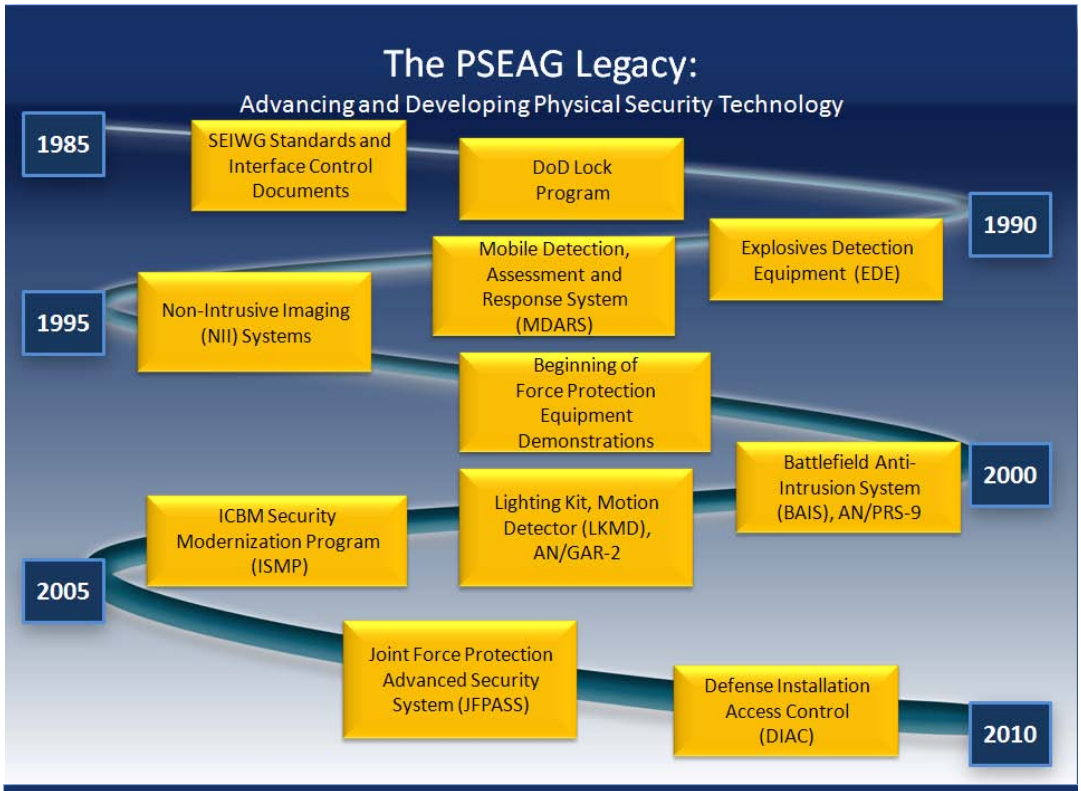
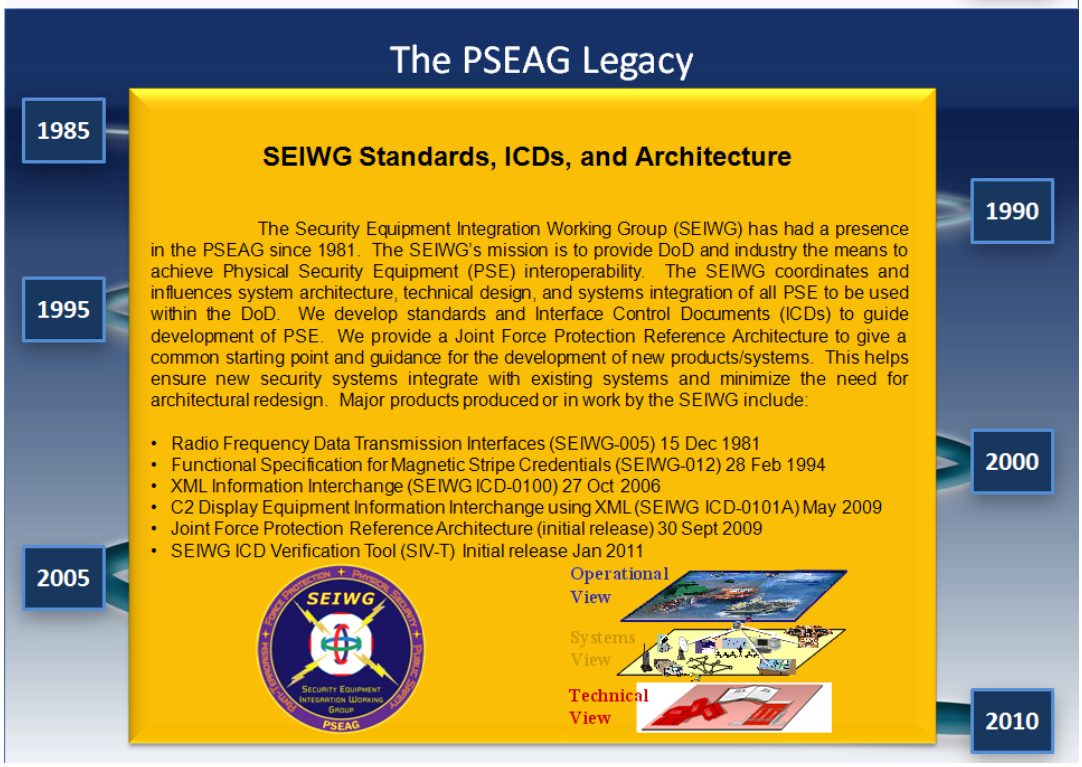
SECTION 7.0 – APPENDICES

