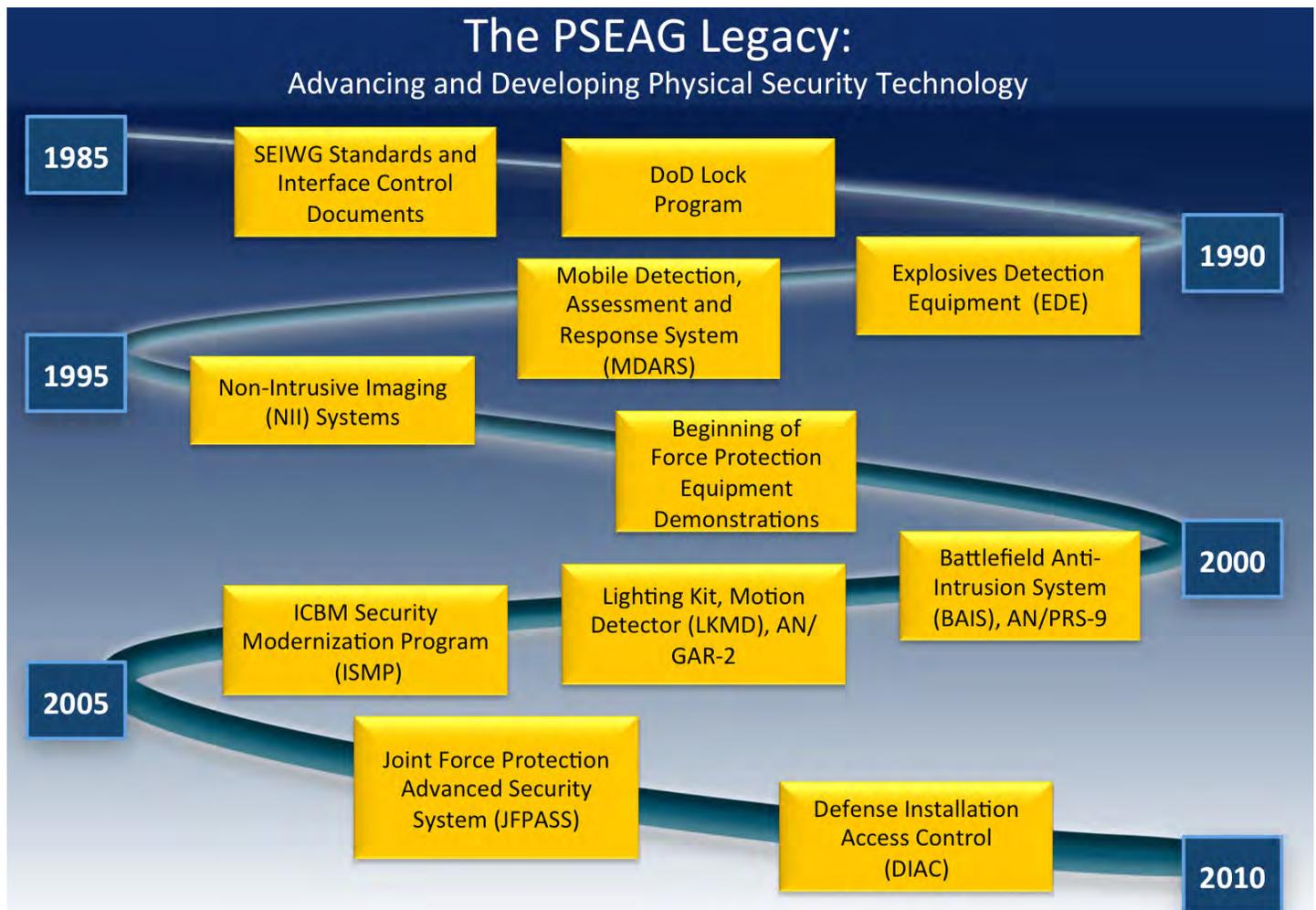
- Nuclear Weapons Physical Security
- Conventional Physical Security
- Countering Nuclear Threats

FY 2011 MAJOR INITIATIVES:

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



PSEAG SUCCESSES



DoD Locks, Safes, Vaults, Seals, and Containers Program

The "DoD Lock Program" was designated by the Secretary of the Defense in 1976 (DoD Directive 3224.3) to provide management, operation, and support functions for development, testing, and procurement of locking devices, security containers, and related delay devices. The Lock Program, administered initially by the Army and currently by the Navy, was assigned to the Navy in 1984 and has since then been in the Navy for three decades.

