Naval Security Enterprise Newsletter

VOLUME II, ISSUE I 1ST QUARTER FY 2016

INSIDE THIS ISSUE:

Security Director's Message	1
Information Security	2
Physical Security	2
Personnel Security	2
Industrial Security	3
Enterprise Branch	3
Acquisition Branch	3
Security Education and Training	4

DUSN (P) Security Director's Corner

It's been a busy summer and early fall for security professionals. We continue to work issues related to the two OPM data breaches which came to light over the summer. Notifications for data breach two, which affected more than 22 million people, continue. As of mid-November OPM has contacted about seven million people and report that they are on track to finish notifications by the end of 2015. Additionally, by the middle of December OPM will establish a call center to answer questions from both people who have been notified that their information was stolen and from people who believe their data was taken, but have not yet received notification. Responsive information remains available at the DON OPM Data Breach website at http://www.secnav.navy.mil/OPMBreachDON/Pages/default.aspx

The tragic shootings at the Navy Operational Support Center (NOSC) and Armed Forces Recruiting Center in Chattanooga highlight the threat of "lone-wolf" attacks. Our office has worked with DoD, Navy, and the Marine Corps addressing direction provided by the Secretary of Defense to close gaps in security at off-installation locations. SECDEF directed the services pursue actions along three lines of effort – augment security including arming appropriate trained additional personnel; improve mass warning and notification capabilities; and improve physical and procedural security. This is a particularly complicated problem given the number of DoD off-installation locations and the multiple federal, state, and local jurisdictions and entities involved. Both services are moving quickly to identify and close gaps and the Secretary of the Navy is personally engaged in overseeing the efforts.

Some of you attended the DoD Security Conference in mid-September. DoD has not hosted a worldwide conference in several years. This was a great opportunity for security professionals from across the services and other DoD entities to share information. I thought the Defense Security Service/Center for Development of Security Excellence did a great job hosting the conference. We can expect a DoD level conference every two years.

Our office, working with the two services, will focus on building the DON Insider Threat Program capability during FY 2016 with the goal of having the service Insider Threat Hubs operational by the end of the fiscal year.

We are working quickly to stand up the Continuous Evaluation capability across DoD which monitors information about the cleared workforce in real-time. Both services are expanding their ability to monitor user activity on the classified networks. Both these capabilities, plus others will feed information into the service hubs giving us a better capability to early identify potential insider threats to information and physical security.

Service leads are, Director, Navy Staff (DNS) for the Navy program and Deputy Commandant, Plans, Policies, and Operations/Security Division for the Marine Corps program.

Lastly the events in Paris remind us that security can never be taken for granted. Each of you play a vital role for your command to make sure our efforts are as effective as possible. You make a difference every day with the work you do!

For more information on the following click the appropriate links:

Insider Threat

Counterintelligence

Information Security

The status of actions completed or pending related to general Information Security Program policy matters are included in the "Information Security Updates, ISB Newsletter Topics.pdf," available at the DUSN(P) Security SharePoint portal. This also includes information on the collaborative efforts between DUSN(P) Security-Information Security Branch and Cyber technology stakeholders. Our endeavors are part of the Department of the Navy's cyber/traditional security partnership for the protection of national security information and information systems.

Representative sample of topics covered are as follows:

- Authorities of the Secretaries of the MilDeps to grant waivers/exceptions to Information Security policy.
- Status of the rewrite of SECNAV M-5510.36.
- Request for Fundamental Declassification Guidance Review.
- Draft policy on DON Information/Information System (IS) User Access Program, includes requirements for derivative classification training prior to being granted access to classified IS and biennially.
- Requirements for use of Personal Portable Electronic Devices (PEDS).

To access the document in it's entirety and/or request permission to the DUSN (P) SharePoint portal, click here. Visitors requesting access to the portal must select the CAC email certificate.

"If you See something Say something."

Physical Security

Value of Physical Security and other organizational relationships. Physical Security and the protection of our facilities across the Department of Navy enterprise continue to evolve.

As we look at writing our inaugural SECNAV Instruction for physical security the recent events at Chattanooga remains a vivid reminder for security directors, managers and others in the security profession. We also have a fiduciary responsibility of not only ensuring facilities are compliant internally, but also external relationships are proactive in the security and protection of the mission, personnel, and visitors. Currently, uniform principles are being reviewed to assist local commanders who are considering augmenting security at their facilities who are not regularly engaged in, or directly supervising security or law enforcement activities. Contact information: don_security_phys@navy.mil

Personnel Security

Continuous Evaluation!

The Continuous Evaluation cell continues to process personnel and will be adding another 125K personnel to the system the first week of December. The CECD system identifies personnel who have had a change in their life which is reportable under the National Security Adjudicative Guidelines, but have potentially failed to report.

The system will notify the command with the name of the individual and the unreported incident. The command is then required to validate and submit an Incident Report in JPAS.

