SEIWG

Security Equipment Integration Working Group

MARCH 2012

Inside this issue:

| | |
|---|---|
| Defense Installation Access Control (DIAC) | 2 |
| JIGSAW Embracing the Latest SEIWG Standards | 3 |
| A Timeline of SEIWG Documents | 4-5 |
| Use of ICD-0101 in Open Architecture Security | 6 |
| A New Look for the SEIWG | 7 |
| Upcoming Events | 7 |
| SEIWG SIV-T Demonstration | 8 |
| Do You Know... | 8 |
| JFPRA Technical Standards Profile | 9 |
| The SEIWG Mission | 9 |

# US AIR FORCE AND NAVY SEIWG PRINCIPALS SELECTED

## Welcome Dr. Jeff Wit and Chris Hernandez

**Dr. Jeff Wit**
***USAF SEIWG Principal***

Dr. Wit received his Doctorate in Mechanical Engineering from the University of Florida in 2000, where his research focused on unmanned ground vehicle technologies. After receiving his degree, Dr. Wit began working for the Air Force Research Laboratory (AFRL) as a contractor in the Airbase Technologies Division at Tyndall AFB, FL.

In 2010, Dr. Wit began his public service and is currently a Senior Research Engineer for AFRL Airbase Automation projects. While at AFRL, he worked on robotic projects for several missions areas including range clearance, fire fighting, and perimeter security. Two of the perimeter security projects include the Remote Detection Challenge and Response (REDCAR) project and the Force Protection Joint Experiments (FPJEs).

In 2003 Dr. Wit led the systems integration for REDCAR and used the SEIWG ICD 0100 and the Joint Architecture for Unmanned Systems (JAUS) to integrate physical security equipment with the robotic systems. In 2006, Dr. Wit led the development of an armed ground robotic vehicle for the FPJEs conducted at site C-3 at Eglin AFB, FL. This vehicle integrated a weapon's watch payload that supported both JAUS and the SEIWG ICD 0100.

Dr. Wit has over 10 years of experience in developing standards in support of unmanned systems interoperability. He has been actively involved with the JAUS Working Group since 2000, and he is currently the chair of SAE's AS-4C Committee, Information Modeling and Definition, which is the successor to JAUS.

**Chris Hernandez**
***US Navy SEIWG Principal***

Chris Hernandez has 12 years of service as a DoD Civilian. He possesses Masters of Science degree in Industrial Technology: Focus in Biometrics/Project Management; a Bachelors of Science in Health Promotion/Exercise & Fitness; and an Associates degree in Science, Electrical and Computer Engineering Technology. All degrees were obtained through Purdue University.

Since 2006, Mr. Hernandez has served as the current Integrated Product Team (IPT) lead for the Federal Systems and Applications. He is also a project engineer for Special Operations Command, Pacific (SOCPAC) biometric scanning missions who manages the schedule and performance for deployment of a biometric scanning system in the Area of Responsibility with a mission of scanning 800K fingerprint cards and providing that data to the US Government. The Effort includes collaboration with stakeholders from SOCPAC, Federal Bureau of Investigation (FBI), Biometrics Identity Management Agency (BIMA), and host nation federal employees and local nationals.

Since 2005, Mr. Hernandez has served as the SEIWG Technical Representative & Liaison to Security Equipment Working Group (SEIWG) providing support to the Navy representative to SEIWG. As part of SEIWG duties, he has conducted technical reviews of SEIWG force protection interface control documents and architectural artifacts. He has also represented the SEIWG at multiple Security Industry Association (SIA) Government Summits, briefing industry professionals on current SEIWG efforts and promoting the use of SEIWG products. Mr. Hernandez represents the SEIWG at the SIA standards group.

Mr. Hernandez continues to participate in numerous identity management efforts as Navy & SEIWG representative. He is currently acting as the SEIWG representative to the Federal Identity and Credential Access Management group, participating in working group meetings and technical review of Federal Identity, Credential Access Management (FICAM) publications. He has acted as an editor for the National Industry of Standards and Technology (NIST) Special Publication 800-116, a guide for implementation of Homeland Security Presidential Directive (HSPD)-12 and the Federal Information Processing Standards (FIPS)-201 for physical access control across the federal government.