The RDT&E team is known for its highly effective and innovative solutions and those benefiting include: all DoD Services, the Department of Energy (DOE), the Department of Justice (DOJ), the National Intelligence (DNI), General Services Administration (GSA), and Nuclear Regulatory Commission (NRC). The Field Support Hotline to provide quick hardware selection, requirements, training, and technical support.

The DoD Lock Program has been successful in its tenure, to include the Internal Locking Device (ILD), on March 6, 1991, to be "an padlock and hasp requirement" and today it is used to secure nuclear weapons.

Additionally, the PSEAG's Weapon Storage Magazines program and the DoD Lock Program are transitioning to the USAF's



ICBM Security Modernization Program

In the early 2000's, the PSEAG, in cooperation with the Security Policy Verification Committee (SPVC), played a key role in moving forward three key initiatives as part of the USAF's ICBM Security Modernization Program.

Remote Visual Assessment (RVA) was one of the three critical elements and it increased security of remote Minuteman III launch facilities. RVA was implemented per DoD S-5210.41M to provide immediate visual assessment of alarm notifications of the Improved Minuteman Physical Security System (IMPSS).

The Fast B-Plug was a second initiative: The B-Plug is a 14,000 pound cylindrical vault door used to delay access to the launcher equipment rooms. New built-in delay features include the ability to rapidly secure (raise) the B-Plug within 30-seconds. Early system development and design identified that in the event of a power failure at one of these locations the B-Plug would still need to meet the intent of rapid secure.

Launch Facility Concrete Enhancement (Head Works) used early RDT&E funds to provide a proof of concept demonstration and provided an answer to the 1998 Launch Facility Engineering study finding. Subsequently in 2004, DoD S-5210.41M identified the requirement for increased launch facility delay and the Head Works concept was employed.



Force Protection Equipment Demonstrations (FPED)

FPED was an outgrowth of the 1996 Downing Commission report on the Khobar Towers bombing on June 25, 1996 which the commission's key findings was that information commercial-off-the-shelf (COTS) physical security/force protection equipment deployed commanders and force protection/anti-

terrorism was proposed, received approval, and funded an initial event in September 1997. The event was so successful, that seven events have been sponsored, increasing in size and scope. The event has also grown to include other military involvement. The next FPED is scheduled for May 2010 at Stafford, VA: current estimates are for over 500 attendees by 10,000 attendees.



GOAL ONE

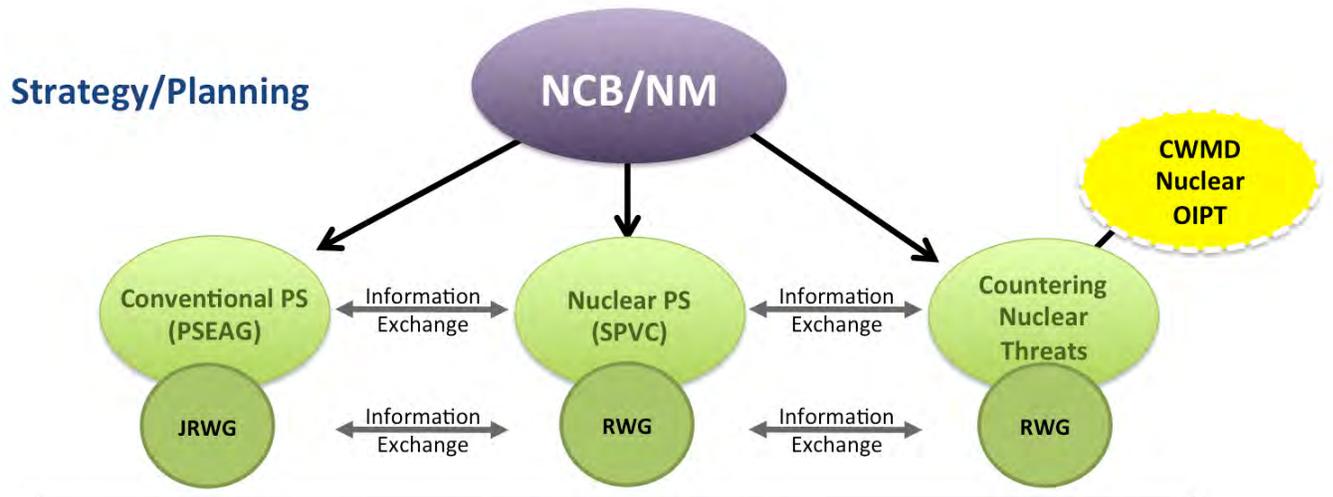
Leverage investments to achieve Physical Security enterprise-wide solutions across conventional and nuclear environments.



