



SEIWG

Security Equipment Integration Working Group

SUMMER 2013



Inside this issue:

New AF Principal Appointed	1
Army Representation Transitions	1
What's New in the SEIWG	2
TDAs, TAAs, and FN's, Oh My	3
Conformance Verification & Validation	4-5
JIGSAW	6
Defense Installation Access Control	7
SIV-T Updates	8
Do You Know...	8

NEW US AIR FORCE SEIWG PRINCIPAL APPOINTED

Welcome Richard Johnsen

Mr. Richard Johnsen
USAF SEIWG Principal

Rick Johnsen has 35 years of federal service; first serving as an active-duty US Air Force Security Policeman from 1978 until his retirement in 1998, then as a contract senior network engineer for the Headquarters Air Force Security Forces Center (HQ AFSFC) from 1998 to 2010. For the last three years, Rick has served as the Chief of Information Technology and senior engineer at the HQ AFSFC as a DoD civilian.

Though his expertise focused primarily on the infrastructure aspects of Information Technology (IT) and implementation of networking capabilities, which includes unclassified commercial Internet service through Top Secret networks at Security Police/ Security Forces units, Major Commands, and Air Staff locations worldwide, he has worked on numerous AF projects requiring highly technical and specialized research.

Mr. Johnsen is the Certification Authority/Agent for nearly 700 Security Forces Platform Information Technology (PIT) systems providing protection and assessment for Protection Level 1-4 resources deployed across the Air Force. In this capacity as a Trusted Agent of the AF SIAO, through comprehensive evaluation of technical and non-technical security safeguards, he provides risk-based security assessments to support accreditation decisions to the Designated Accrediting Authority (DAA). His team determines the extent to which the safeguards are implemented correctly, operating as intended, and producing the desired level of protection. They leverage the information assurance (IA) controls identified in DODI 8500.2, Information Assurance Implementation, in addition to program unique IA requirements and testing to establish acceptable security baselines for a decision by the DAA.

SEIWG ARMY REPRESENTATION TRANSITIONS

The SEIWG Army representation has transitioned from Mr. Richard Goehring of PM-FPS to Mr. Robert Bednarczyk, Product Manager, Force Protection Systems. Mr. Goehring is considered a plank holder for the SEIWG and served for 19 years beginning in 1994.

On behalf of the ASD for Nuclear, Chemical and Biological Defense Programs, the Physical Security Enterprise Analysis Group (PSEAG) and the SEIWG, we welcome Rob to the team and extend our sincere thanks to Richard for his contributions to the security and protection of our war fighters.

By:
Sandy Freiter,
SEIWG Project
Engineer

What's New in the SEIWG?

The Security Equipment Working Group (SEIWG) has been busy since the last issue of the SEIWG newsletter. The team awarded the next Spiral contract, began developing a new Interoperability Standard, and is implementing a Compliance Verification and Validation (CVV) process for two of the SEIWG products.

In June 2012, the SEIWG awarded the Spiral 6 contract to L-3 Global Security & Engineering Solutions (GS&ES) and Science Application International Corp. (SAIC). Both contractors are part of the Air Force Materiel Command's overarching Force Protection Security Systems (FPS2) contract which is designed to provide support for physical defense of installations and assets.

Under the Spiral 6 contract, the SEIWG began developing the Force Protection Systems Sensor Information Interchange Using XML Interoperability Standard which is more commonly known as SEIWG-0101C. This interoperability standard defines the structure and sequencing of information for communication between force protection sensor components and Command and Control Display Equipment (CCDE), also known as an annunciator. SEIWG-0101C is an update to SEIWG-ICD-0101B which was published by the SEIWG in June 2011. In developing SEIWG-0101C, the SEIWG responded to feedback from the Force Protection community requesting that the standard be more prescriptive. SEIWG-0101C presents a prescriptive, non-ambiguous operational profile for subscription-based data exchanges via a raw TCP/IP socket connection. The SEIWG expects the increased prescriptive nature of SEIWG-0101C will allow vendors to more easily

adhere to the standard. Additionally, the SEIWG plans to develop additional operational profiles in the future and will offer them to the force protection community as optional implementations for SEIWG-0101C. The current SEIWG XML communication standard, SEIWG-ICD-0101B, has been implemented by multiple sensor vendors and has strong support across the four Services. The SEIWG expects SEIWG-0101C to receive equally positive support from the force protection community when it is published in November 2013.