Mr. Hernandez supports numerous Navy Anti-terrorism Force Protection (ATFP) Ashore systems engineering activities in CONUS and OCONUS for NRSWA, CNRSE, Djibouti, CNREUR, Naval Consolidated Brig Charleston, SC, Naval Consolidated Brig Miramar, CA, Naval Consolidated Brigford Island, HI, Charleston, SC, Camp Lejeune Pre-Trial Confinement Facility, and SUBASE Kings Bay and SUBASE Bangar.

Mr. Hernandez is employed by Space and Naval Warfare Systems Center Atlantic and is based in Charleston, SC.

# Defense Installation Access Control (DIAC)

*By:*
*Rodney Rourk,*
*Chairman, Security Equipment Integration Working Group*

*SPAWAR Systems Center Atlantic*

*USMC Systems Engineering IPT*

Current DOD physical access control systems (PACS) procedures are governed and implemented under Service-unique direction and are not fully interoperable between Service installations. No enterprise capability exists for linking DoD installations for electronic authentication of credentials. OUSD(I) Directive -Type Memorandum (DTM) 09-012 mandates that DOD 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.

The DOD Joint Services face a Physical Security vulnerability today with the lack of standard authentication measures for credentials and continuous vetting of individuals against authoritative data sources, which prevents the services from determining if persons entering military installations are "a threat" and leaves DOD assets vulnerable. Section 1069 of Public Law 110-181(Appendix 2), tasked the Secretary of Defense (SECDEF) to determine the fitness of personnel entering military installations in the United States.

To aid the services in establishing compliance with policy, in FY2009, the PSEAG sponsored the first in a series of Defense Installation Access Control (DIAC) RDT&E demonstrations. The DIAC is comprised of Core and Technical working groups. The Core group consists of senior OUSD(I) policy and DOD physical security representatives from each of joint services. The DIAC Technical Working Group (DTWG) consists of DOD physical security equipment subject matter experts from each of joint services and is lead by the SEIWG.

In FY09, the DTWG developed and published the DIAC notional architecture and Joint Gatekeeper Services (JGS) Interface Control Document (ICD), which specifies a standard interface to be used for data interchange between middleware/regional PACS server and local PACS. The JGS is a data services platform that provides identity management web services, enabling a conduit for information exchange between PACS and external authoritative databases.

In FY10, the DTWG successfully completed phase I demonstration at three locations: Site C-3/ Eglin AFB, Florida (USAF), Space & Naval Warfare Systems Command (SPAWAR), Charleston, South Carolina (USMC) and the Washington Navy Yard, Washington DC (USN). The DTWG lead the incorporation of the JGS ICD into multiple COTS PACS and demonstrated the capability to support the Use Cases that were developed by the joint services. Demo I validated that the capability currently exists to immediately exchange data with an authoritative source (DEERS) via a middleware/regional server within a web services architecture and to return information accurately to PACS. The demo was a success in that each of the Services' PACS was responsive and exchanged data with DEERS without issue. The interoperability between sites proved equally successful as cards registered at one site were electronically authenticated at the other sites.

In FY11, the DIAC expanded the enterprise architecture to support multiple authoritative source systems. Demonstration II used four test sites. The focus of this Demonstration was developing and evaluating a Continuous Information Management Engine (CIME) capability to send information to the PACS when data on an individual's fitness for access to an installation changes. This capability was paired with an Interoperability Layer Service (IoLS) that ensured the data reached each Service-level PACS so that the entry control point security guard will know whether to authorize or deny entry. The availability of National Crime Information Center (NCIC) and Terrorist Screening Database (TSDB) data was demonstrated via a simulated database, accessed upon demand.

The results of Demonstration II proved the art-of-the-possible for delivering the ability to exchange personnel identification data between installation PACS, IoLS, a CIME and test data representing authoritative source systems (NCIC & TSDB). Demonstration II also successfully demonstrated the ability to pass registration, revocations, debarment, felony wants/warrants, and terrorist screening information between DoD Components. Unique to this Demonstration was the execution of Global Name Recognition, which is an enhanced name checking function that increases accuracy by matching across alternate forms of a given name. By creating a new Identity

## Defense Installation Access Control (DIAC) *continued*

Management Enterprise Services Architecture and exercising it with a 100 percent success rate, the decision to proceed with the Architecture's continued evolution and future demonstration/implementations at operational DoD installations was fully supported by the joint services.