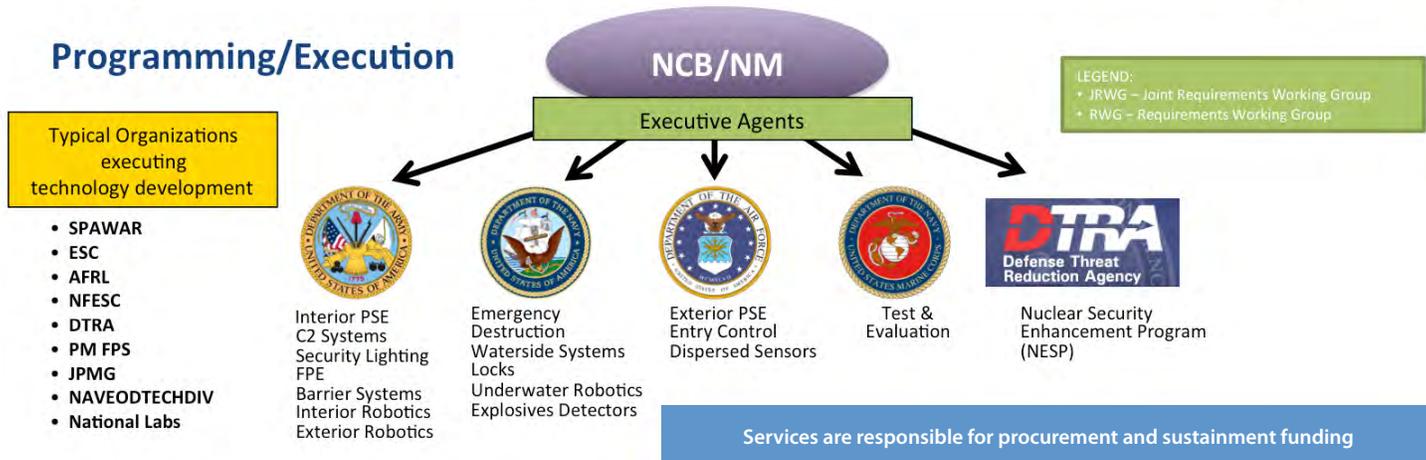
Across DoD, requirements from both conventional and nuclear physical security environments are merged, where applicable, resulting in increased efficiencies and effectiveness to meet these very demanding physical security missions. These requirements are rigorously defined in order to meet the specific needs of the PSEAG's customers, the services and the combatant commands, to place the needed capability into our customers' hands, on time and on schedule. To fulfill these warfighter requirements, the PSEAG collaborates aggressively across services sharing lessons learned, best practices, and project data concentrating on

physical security capability gaps and closing and mitigating security vulnerabilities. The PSEAG also leverages other organizations with similar security responsibilities to discover new solution sets. These include the DOE/NNSA, NRC, and the DHS which all have similar nuclear security responsibilities. In the non-nuclear mission space, we also work closely with many organizations including the Technical Support Working Group, the Joint Improvised Explosive Device Defeat Organization, and the Joint Non-Lethal Weapons Directorate.

STRATEGY and EXECUTION



Programming/Execution



GOAL TWO

Be the Department's focal point for Physical Security RDT&E initiatives and information sharing, both inside and outside of DoD.

The PSEAG acts as the Department's single point of influence to focus and integrate Service RDT&E efforts aimed at producing technology solutions for reducing or eliminating Physical Security Capability Gaps.