Also under the Spiral 6 contract, the SEIWG is developing the SEIWG Interoperability Verification Tool (SIV-T). This software tool assists force protection device developers in designing products that adhere to the SEIWG interoperability standards. It has the capability to check the content and structure of XML messages against the SEIWG interoperability standards (and past interface control documents such as SEIWG-ICD-0101A and 0101B) and make recommendations for achieving SEIWG compliance. An Installation Manual and a User's Guide are available with the tool.

Both the SEIWG-0101C Interoperability Standard and the SIV-T software are essential to the new CVV process the SEIWG is implementing. Department of Defense (DoD) programs are interested in force protection devices that comply with the SEIWG interoperability standards. However, until recently, there was no formal process for verifying and validating conformance with the SEIWG standards. During the past several months, the SEIWG developed a plan for formal CVV testing of force protection devices. The SEIWG is currently putting that CVV process in place. As of 1 May 2013, the SEIWG will be able to test several classes of force protection devices for compliance with SEIWG-ICD

What's New in the SEIWG? (continued)

-0101B. By 1 December 2013, the SEIWG will have the ability to test all device classes identified in the interoperability standards for compliance with SEIWG-ICD-0101B and SEIWG-0101C. For more information on the CVV test process, please see the related article on pages 4-5 or visit the SEIWG website at: <http://www.acq.osd.mil/ncbdp/nm/pseag/about/seiwg.html>.

TDA, TAA, and FN, Oh My!

By: Becky Terpstra, SEIWG Operations Manager

To promote information sharing, the Security Equipment Integration Working Group (SEIWG) has developed two types of agreements that can be entered into with U.S. or Canadian-based Enterprises and other U.S. Federal Government Agencies to receive SEIWG products.

Technical Data Agreements

For U.S. or Canadian-based Enterprises registered with the Defense Logistics Agency (DLA) Joint Certification Program (JCP), a Technical Data Agreement (TDA) can be entered into with the SEIWG. Once the SEIWG verifies the Enterprise's participation with the JCP, communication will be established with a single point of contact within the Enterprise to arrange delivery of SEIWG product through AMRDEC Secure Access File Exchange (SAFE). Applications are processed on a per document basis. The SEIWG will not manage or process multiple requests or applications that are submitted by the Requesting Enterprise's employees, business partners, affiliates, subsidiaries or industry partners. It is the Requesting Enterprise's responsibility to manage and control further distribution to its employees, business partners, affiliates, subsidiaries or industry partners in a manner that fully complies with the terms of JCP. The expiration of the TDA will correlate to the JCP expiration or at any time in which the U.S./Canadian Joint Certification Program Office terminates the Enterprise's Military Critical Technical Data Agreement. The TDA does not authorize the Enterprise to

establish equivalent agreements with non-U.S. or non-Canadian subsidiaries or affiliates (any Foreign person, business partners, affiliates, subsidiaries, industry partners or foreign government) to further share SEIWG Technical Data.

Trusted Agency Agreements

Any other U.S. Federal Government agency that is interesting in receiving SEIWG products that are controlled with distribution can enter into a Trusted Agency Agreement. Once an agreement has been established, it is the Requesting Agency's responsibility to manage and control further distribution to its offerors, contractors, or industry partners. The SEIWG will not manage or process individual requests for access that are submitted by the Requesting Agency's offerors, contractors, or industry partners. The Trusted Agency Agreement does not authorize the Requesting Agency to establish equivalent agreements to further share SEIWG artifacts with other U.S. Federal Government Agencies.