In FY12, the DIAC is pursuing a Joint Capability Technology Demonstration (JCTD) to build the enterprise architecture connecting the NCIC, TSDB, TWIC CRL, and Federal and non-DOD verification (PIV/PIV-I) databases. The information will then be accessible by each Service's Physical Access Control Systems at DOD bases/facilities. The DIAC TWG is in progress on the development of a standard DOD Local Population Credential, which applies to the category of persons who require access to DOD facilities and bases that do not have a DOD centrally issued credential like CAC or the TESLIN card (e.g. short term contractors, service vendors, visitors, etc.). Today these populations are authenticated and vetted for access by each individual base with their Identity Information (PII) records being stored within each local base's Physical Access Control System (PACS) solution. The DOD Local Population Credential will be a federated identity credential, which will be electronically authenticated across all four services.

The Joint Services anticipate the installation access threat to continue, and the DIAC (with SEIWG technical standards leadership) continues to provide the capability for standards based authentication measures for federated DOD and federal credentials and continuous vetting of individuals seeking access to DOD military facilities and installations.

# JIGSAW Embracing the Latest SEIWG Standards

***By:***
***Norbert Stiepel***

*For more information, please email:*
*Norbert.stiepel@navy.mil*

Project JIGSAW is a PSEAG sponsored project that aims to put all the "pieces" together to allow DoD Joint Services to have a unified approach to Command and Control across all integrated physical security programs.

JIGSAW is working to develop a system that will provide a Service Oriented Architecture (SOA) specific to force protection (FP) environments. This system will host sensors in a 'sensor cloud' and allow data subscriptions from 'Software Interface Modules' (SIMs). These SIMs can then be assembled to support Integrated Base Defense applications such as Forward Operating & Fixed Base perimeter surveillance. This decreases complexity, cost and time associated with integrating control systems such as Access Control, Intrusion Detection, Fire & Emergency Services and Weapons Systems.

The JIGSAW team's goal was to utilize standard device and computer platform communication protocols. Naturally, the JIGSAW team decided to implement the SEIWG ICD-0101B – Sensor & CCDE Communication Protocols as well as the SEIWG ICD-0300 CCDE to IBDC2 protocol to support messaging across the Integrated Base Defense domain. The collaboration between SEIWG and JIGSAW teams has been beneficial to both groups. The SEIWG provided guidance, subject matter expertise, the recently released SEIWG Interoperability Verification Tool (SIV-T) software application that have helped the JIGSAW team implement the ICD. The JIGSAW team has provided valuable feedback as a partner and end-user of SEIWG products.

This PSEAG sponsored initiative is one example of the PSEAG's mission to provide programming, planning and RDT&E support for PSE materiel requirements while eliminating duplication of products, pursuing the use of commercial-of-the-shelf (COTS) products, ensuring systems integration, and promoting interoperability and sustainability.

Norbert Stiepel is a physical Security Subject Matter Expert who supports the Marine Corps Electronic Security Systems program at SPAWARSYSCEN Atlantic and is the lead for project JIGSAW.

# A Timeline of SEIWG Products

## 2012

| | |
|---|---|
| January | SEIWG 0400 Security Equipment Integration Working Group (SEIWG) Joint Anti-Terrorism/Force Protection Technical Standards Profile Technical View 1 (TV-1)* (A JFPRA DoDAF product) |
| January | SEIWG 0300 Force Protection Systems Command and Control Information Interchange |
| January | SEIWG 005D Interface Specifications (RF Data Transmission Interfaces) for DoD Base & Installation Physical Security Systems |
| January | SEIWG Interoperability Verification Tool (SIV-T) |

## 2011

| | |
|---|---|
| June | SEIWG ICD-0101B Command and Control Display Equipment (CCDE) Information Interchange using XML |
| April | SEIWG ICD-0101A Command and Control Display Equipment (CCDE) Information Interchange using XML accepted as a mandated standard and added to Department of Defense Information Technology Standards Registry (DISR) |
| February | Joint Gatekeeper Services (JGS) ICD 2.0 in support of DIAC II |