APPENDIX A – PSEAG SUCCESSES





The PSEAG Legacy

1984 | 1990 | 1995 | 2000 | 2005 | 2010

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 operated under PSEAG-sponsorship for more than three decades.

The RDT&E team is knowledgeable on current threats and mitigation techniques, and have developed highly effective and economical weapons protection systems. Sponsors and those benefiting include: all DoD Services, DoD Agencies, Other Government Agencies, to include the Department of Energy (DOE), Central Intelligence Agency (CIA), Director of National Intelligence (DNI), General Services Administration (GSA), National Nuclear Security Administration (NNSA), and Nuclear Regulatory Committee (NRC). The Program maintains a Field Support Hotline to provide quick and accurate answers to the warfighter regarding hardware selection, requirements, training, specifications, stock numbers, and troubleshooting.

The DoD Lock Program has developed numerous key products throughout its tenure, to include the Internal Locking Device (ILD), which was approved by OSD policy maker, OUSD(I), on March 6, 1991, to be "an alternative solution to the then current high security padlock and hasp requirement" and today is approved for use on structures protecting chemical and nuclear weapons.

Additionally, the PSEAG's DoD Lock Program has an active Physical Security of Weapon Storage Magazines program and Attack Tools and Material Resistance initiatives, both of which are transitioning to the USAF's current Nuclear Weapons System protection concepts.

The PSEAG Legacy

1985 | 1990 | 1995 | 2000 | 2005 | 2010

Mobile Detection Assessment Response System (MDARS)

The family of Mobile Detection Assessment Response System (MDARS) systems, both Interior and Exterior, received initial PSEAG funding, coupled with the Joint Robotics Program dollars, in the early 1990's, which helped to facilitate early limited user Testing. What was originally MDARS-E (for Exterior) and now commonly referred to as MDARS ,began its Systems Design and Development (SDD) phase in 2002. Production systems have now been fielded to Hawthorne Army Depot and the US Department of Energy Nevada Test Site (NTS).

MDARS provides facilities and installations an electro-mechanical capability to conduct semi-autonomous random patrols and surveillance activities to include barrier assessment and theft detection functions. MDARS can be used at a variety of military and federal installations (i.e., depots, storage areas for rail, air, and port facilities, and Arms, Ammunition and Explosives (AA&E) storage facilities) to detect unauthorized access to a facility; verify the status of barriers and products; and investigate the source of alarms from remote locations before dispatching armed guards to the scene.