The PSEAG Chairman interfaces with uniformed and civilian counterparts within the Department to identify and pursue Department wide Physical Security initiatives, to coordinate investment strategies, and to provide Department level oversight of Service physical security programs and projects. The PSEAG Chairman reaches beyond the Department to Other Government Agencies to identify cross-cutting technology development opportunities and initiate cost effective collaboration strategies.

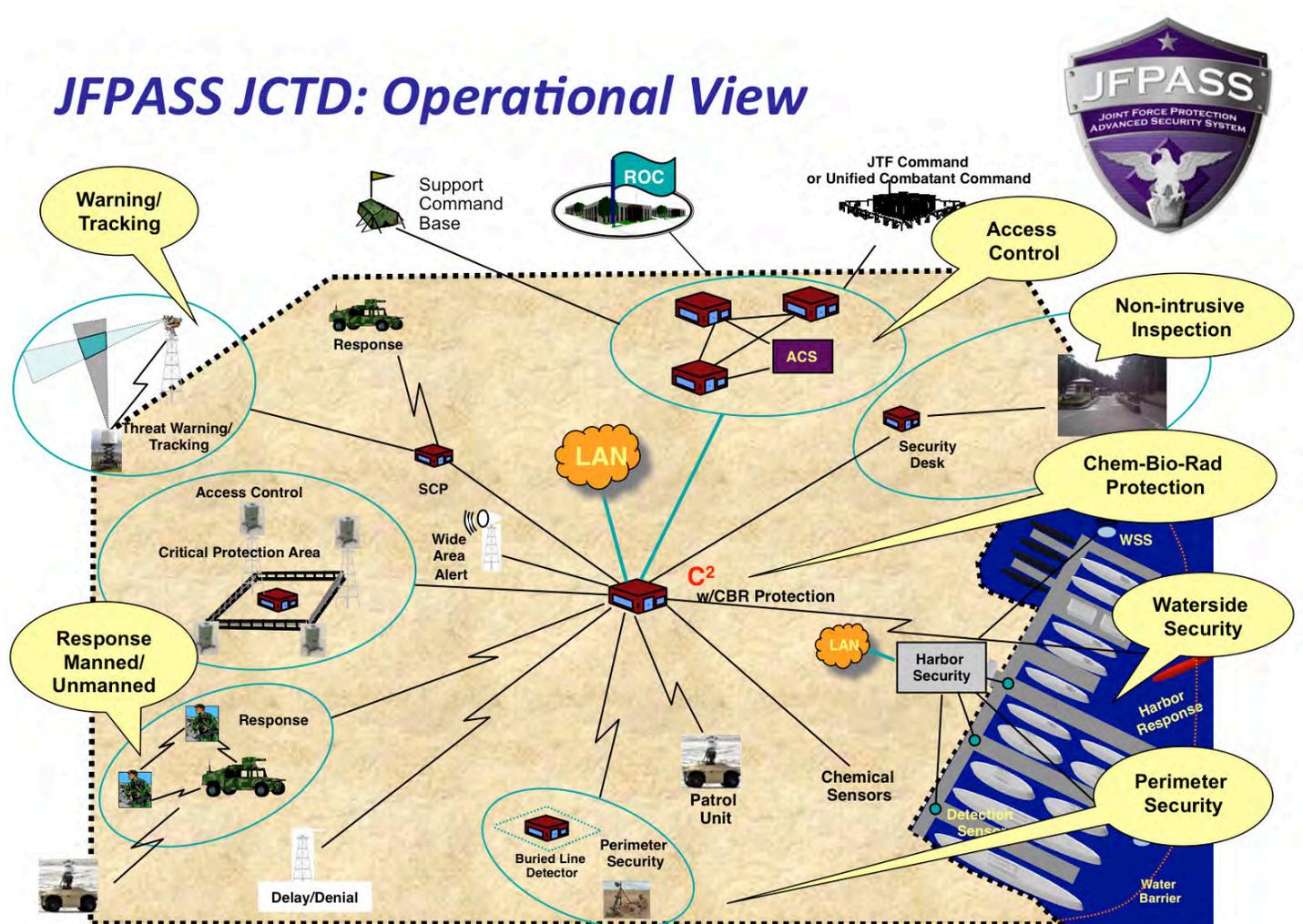


GOAL THREE

Harmonize physical security requirements while reducing RDT&E duplication and strengthening programmatic efficiencies.