Foreign Nationals

For any Foreign person, business or government requests through the TDA or TAA, the Enterprise or Requesting Agency shall control distribution in accordance with the following:

- The International Traffic in Arms Regulations (ITAR) or the Enterprise's or Requesting Agency's equivalent to the ITAR process shall be followed before SEIWG artifacts are released

- If the ITAR process is approved, then only individual documents will be conveyed
- Under no circumstance will a Foreign National or Foreign Owned business be granted access to the SEIWG SharePoint site

Should anyone have an interest in receiving copies of any of the products, contact the SEIWG for additional information on how to enter into an information sharing agreement today!

For more information about the U.S./Canada Joint Certification Program, visit:

<http://www.dlis.dla.mil/JCP/Default.aspx>



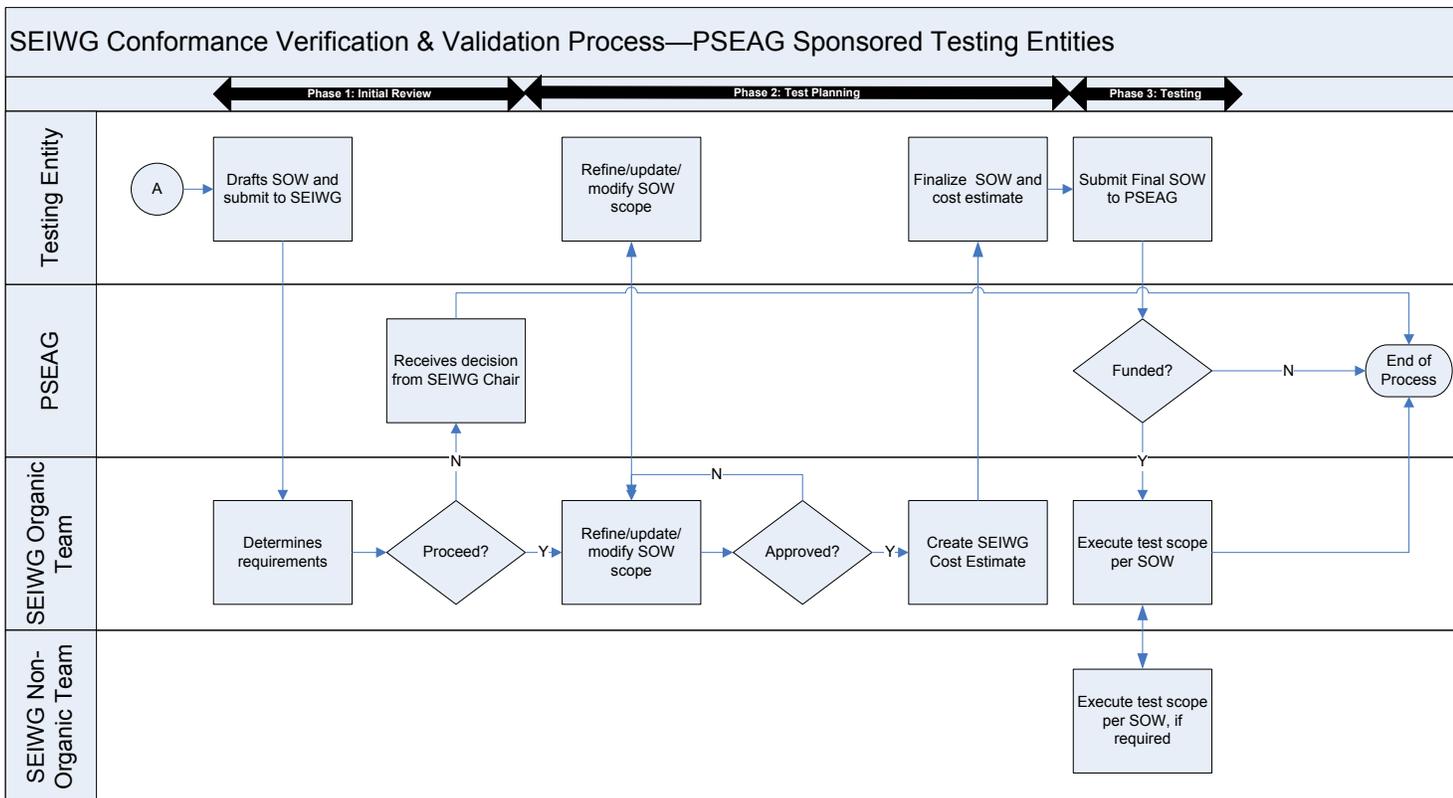
Introducing...SEIWG Conformance Verification & Validation (CVV) Process