MDARS can provide commanders with an enhanced alternative capability (alternative to manual manned response) to counter covert and overt threats, reduce risk to personnel, and reduce manpower requirements used for security and inventory functions.

MDARS at Technical Feasibility Test (TFT) - 2000

MDARS at Early User Assessment (EUA) - 2005

MDARS on Night Patrol at DOE-Nevada Test Site (NTS) 2010

The PSEAG Legacy

1985

1990

1995

2000

2005

2010

Explosive Detection Equipment (EDE) Program

The Explosive Detection Equipment (EDE) Program is an RDT&E program funded by the PSEAG since the early 1990s. In 2001, NAVEODTECHDIV was designated the technical directive agent for the program. The program seeks EDE that will effectively and economically confirm the presence or absence of energetic material or IED components in or on mail/ parcels/cargo, vehicles, and personnel. EDE includes systems that detect and identify specific explosive compounds as well as anomaly detection systems for screening personnel, vehicles, and mail and packages.

Since 2001, NAVEODTECHDIV has conducted evaluations on over 90 different EDE systems and has helped develop over six new explosive detection systems. These evaluations have been published in over 50 reports which are posted on the PSEAG portal,

PSEAG funding has enabled the EDE Program to become recognized as DODs subject matter experts in the area of Explosive Detection. Agencies within and outside the DOD have requested support and/or participation with their EDE efforts to include: DHS, DTRA, Army, Air Force, JIEDDO, TSWG, EOD/LIC, ONR, etc. Some significant accomplishments are:

- Handheld Trace Comparative Study – 2002: ~800 VaporTracer^2 bought for Navy Ships
- Desktop Trace Comparative Study – 2006: Numerous systems bought by Army, Navy, DoS, Coast Guard
- Development of QinetiQ's SPO-20: Utilized in the CB2 ACTD. Technology transferred to TSA for use in an indoor environment and deployment of 20 systems in airports
- Handheld Trace Comparative Study – 2008: Over 400 Mobile Trace systems procured for OIF and OEF
- Deployment of two SMEs to OIF and OEF in 2008 to assist Army PM-FPS in field assessments of NIIS
- Testing Ahura First Defenders- 2008/2010: Over 500 systems fielded to OIF and OEF
- Several Test Evaluations – 2009: Led to the selection of the systems for the 19 fielded HME ID Kits
- Colorimetric Comparative Study – 2010: 100,000 colorimetric kits bought for OEF
- Non-Intrusive Imaging Systems Testing – Over 400 systems procured by the Army

The PSEAG Legacy

1985

1990

1995

2000

2005

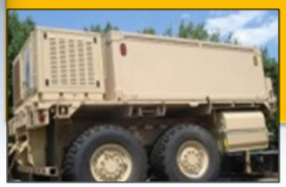
2010

Non-Intrusive Inspection Systems (NIIS)

The PSEAG played a key role, beginning in the mid 1990's, in the eventual fielding of over 400 Non-Intrusive Inspection systems. The role of the PSEAG in the early years was primarily focused on development , to include procurement of prototypes, and testing of commercial of-the-shelf products against stated military requirements. Eventually, the PSEAG designated the U. S. Army, more specifically the Product Manager, Force Protection Systems, as the lead organization for DoD NIIS initiatives. PM FPS, on behalf of the PSEAG, performed numerous functions throughout the years, to include the procurement and fielding of mobile, fixed and re-locatable NII system configurations from various contractors. The technologies used by NII systems have proven to be a significant Force Protection measure. They look into vehicles and cargo containers to detect anomalies which may indicate the presence of explosives, weapons, or other contraband.

The success of the NII program can be attributed to effective coordination between PM-FPS, system manufacturers, and the other military Services. In addition to conducting verification testing of NII commercial products, PM-FPS works closely with the US Navy, the lead Service for the RDT&E of explosive detection technology.