## 2010

| | |
|---|---|
| November | UPDATE: Joint Force Protection Reference Architecture* |
| October | JFPASS JCTD OD-2 Tailored Architecture (MTR 100312) (includes OV-1, OV-2, OV-3, OV-5, OV-6C, SV-1, SV-2, SV-4, SV-5, SV-6*, and Business Process Models for JFPASS Fusion Engine Logic) |
| April | Joint Force Protection Advanced Security System (JFPASS) – Operational Demonstration One (OD-1) Tailored Architecture Final (MP 080221) (includes OV-1, Capability Taxonomy, Capability Weights, OV-2, OV-3, OV-5, OV-6C, SV-1, SV-2, SV-4, SV-6*, and Business Process Models for JFPASS Cohesion IF Fusion Engine Logic) |
| March | JFPASS JCTD OD-1 Tailored Architecture (OV-1, Capability Taxonomy, Capability Weights, OV-5*, Nodes and Functions Report, SV-5 Traceability Report |

## 2009

| | |
|---|---|
| September | Final Report, Complete Joint Force Protection Reference Architecture (OV-1, 2, 3, 4, 5, 6c; SV-1, 4, 5, 6*) |
| September | First Draft Report, Complete Joint Force Protection Reference Architecture (OV-1, 2, 3, 4, 5, 6c; SV-1, 4, 5, 6*) |
| July | First Draft of Complete Joint Force Protection Reference Architecture (OV-1, 2, 3, 4, 5, 6c; SV-1, 4, 5, 6, TV-1*) |
| July | Draft Joint Force Protection SV-5* |
| July | Joint Force Protection Operational Views (OV-2, OV-3, OV-5)* |

**LIST OF ACRONYMS**

JFPASS – Joint Force Protection Advanced Security System JCTD – Joint Capability Technology Demonstration IA – Integration Assessment OD – Operational Demonstration
* denotes SEIWG DoD Architect Framework (DoDAF) compliant products.

## A Timeline of SEIWG Products (continued)

| | | |
|---|---|---|
| 2009 | May | Joint Force Protection Advanced Security System (JFPASS) Operational Demonstration 1 (OD-1) SV-4* for VIP Day |
| | May | Final Draft Joint Force Protection OV-6c* |
| | May | SEIWG ICD-0101A Update to SEIWG-ICD-0101 |
| | April | Draft Joint Force Protection Operational Event-Trace Diagrams |
| | February | Joint Force Protection Architecture OV-2, OV-3, and OV-5* |
| | January | SEIWG ICD-0101 Command and Control Display Equipment (CCDE) Information Interchange using XML |
| 2008 | December | JFPASS-JWARN Integration Plan |
| | July | Joint Force Protection Advanced Security System (JFPASS) Integration Assessment 4 (IA-4) Systems Architecture (MTR080178), including SV-1, SV-2, SV-4, SV-6, SV-10c* |
| 2007 | October | Joint Force Protection Architecture Overview and Summary Information (AV-1*) |
| | October | Joint Force Protection Operational Activity Model (OV-5) |
| | February | SEIWG Integrated CCDE-to-CCDE ICD update leading to SEIWG ICD-0101 |
| | January | Interface Control Document, SEIWG Integrated CCDE ICD update leading to SEIWG ICD-0101 |
| 2006 | December | ICD for Access Control Systems XML Schema Definitions for XML Data Exchange update leading to SEIWG ICD-0101 |
| | October | SEIWG ICD-0100 XML Information Interchange |
| 2003-1981 | February 2003 | ICD-002 Generic Device Interface Control Document using XML |
| | February 1994 | SEIWG-012 Prime Item Product Function Specification for Magnetic Stripe Credentials (MSC) |
| | 1981 | SEIWG 005 Interface Specifications (RF Data Transmission Interfaces) for DoD Base & Installation Physical Security Systems |

**LIST OF ACRONYMS**

JFPASS – Joint Force Protection Advanced Security System JCTD – Joint Capability Technology Demonstration IA – Integration Assessment OD – Operational Demonstration
* denotes SEIWG DoD Architect Framework (DoDAF) compliant products.