The SEIWG has developed a Conformance Verification and Validation (CVV) Process that outlines the requirements that must be followed in order to declare a device conformant with SEIWG ICD-0101B Profile. The CVV Process Specification states the device/product may be a Command & Control Display Equipment (CCDE), a sensor, an access control system, or any other device to which the interface is defined in and applicable to selected SEIWG-ICD-0101B appendices and its companion Implementation Requirements Guide identified in SEIWG ICD-0101B Profile 1.

Precedence will be given to PSEAG sanctioned CVV tests that are specified to be required in a PSEAG sponsored project Statement of Work (SOW). All other unofficial commercial vendor test requests are required to be approved by the SEIWG Configuration Control Board (CCB) to determine if the test can be

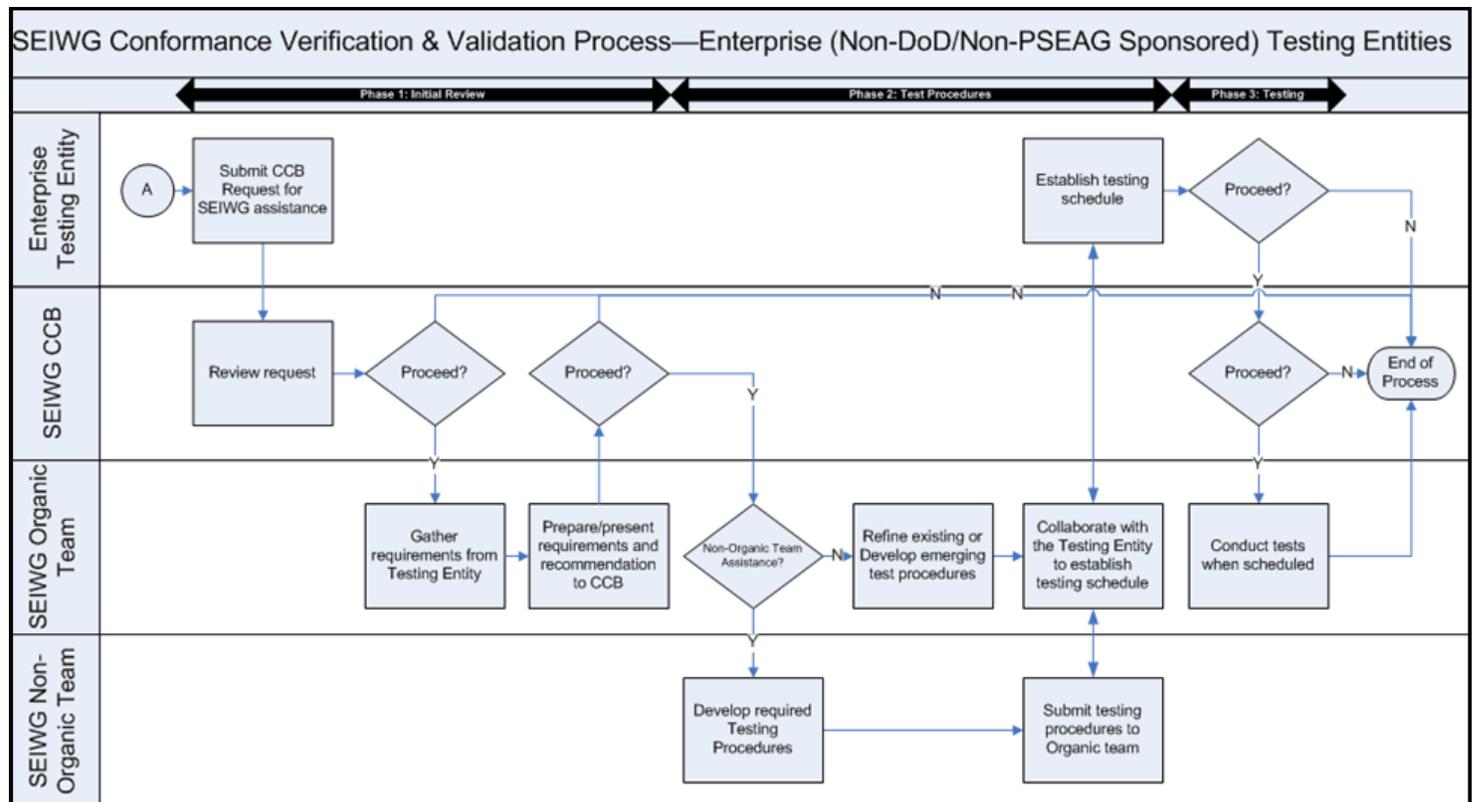
supported and if approved, will be scheduled as not to conflict with or delay any official PSEAG sanctioned CVV tests. The SEIWG reserves the right to not assist or support commercial vendor tests, and to delay or stop commercial vendor tests that are in progress at any time.