Various technologies make up a family of systems approach. X-ray (backscatter and transmission) and nuclear (gamma) rays are used to non-intrusively inspect stationary and moving vehicles and cargo containers. Under optimal conditions, they can scan up to 100 vehicles per hour. The rapidly re-locatable systems quickly inspect stationary vehicles at entry control points. The gamma ray technology can inspect larger vehicles and cargo containers for explosives, weapons, people and other contraband. There are a number of systems, including militarized ones, included in the NIIS family.



The PSEAG Legacy

1985

1990

1995

2000

2005

2010

Force Protection Equipment Demonstrations (FPED)

The concept for the FPED was an outgrowth of the 1996 Downing Commission which looked at lessons learned from the Khobar Towers bombing on June 25, 1996 which killed 19 American servicemen. One of the commission's key findings was that information about existing and ready to field commercial-of-the-shelf (COTS) physical security/force protection products was not available to deployed commanders and force protection/anti-terrorism experts in the field.

Key leaders in the PSEAG proposed, received approval, and funded an initial FPED at Quantico Marine Corps Base in September 1997. The event was so successful, FPEDs were continued biannually and now seven events have been sponsored, increasing in the number of vendors, products and attendees. The event has also grown to include other federal agency, state and local municipality involvement. The next FPED is scheduled for May 17-19, 2010, at Stafford Regional Airport, Stafford, VA: current estimates are for over 500 vendors to display 3500 products and be seen by 10,000 attendees.

The PSEAG Legacy

1985

1990

1995

2000

2005

2010

Battlefield Anti-Intrusion System (BAIS), AN/PRS-9

The BAIS Program was initiated in 1997 at the US Army Infantry Center (USAIC), Fort Benning, GA as a replacement for the obsolete and unmaintainable Platoon Early Warning System (PEWS), AN/TRS-2. The Operational Requirements Document (ORD) was approved on 11 September 2003. Development of the BAIS was initiated in 2001 with RDT&E funds provided by the DoD PSEAG.

The BAIS, AN/PRS-9, was approved to enter Full Rate Production at the Milestone C in October 2003. First Unit Equipped was in February 2006 and Initial Operational Capability achieved in May 2006.

BAIS is a compact, sensor-based early warning system that provides detection and classification of intrusions for small units and troops during various tactical missions. It can be used either as a tactical stand-alone system or as a supplemental device for other security missions. To date, 1,325 systems have been fielded to US Army and Army National Guard units and proven highly reliable during operations in Theater. A separate DOD PSEAG-funded BAIS Modernization Program developed and tested an upgraded system that includes a BAIS Hand-Held Monitor/Transmitter and Sensor/Transceiver. These improvements continue to ensure current technology and improved performance are available to the field. A follow-on production contract was competitively awarded in August 2010 and included the upgrades resulting from the Modernization Program. This contract will provide an additional 4,112 systems scheduled for delivery beginning June 2011.

The PSEAG Legacy

1985

1990

1995

2000

2005

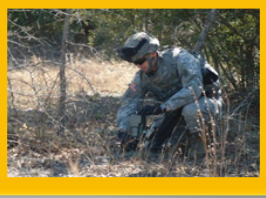
2010

Lighting Kit, Motion Detector (LKMD), AN/GAR-2

The genesis of the LKMD, formally known as the Electronic Trip Flare (ETF), was to provide a technologically advanced sensor system as an alternative to the M49A1 Surface Trip Flare. The LKMD program received initial PSEAG funding in FY04 to pursue a Milestone B decision. LKMD was granted approval to enter the System Development and Demonstration (SDD) phase in April 2004. A SDD/production contract was subsequently awarded in May 2005. Full Rate Production began in February 2010.

Over 650 production systems have now been fielded to various U.S. Army Active, Reserve, and National Guard units. The U.S. Army projects to field over 34,000 LKMD systems to U.S. Army units over the next several years.

The LKMD is a portable, compact, modular, sensor-based early warning system providing programmable responses of illumination and sound, resulting in increased operational reaction time. LKMD may be used as a tactical stand-alone system or as a supplemental device for use with other force protection systems such as the Battlefield Anti-Intrusion System (BAIS), AN/PRS-9. LKMD provides early detection and warning in order to enhance force effectiveness and increase situational awareness during all types of combat operations ranging from Military Operations in Urban Terrain (MOUT) to high intensity combat. Using LKMD as part of an integrated, in-depth, layered security concept will further enhance for protection.