The PSEAG conducts systemic processes to develop and review proposed programmatic solutions to Service and Department level Physical Security capability gaps, prioritize solutions for funding, and oversee the effective execution of programmed RDT&E programs. Review processes identify and conduct cost benefit analysis of potentially duplicative products for adjudication by the PSEAG Chairman. DoD Best Practices and continuous process improvement techniques are employed to assist Service PSEAG-funded program managers to meet or exceed DoD program performance objectives.

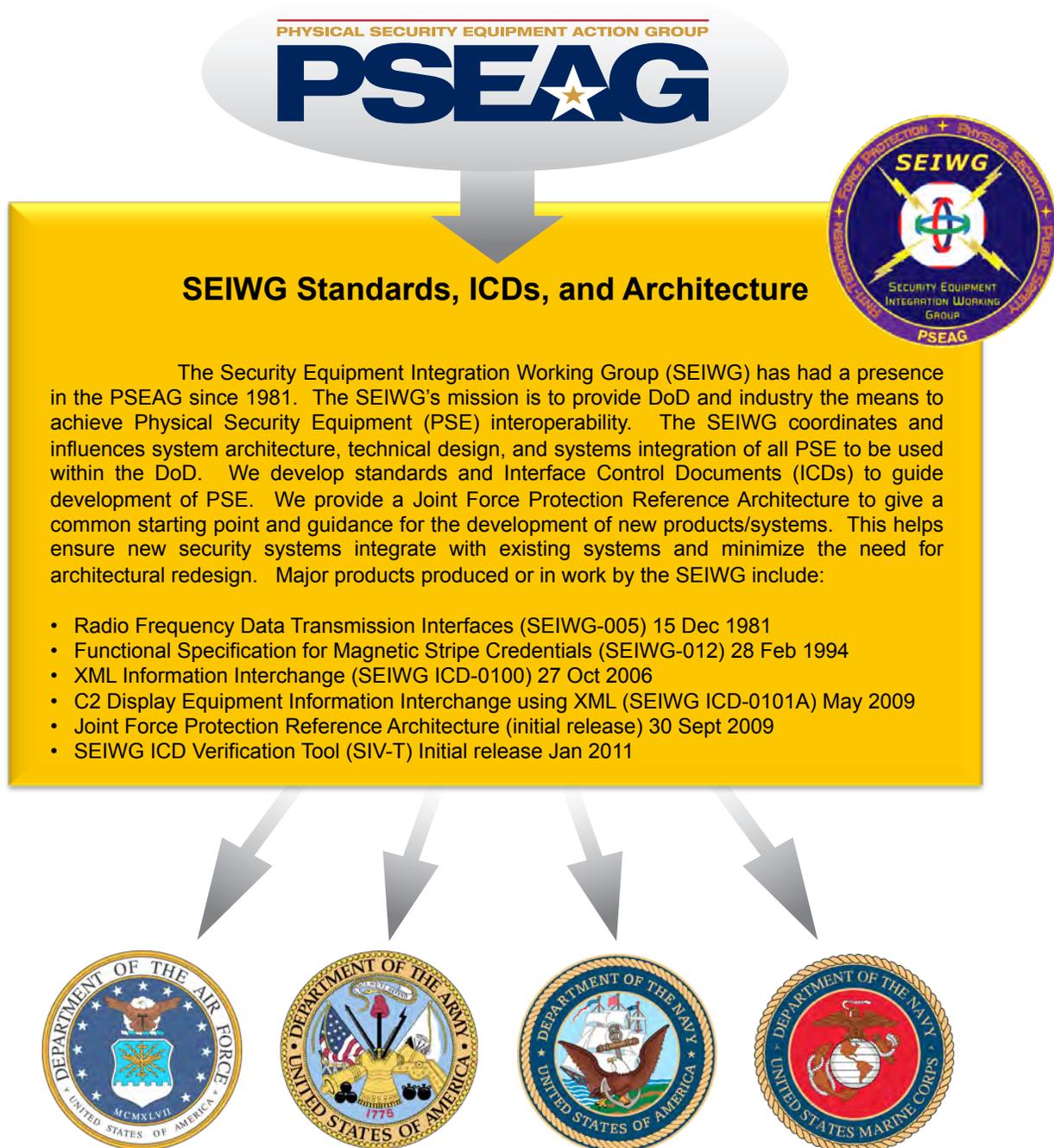
JFPASS JCTD: Operational View



GOAL FOUR

Lead the development and sustainment of architectures and standards to achieve Interoperability for Physical Security systems across the DoD.