A copy of the CVV Process Specification, SEIWG-ICD 0101B Implementation Requirements Guide, or SEIWG-ICD 0101B Profile Description can be obtained by visiting the SEIWG website at: <http://www.acq.osd.mil/ncbdp/nm/pseag/about/seiwg.html>.



The CVV Process Steps

- ✓ Contact SEIWG to request CVV Support
- ✓ Define requirements
- ✓ Perform Self-Test
- ✓ Submit “Declaration of Readiness”
- ✓ Perform Internet test, where applicable
- ✓ Perform SEIWG-Witnessed Test, where applicable
- ✓ Determine Certification of Conformance (SEIWG function)



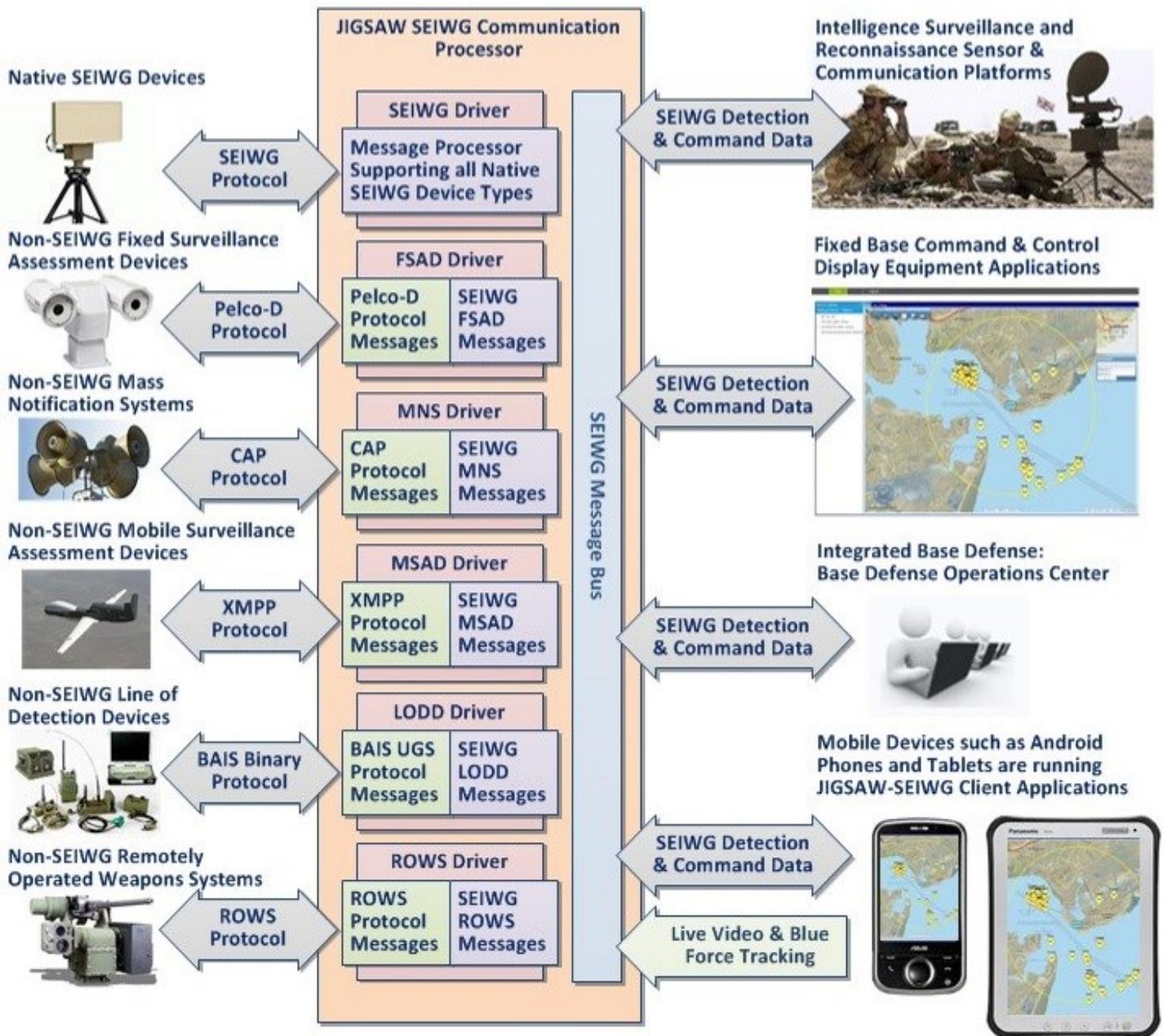
Complete Force Protection SEIWG Sensor Networks being Created Using JIGSAW