# Use of ICD-0101 in Open Architecture Security

*By:*
*Mike Slocik*
*Greg Valenzuela*

*General Dynamics Advanced Information Systems*

*For further information, please email:*

*Michael.Slocik@gd-ais.com*

Maintaining the security of highly sensitive facilities against terrorist attacks requires an increasingly complex application of sensors, processing and Command and Control technologies to security systems. These systems must be scalable to accommodate expansion in capabilities, sensors, and human operator roles. Components need to be periodically upgraded or replaced without affecting the operation of the security system. Additionally, new technologies continue to be developed that have the potential to significantly enhance mission effectiveness. However, the continued expansion or upgrade of legacy systems involving point-to-point or analog hardware connections can become increasingly costly.

General Dynamics Advanced Information Systems recognized that an open architecture approach, pioneered and proven on core mission systems for surface ships, could be applied to the design of a distributed facility security system. The architecture approach is based on a Data Exchange Infrastructure (DXI) consisting of a standards-based set of messages and data distribution mechanisms. The message structures and data exchange characteristics of the architecture are described in an Open Data Model (ODM) in the Unified Modeling Language (UML). An associated model-driven integration process that generates documentation and software artifacts substantially reduces the effort needed to integrate subsystems, or change proprietary software each time a new system or capability is required to be integrated. To enable interoperability among the integrated systems and devices, the ODM is defined based on current security industry standards, using the SEIWG ICD-0101 as the baseline. Data distribution mechanisms such as the Data Distribution Service (DDS) publish-subscribe standard were selected based on the objective operating characteristics. The ODM defines data classes and enumerated types (e.g., the ICD-0101 basic types) used for building up more complex classes. Message structures for data exchanges (e.g., commands and reports) are defined by composition or aggregation of the common classes, guided by the ICD-0101 schemas. In developing the ODM content, the ICD-0101 schemas were mapped to binary equivalents, which support the data-centric aspects of DDS.

The ICD-0101A XML schemas are stored in the DoD's Metadata Registry, making them available to the broader DoD community for reuse and review. The SEIWG message set strikes a balance between simplicity and flexibility. It is recommended that more vendors of security technology to the military become familiar with and provide feedback on the specification as it contains the definitions, data exchange examples, populated message examples, and other important information usable for a variety of security applications.

DXI enables an integrator to efficiently combine multiple disparate capabilities into a single, unified security system with subsystem output data readily available on the network for use by other components. This simplifies the job of the security system operators by establishing common operational concepts and a unified user interface across all subsystems. Technology refresh is transparent to the user since the architecture supports co-existing security systems and the ability to manage the phasing in and out of technology. General Dynamics Advanced Information Systems is applying DXI to a U.S. Navy facility security system. On this program, the architecture delivers benefits to the U.S. Navy through:

- Rapid insertion of new physical security devices/ sensors
- Availability of data from disparate, distributed security subsystems for automated processing
- Common user interfaces and consoles providing access to information brought together from a variety of security subsystems
- Full rights to the interface definitions and runtime configuration

Building on the success of this program, General Dynamics Advanced Information Systems plans to apply the DXI approach to all physical security distributed software systems in which adherence to a common data interchange model and data distribution mechanism is advantageous to the customer.

**SEIWG Addresses General and Specific Service/Agency PSE Requirements by:**

- ✓ Providing DoDAF Architecture products/ views
- ✓ Providing Interoperability Standards
- ✓ Sharing Information

# A NEW LOOK FOR THE SEIWG

**By: Brad Davis**

The SEIWG recently updated its logo building upon the ideology behind the former logo while maintaining focus on commonality with our parent sponsor, the Physical Security Enterprise & Analysis Group (PSEAG) logo. The logo symbolizes the SEIWG structure and mission to increase Physical Security Equipment interoperability through a joint approach.