The PSEAG provides Department level resources and oversight to foster the development, publication, and sustainment of broad PS architectures and lower level interface standards necessary to achieve interoperable, synergistic, affordable, and cost-effective PS solutions. Such solutions contribute to mission effectiveness and to reducing the overall RDT&E development timeline.

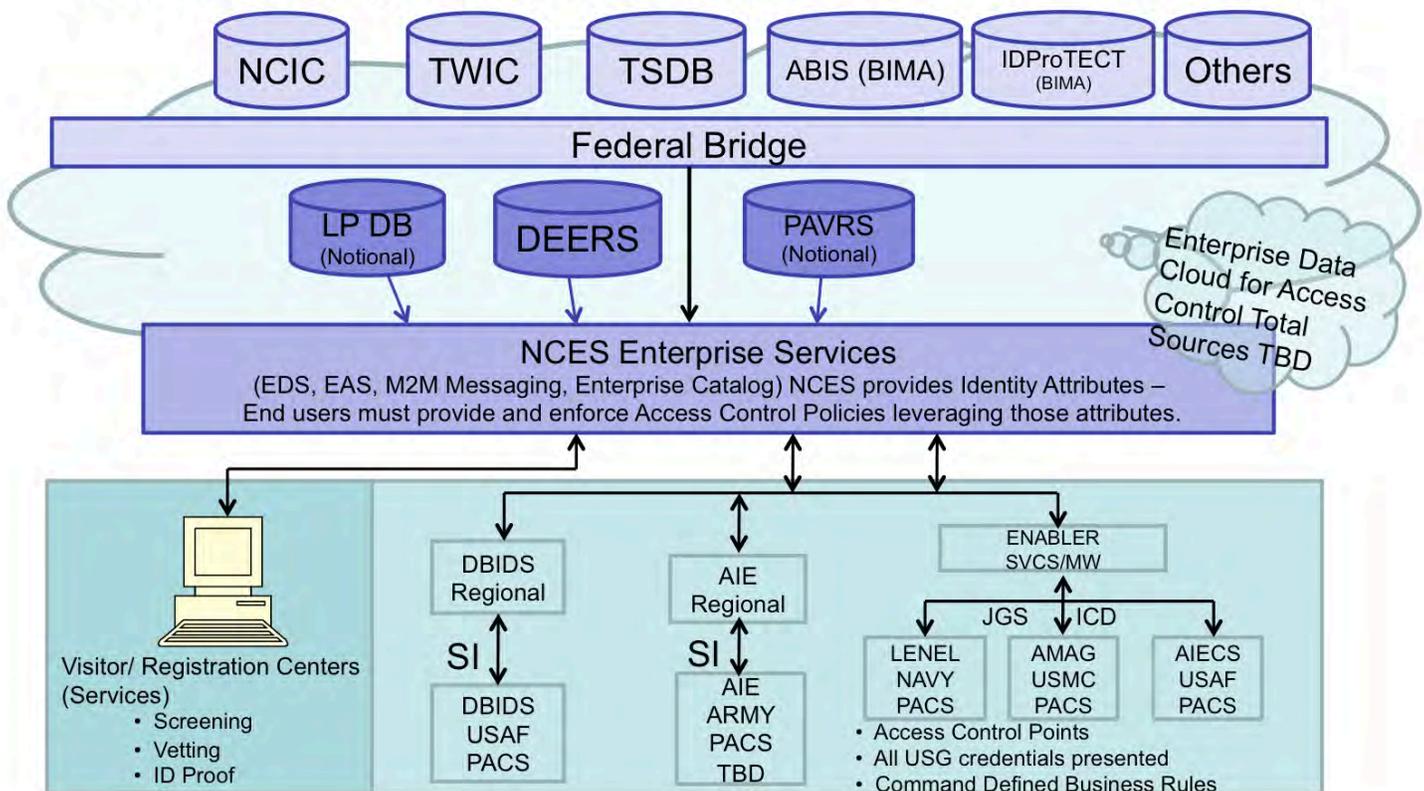


GOAL FIVE

Lead the pursuit of Department-wide Physical Security RDT&E initiatives which address Component and Joint capability gaps.