Innovation for SEIWG Sensor Communication:

PSEAG Project JIGSAW has developed an innovative approach that is 100% government owned. Drivers are now built that allow sensors that were not developed to SEIWG standards to be integrated as compliant SEIWG sensors with compliant CCDE (annunciators). SEIWG is exploring the concept of offering these drivers to industry to be shared across programs reducing engineering costs. The sensor data can then be published to automated processes, providing an ideal platform for data Fusion applications.

Innovation for Command & Control Interfaces:

Truly modular FPS Command & Control (C2) client applications are built using JIGSAW. Since all Sensor Detection and Command data follows SEIWG protocol, all messages to and from client applications are well defined. Mobile clients (smart phones, tablets) fixed based C2 clients and Integrated Base Defense (IBD) clients are currently running in a distributed JIGSAW enterprise architecture!





DEFENSE INSTALLATION ACCESS CONTROL

By: Rodney Rourk, SEIWG Chair

Preventing bad people from entering military installations is critical in protecting Department of Defense (DoD) personnel and resources. The Defense Installation Access Control (DIAC) Working Group has a key role in supporting DoD efforts to achieve an enterprise access control capability and enhanced Force Protection at installation entry control points.

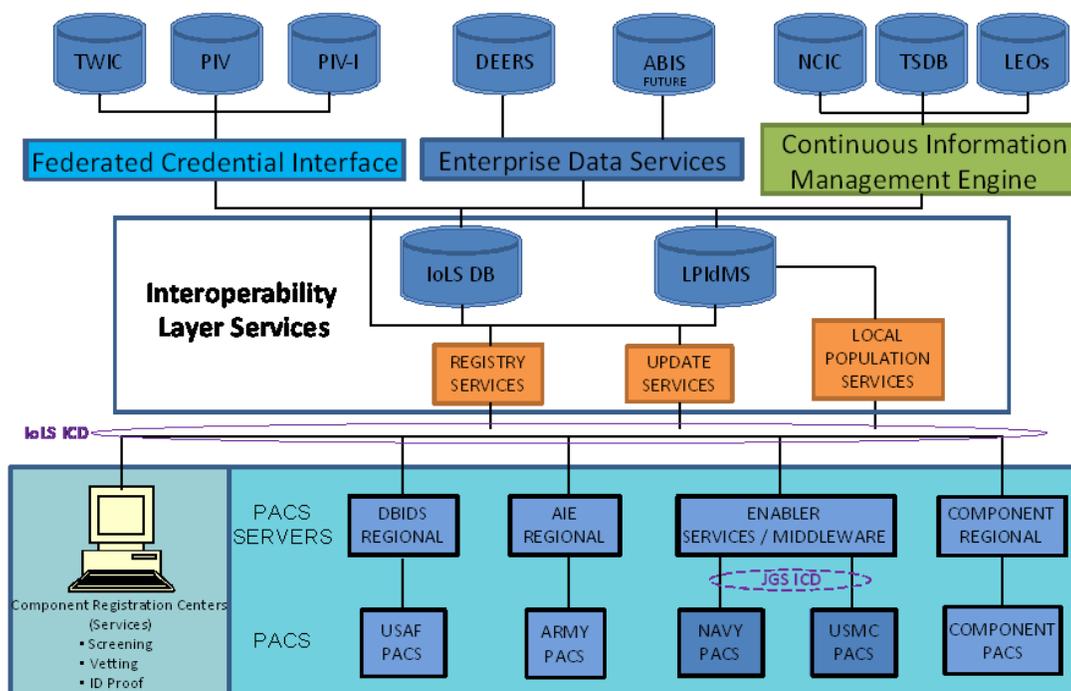
Today, DoD Joint Services/Components face a physical security vulnerability with the lack of standard authentication measures for credentials and continuous vetting of individuals against authoritative data sources, which prevents the Services from determining if persons entering military installations are a threat and leaves DoD assets vulnerable. Current DoD PACS procedures are governed and implemented under Service/Component-unique direction and are not fully interoperable between Service/Component installations.

No enterprise capability exists linking DoD installations for electronic authentication of physical access credentials to determine the fitness of personnel entering military installations in the United States. OUSD(I) Directive Type

Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control," mandated that DoD PACS must support a DoD-wide and Federally interoperable access control capability that can authenticate U.S. government physical access credentials and support access enrollment, authorization processes, and securely share information. Section 1069 of Public Law 110-181 tasked the Secretary of Defense (SECDEF) to determine the fitness of personnel entering military installations in the United States.