The purple tinted globe as a backdrop reflects the joint community and the SEIWG's commitment to worldwide Service to the DoD. Each of the colored rings that interlock the Pentagon represents a key contributor, and converges in the center to produce a purple star, symbolizing joint collaboration. The SEIWG's relationship with the Physical Security Enterprise & Analysis Group, as a Permanent Working Group, is captured in the banner as well as the appearance of the shield with crossed swords, and the Pentagon amidst the shield, which can be found on the PSEAG's current logo. The key contributors to the mission are also represented by colored stars in the lower portion: US Army in green, US Navy in navy blue, US Air Force in light blue, US Marine Corps in red, and the Defense Threat Reduction Agency (DTRA) in white. Finally, the SEIWG's mission to provide Physical Security solutions to the Joint Community, by establishing Force Protection Systems Interoperability Standards, is captured in the lower half of the outer ring.

The updated logo, as a whole, embodies the SEIWG's commitment to the Department of Defense Joint Community. As an innovator of interoperability solutions through standards and architecture, as well as the continued success of a collaborative working environment, the SEIWG remains "at the ready" to address the ever-changing requirements of Force Protection.

## UPCOMING EVENTS

| Date | Event | Location |
|---|---|---|
| **28-30 March 2012** | **ISC West**<br>SEIWG Workshop on ICD 0101 Series and SEIWG Interoperability Verification Tool (SIV-T) | **Sands Expo and Convention Center Las Vegas, NV** |

ISC WEST
EXHIBIT HALL MARCH 28-30 2012
SANDS CONVENTION CENTER LAS VEGAS
ISC PREMIER EDUCATION SERIES
March 27-29, 2012

## SEIWG INTEROPERABILITY VERIFICATION TOOL (SIV-T)

**By: Mark Simeone**

The SEIWG has developed a SEIWG Interoperability Verification Tool (SIV-T) for the Joint DoD Services' use to determine if their physical security equipment is in compliance with the SEIWG suite of standards. The SIV-T, released in Jan 2012, is a software based application that supports SEIWG standards 0100, 0101, 0101A and 0101B with support in the works for SEIWG standard 0300 (CCDE to IBDC2 support). The tool supports Windows XP, Vista and Windows 7 operating systems.

A user-friendly Graphical User Interface (GUI) will indicate if a PSE is able to transmit and/or receive XML messages as described by the SEIWG standards. The SIV-T can also identity any messages that do not comply with the standard, or that are not valid for the specific device being tested for compliance. For messages that have been flagged as non-conformant to the standard, the tool will indicate which portion of the message is in error and provide recommendations to achieve compliance.

In addition to sending/receiving XML messages, the tool allows the operator to configure XML messages specific for a particular device (i.e. CCDE, Two-State Sensor, etc.). The XML message builder allows the operator to select an element and configure the parameters such as latitude, longitude, azimuth, elevation, etc. This message is then cut and pasted into the appropriate window and sent to the device under test. A tutorial video, in addition to a user's manual, is under development to aid the user in installing and using the tool.

The SEIWG has worked with Joint Service test labs and OEMs over the last year refining the tool. Presently the SIV-T is available for the DoD Joint Services and their industry partners to download from the SEIWG SharePoint site. To gain access to this site, send an email to seiwg@hanscom.af.mil for instructions.

A demonstration of the SIV-T will take place at the ISC West SEIWG Workshop on Thursday, March 29 from 2-4 PM. The SEIWG will be demonstrating the tool using Future Fibre Technologies' ® fibre optic intrusion detection fence sensor as the test device.

Also at the ISC Workshop, the SEIWG Chairman and other Service representatives will be in attendance and a presentation on the SEIWG Suite of Interoperability Standards and general SEIWG information will be provided before the SIV-T demonstration.

## Do You Know...the SEIWG Chief Architect?

***Name:*** Dr. Robert Rains, Ph.D., Engineering, 1972.

***Job:*** Dr. Rains has served as the SEIWG Chief Architect for three years. Dr. Rains leads a team that specializes in development of DoD Architecture Framework-compliant products both in support of the SEIWG and also in support of Force Protection/Physical Security programs that request assistance tailoring the Joint Force Protection Reference Architecture (JFPRA). Dr. Rains also provides engineering support to the US Air Force's Force Protection Branch.