The PSEAG is an important player in addressing Department-wide physical security protection challenges and problems. The DoD Services are focused on solving Service-specific problems. The PSEAG, focusing on physical security technologies, looks to the outyears, creates standards and interface control documents, to ensure that capability requirements, whether directed from the national level or implied through internal DoD interoperability concerns, are met. Recent Examples of the PSEAG's forward looking philosophy includes its key sponsorship role in both the recent Joint Force Protection Advanced Security System (JFPASS) JCTD and ongoing Defense Installation Access Control (DIAC) Concept Demonstrations. "If not us, then who?"

Notional Identity Management Enterprise Services Architecture



DoD Installation Access Control (DIAC)

FY 2011 – 2015 PRIORITIES

- Continuously sponsor high-impact information sharing opportunities, utilizing Force Protection Equipment Demonstration (FPED) venues, Technology Outreach initiatives, and other select approaches.
- Advance DoD installation Access Control initiatives to meet Homeland Security Presidential Decisions and other mandates.
- Respond to Combatant Commander Joint Urgent Operational Need Statements to upgrade near term Integrated Base Defense capabilities.
- Identify and develop technologies to more effectively integrate waterside security concepts.
- Leverage conventional and nuclear physical security investments while integrating Protect functions of the countering weapons of mass destruction/ countering nuclear threats capability sets.
- Lead RDT&E initiatives to maintain a safe, secure and effective deterrence of conventional forces, installations and equipment – well integrated with the approach to providing similar capabilities for the nuclear force.



POINTS OF CONTACT

PSEAG Acting Chairman

Mr. Thomas J. Whittle, PE
 SPAWARSCEN Atlantic
 700 Robbins Avenue, Bldg 2A
 Philadelphia, PA 19111
 Phone: (215) 847-3104
 Fax: (215) 702-7574
 Tom.Whittle@navy.mil

U.S. Army PSEAG Representative

Mr. Eugene A. Smith
 HQDA DAPM-MPP-PS
 2800 Army Pentagon
 Washington, DC 20301-0800
 Phone: (703) 695-4210
 Fax: (703) 614-6967
 Eugenea.Smith@us.army.mil

U.S. Navy PSEAG Representative

Mr. Jeff Jones
 Assistant Secretary of the Navy (E, I & E)
 1000 Navy Pentagon
 Room 4E739
 Washington, DC 20350-1000
 Phone: (703) 602-3825
 Fax: (703) 602-5664
 Jeffrey.r.jones2@navy.mil

U.S. Air Force PSEAG Representative

Mr. John Salley
 HQ AF/A7SX
 1800 Air Force Pentagon
 Washington, DC 20330-1800
 Phone: (571) 256-0556
 John.Salley@pentagon.af.mil

U.S. Marine Corps PSEAG Representative

Mr. Charles "Tony" Pierce
 Headquarters Marine Corps
 Security Division (PS)
 3000 Pentagon Room 4A324
 Washington, DC 20350-3000
 Phone: (703) 695-7202
 Charles.a.pierce@usmc.mil

DTRA Representative

Mr. Vincent "Vince" Vetere
 Defense Threat Reduction Agency
 8725 John J. Kingman Road
 Stop 6201
 Fort Belvoir, VA 22060-6201
 Phone: (703) 767-4475/DSN 427
 Fax: (703) 767-4237
 Vincent.Vetere@dtra.smil.mil

SEIWG Chairperson

Rodney Rourk
 SPAWAR Systems Center Atlantic
 USMC Systems Engineering Branch
 Phone: (843) 218-4375
 rodney.rourk@navy.mil

JRWG Chairperson

Mr. David Needham
 Marine Corps Security Branch
 Naval Space and Warfare Systems Center
 2921 Ave B, North Bldg 1639
 North Charleston, SC 29405-1639
 Phone: (843) 218-4259
 Fax: (843) 218-4694
 David.Needham@navy.mil



FPED

Force Protection Equipment Demonstration

May 17 - 19, 2011

Stafford Regional Airport, VA

PSEAG



www.fped8.org