To aid the Service/Components in establishing compliance with policy, between FY2009 and 2012, the SEIWG led a group consisting of Joint Services/Component technical representatives in developing an Identity Management Enterprise Services Architecture (IMESA) and Interface Control Documents (ICD) that integrate DoD physical access control systems (PACS) with authoritative databases to register and authenticate credentials and continuously vet personnel who are authorized access to DoD installations worldwide to ensure no "bad" actors gain

(Continued on page 9)



UPDATES TO THE SEIWG INTEROPERABILITY VERIFICATION TOOL (SIV-T)

By: Mark Simeone, SEIWG Systems Engineer

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, 0101B and 0300 (CCDE to IBDC2 support). The SIV-T is being updated to support the latest version of the SEIWG Standard, 0101C. The tool supports Windows XP and Windows 7 operating systems. Further testing will be conducted with Vista this fiscal year.

A user-friendly Graphical User Interface (GUI) will indicate if a device under test is able to transmit and/or receive XML messages as described by the SEIWG standards. The SIV-T can also identify 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 developers with information they need to achieve compliance.

In addition to upgrading the SIV-T to allow testing with SEIWG Standard 0101C, new features have been added. Two of the biggest features that have been added include the ability to

have the SIV-T connect to more than one device at a time and the ability to configure test scripts that can draw configuration information out of device status reports and device configuration reports such as device name/type/category. This allows a generic test script to be written without having to redefine device information for each device under test. A scripting language called Lua was used to develop the scripts. Test scripts may also be developed utilizing features within the SIV-T utility. Other new features include control over execution of a script and searching for keywords or phrases within a test script. All of the new features are described in the Software User's Manual.

The SIV-T also has the capability to test a vendor's device over the Internet. This feature is useful if a vendor would like to have the SEIWG perform preliminary testing on their device to see if it is compliant with the SEIWG standard.