***Employer:*** The MITRE Corporation

***Based at:*** USAF Electronic Systems Center (ESC), Hanscom AFB, MA. [NOTE: The Electronic Systems Center is expected to merge into the new Air Force Life Cycle Management Center (AFLCMC) by Sept 2012.].

***Hometown:*** Born in Long Beach California and raised in Compton, California; Los Alamos, New Mexico; El Monte, California; and Temple City, California.

***Interesting Facts:*** Dr. Rains has a B.A. in Mathematics from the University of California at Berkeley and an M.A. in Mathematics from the University of California at Irvine. He has eight children and 24 grandchildren. He enjoys playing chess, riding a bicycle, and reading science fiction.

***Do You Know Dr. Robert Rains?***

## Joint Force Protection Reference Architecture Technical Standards Profile Technical View TV-1

By: Sandy Freiter

Over the last several years, the SEIWG has developed and refined the Joint Anti-Terrorism/Force Protection Technical Standards Profile Technical View (TV-1). The TV-1 is a listing of standards and protocols currently available for use by the Services in the development and procurement of physical security systems, equipment and components within their domain and those proposed by the Services for use within the next 18 months. The TV-1 currently contains approximately 620 standards related to physical security in the following areas: common infrastructure; communication; command, control, and display equipment; access control; detection; surveillance; assessment; delay denial response; and facilities and installations. The TV-1 is available as a searchable Microsoft Access database and provides various information filters and display options.

The SEIWG TV-1 is an ideal tool for DoD program managers since it greatly reduces the need to conduct "open-ended" searches for program applicable standards. Each standard in the TV-1 has a synopsis and links to the standard or a location where the standard can be obtained. The TV-1 provides current titles and version numbers for contract references and is in sync with the DoD Information Technology Standards Registry (DISR) which identifies standards mandated for use within the DoD.

Using the TV-1 will increase consistency and interoperability across DoD programs by allowing Program Managers to draw from the same pool of standards and use consistent version numbers. Physical security equipment vendors can also benefit from the TV-1 by being cognizant during their design phase of the standards of interest to the DoD. The 2012 TV-1 is currently available on the SEIWG Force Protection web-site or can be requested at SEIWG@hanscom.af.mil.

## The Mission

**To coordinate and influence system architecture, technical design, and systems integration to foster interoperability of all physical security equipment to be used within the DoD.**

## The Primary Objectives

- ✓ Provide DoD and its industry partners the means to achieve Physical Security Equipment interoperability
- ✓ Coordinate and influence system architecture, technical design, and systems integration of Physical Security Equipment to be used within DoD
- ✓ Develop Interoperability Standards to guide the Military services and their industry partners in development of Physical Security Equipment
- ✓ Ensure new systems integrate with existing systems and minimize architectural redesign

The SEIWG strives to accomplish a cohesive and collaborative environment. Not only are Joint DoDAF Architecture Views developed, the SEIWG offers subject matter expertise (SME) to tailor them for individual service programs. Not only are Joint interoperability standards produced, but the SEIWG offers SME to aid in their implementation and provides tools to validate compliance.

## Benefits of Multi-Service Collaboration

- ✓ Speed delivery to the warfighter
- ✓ Reduce duplicative Research, Development, Test & Environment (RDT&E) costs
- ✓ Reduced errors and increased lessons learned
- ✓ Increased interoperability
- ✓ Advanced goal of "plug and play" solutions

# got interoperability?

**The PSEAG is the central manager for all Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E) within the Department of Defense. The SEIWG is a permanent working group of the PSEAG. The SEIWG's goal is to provide the DoD the means to achieve physical security equipment interoperability.**

| Service Representative | Organization | Telephone | E-mail |
|---|---|---|---|
| Mr. Rodney Rourk (chairman) | US Marine Corps | 843-218-4375 | rodney.rourk@navy.mil |
| Mr. Richard Goehring | US Army | 703-704-2524 | richard.h.goehring3.civ@mail.mil |
| Mr. Chris Hernandez | US Navy | 843-218-4613 | chris.hernandez@navy.mil |
| Dr. Jeff Wit | US Air Force | 850-283-2784 | jeff.wit@tyndall.af.mil |

**Visit our website at: http://www.acq.osd.mil/ncbdp/nm/pseag/about/seiwg.html**