The PSEAG Legacy

1985

1990

1995

2000

2005

2010

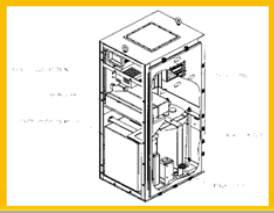
ICBM Security Modernization Program

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.



The PSEAG Legacy

1985 | 1990 | 1995 | 2000 | 2005 | 2010

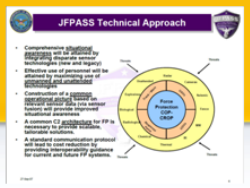
Joint Force Protection Advanced Security System (JFPASS)

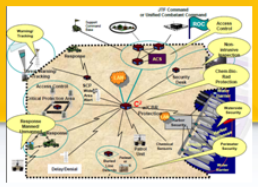
Late in 2007, DoD identified that it was faced with a significant joint warfighting problem – its force protection systems were disjointed and inefficient, lacking the ability to provide comprehensive situational awareness, absorbing too much manpower, and proving too costly as a result of multiple variants and redundancies. These facts were proven out by the Integrated Unit, Base and Installation Protection (IUBIP) capabilities-based assessment conducted during FY07.

Simultaneously, DoD embarked on Force Protection Joint Experiment (JE) conducted throughout FY07 and FY08 to identify the range of existing and potential FP technologies in its portfolio. During FY08, the Joint Force Protection Advanced Security System (JFPASS), entered the DoD budget as a JCTD, with the Army as the lead Service, funding provided by the PSEAG, and an initial objective of demonstrating, assessing and transitioning an integrated Joint FP capability/C2 architecture.

JFPASS is designed to enable the fusion of force protection capabilities by integrating and automating current and emerging systems, sensors, tools and processes to allow operators to focus on responses. The system covers the entire force protection spectrum, including Access Control, Perimeter Security, Intrusion Detection, Waterside Security, CBRNE Sensing, Warning, Incident Management, Unmanned Systems, and Unattended Sensors. As a result of the successful Operational Demo II in August 2010, two abbreviated JFPASS packages are being deployed to a combatant command.

Feb – Mar 2009 JFPASS Technical Demo I
Sep – Oct 2009 JFPASS Operational Demo I
Apr – May 2010 JFPASS Technical Demo II
Jul – Aug 2010 JFPASS Operational Demo II





The PSEAG Legacy

1985 | 1990 | 1995 | 2000 | 2005 | 2010

Defense Installation Access Control (DIAC)

OUSD(I) Directive-Type Memorandum (DTM) 09-012 mandates Physical Access Control Systems (PACS) must support a DoD-wide and federally interoperable access control capability that can authenticate USG physical access credentials and support access enrollment, authorization processes, and securely share information; with provisions for security forces and/or guards to conduct a physical and visual inspection of credentials until electronic PACS are fully deployed. To move toward compliance with DTM 09-012, the DoD Physical Security Equipment Action Group (PSEAG) agreed to sponsor a series of Defense Installation Access Control (DIAC) Table Top Exercises and Operational Demonstrations. The DIAC also began developing a single DoD-wide Enterprise Services Architecture to rapidly, electronically and securely share information among Physical Access Control Systems and authoritative data sources throughout the DoD and authorized Federal Agencies to enable installations/ organizations to authenticate credentials and individual authorization to enter.

Mar - Apr 2009 DIAC TTX I – Charter for building an architecture and developing the Roadmap
Apr – Dec 2009 DIAC WG – Service/Agency collaboration and planning for the Phase I Demo
Apr - May 2010 DIAC TTX II – Refine requirements & define the end-state architecture
Jun 2010 – DIAC Demo I – Data exchange between Service PACS & authoritative source

DIAC
Defense Installation Access Control