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. For more information about the SEIWG, visit our website at: <http://www.acq.osd.mil/ncbdp/nm/pseag/about/seiwg.html>

Do You Know...the SEIWG Systems Engineer?

Name: Mark Simeone

Job: Mr. Simeone has served as a SEIWG systems engineer for almost 5 years. He has been responsible primarily for performing quality assurance tests of the SIV-T and its associated test scripts, and the development of test procedures.

Employer: Bowhead Science and Technology

Based at: Charleston, SC

Hometown: Raised in Lexington, MA and currently resides in Westford, MA.

Interesting Facts: Mr. Simeone has a B.S. in Electrical Engineering from Tufts University. He has two college age children and enjoys photography, astronomy, sports, canoeing, and hiking.



Do You Know Mark Simeone?



Defense Installation Access Control

(Continued from page 7)
access.

Additionally, the concept for a Continuous Information Management Engine (CIME) capability was introduced that will send information to the PACS when data on an individual's fitness for access to an installation changes.

The CIME concept is to continuously vet identities that are registered within installation PACS that are connected to the Enterprise architecture against the FBI's National Crime Information Center (NCIC), which provides security alerts about felony warrants and wanted persons. The vision is to expand on the NCIC capability in the future to include the Terrorist Screening Database (TSDB) and each DoD Service's criminal justice information system. When paired with Web services, this capability facilitates data

exchange with each Service/Component-level PACS and delivers essential identity management information to the base Physical Security registration offices and the base entry control point security sentries.

The DIAC Working Group successfully completed an access control demonstration at three locations, including SSC Atlantic in Charleston. The demonstration validated the capability to immediately exchange data with an authoritative source [the Defense Enrollment Eligibility Reporting System (DEERS)] via a middleware/regional server within a Web-services architecture and to return accurate information to the PACS. Additionally, the DIAC working group demonstrated the CIME capability to send information to the PACS when data on an individu-

(Continued on page 10)

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



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

**SPAWAR Systems
 Center Atlantic**

**USMC Systems
 Engineering IPT**

Defense Installation Access Control (DIAC) (continued)

(Continued from page 9)

al's fitness for access changes. This capability was paired with an Interoperability Layer Services (IoLS) that ensured that data reached each Service-level PACS so that the entry control point security guard will know whether to authorize or deny entry.

The demonstration validated the art-of-the-possible for delivering the ability to exchange personnel identification data between installation PACS, IoLS, CIME, and test data representing authoritative systems (NCIC and TSDB). The SEIWG was instrumental in both demonstrations, both in contributing to developing the IMESA architecture, the Web service Interface Control Documents, and in providing technical engineering support to enable the Services' participation in the Joint demonstrations.

Currently, the DIAC is heavily engaged in supporting a live Joint Capability Technology Demonstration (JCTD) to validate the architecture, the Web services, and continuous vetting concepts, initially connecting the NCIC, then connecting TSDB and other authoritative sources in subsequent phases and demonstrations. A JCTD is a pre-acquisition activity, spanning two to four years, providing an opportunity to assess innovative technologically mature capabilities and determine the military utility.

JCTD Technical Demonstration One (TD1) was conducted in May, 2013. Each of the Joint Services performed their tests at designated test facilities. This demonstration validated the end-to-end functionality of the PACS, IoLS, and CIME in a lab environment prior to production implementation at bases designated to support the Operational Demonstration One (OD1) that is scheduled for October 2013.

The OD1 will demonstrate that OUSD(I) DTM 09-012, and Section 1069 of Public Law 110-181 are achievable through the IMESA. That is, that DoD PACS can support a DoD-wide and federally interoperable access control capability that can authenticate U.S. government physical access credentials and support access enrollment, authorization processes, continuously vet fitness, and securely share information. After OD1, the DIAC will continue to support subsequent JCTD phases and demonstrations to connect TSDB other authoritative sources, and potentially extend to a third year to include biometric identification capability.

Based on successful preliminary demonstrations in 2013, the IMESA full operational capability is expected in 2015.

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.



Visit our website at: <http://www.acq.osd.mil/ncbdp/nm/pseag/about/seiwig.html>