OPM Investigation Changes:

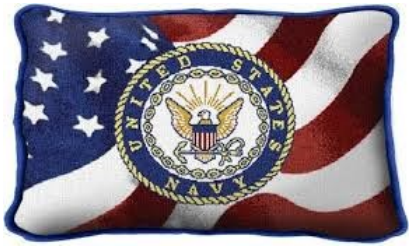
The Tier 3 and Tier 3R became effective 1 October 2015 and have replaced both the NACLC and the ANACI. There are specific conditions where you would order the Tier 3 or 3R depending on situation and position of the member.

Electronic Questionnaires for Investigations Processing (eQIP):

After the OPM data breach, eQIP was disabled for several weeks, but at this point all systems are operational. All accounts should have been reset and be accessible by the user.

Detailed information for these issues is available at http://www.secnav.navy.mil/dusnp/Security/Pages/PersonnelSecurity.aspx

Industrial Security



Defense Security Service

DUSN (Policy) office is working with the Defense Security Service (DSS) to create the first Industrial Security Basics Course.

This course will provide an overview of various industrial security databases and systems used in the NISP to our government Industrial Security representatives, Counter-Intel personnel and DoD Security Specialists student base with little or no industrial security background or experience.

This course is in the Beta testing phase and is expected to be available to industry Calendar year 2016. The DUSN (Policy) office will provide up-to-date information to everyone as time grows closer for implementation.

Industrial Security DD Form 254

DUSN (Policy) is working with the Defense Security Service (DSS) ICO the National Industrial Security Program (NISP) Contract Classification System (NCCS) DD Form 254 database which is part of the Wide Area Workflow (WAWF).

The database is currently in the "Operational Acceptance Testing" (OAT) phase. The expected roll-out date of the new DD Form 254 database is Calendar year March 2016. National Interest Determinations (NIDs) DSS plans to implement the following ICO National Interest Determinations: 1. Update the DSS NID website and ensure templates are included. 2. Include GCA POCs on the NID website so that program offices can dialog with their proper HQ personnel regarding NID submission packages. 3. Create a NID share-point site for DSS information pertaining to NIDs.

Enterprise Branch

Recent, high profile insider threat-related incidents highlight the requirement to improve the manner in which the Department of the Navy (DON) safeguards classified national security information from unauthorized disclosure and protects its personnel from potential workplace vulnerabilities.

There are three offices that oversee Insider Threat:

* DON Insider Threat: Deputy Undersecretary of the Navy for Policy (DUSN (P))
* Operational Navy: Director of the Navy Staff (DNS)
* Marine Corps: Deputy Commandant for Plans, Policies and Operations (DC, PP&O)

The DON Insider Threat Program Implementation Plan is currently in staffing for coordination. It's the DON roadmap for implementing the National, DoD and Navy requirements for an Insider Threat Program and Hub. This plan is a living document and will evolve as requirements are further refined.

The DoD Insider Threat Management and Analysis Center (DITMAC) is the DoD Insider Threat Hub that will provide support to DoD personnel, promoting collaboration and information sharing on insider threats to DoD personnel, information and facilities. They are also developing a DoD case management tool that will be the single repository for DoD insider threat related information.

Please follow the link to see the mandatory threshold reporting requirements to the **Insider Threat Hubs Click Here!** POC for this article is Tony Simmons, DON Insider Threat Program Manager (703) 601-0537 tony.simmons@navy.mil.

Acquisition Security Branch

The Acquisition Security Branch spent the last year identifying policy gaps and alignment issues within the Program Protection construct. We have several initiatives for FY 2016. Our first objective is to initiate a new DON Research and Technology Protection Working Group Charter.

The purpose of this charter is to establish a robust multidisciplinary Department of the Navy (DON) Acquisition Security Working Group (ASWG), formally known as the DON Research and Technology Protection (RTP) Working Group (established in 2006 but inactive since 2012).

The ASWG will work to develop, coordinate, and assist in the implementation of Acquisition Security and related policies in order to align program protection activities across the DON. If you are interested in providing input or have questions about the ASWG you can email us at: ***don_don_security_acq@navy.mil.***

Security Education and Training Awareness

Have you ever wondered what it takes to become a component security professional? There are many theories that are probably based on one's technical capability, job experience and education to name a few. Currently the Defense Security Service Center for Development of Security Excellence (CDSE), Education Division, offers a curriculum of advanced and graduate courses. The CDSE Education curriculum is designed for DoD security professionals seeking to broaden their knowledge and understanding of the security profession. All of the courses are tuition free, and offered in a virtual instructor led environment. CDSE is accredited by the Council on Occupational Education (COE), a national accrediting authority recognized by the U.S. Department of Education. All of the courses have been or will be evaluated by the American Council (ACE) for credit recommendations. The ACE connects workplace learning to universities by helping employees gain access to academic credit for formal courses and examinations taken outside traditional degree programs. The CDSE program offers certificates in five concentrations. Students can earn education certificates in Risk Management, Security Leadership, Security Management, Security (Generalist), and Systems and Operations. More information about the certificate program is available at: http//www.cdse.edu/education/certificates.html

CDSE LINK

Points of Contact:
Mailing Address:
Deputy Under Secretary of the Navy, (Policy)
1000 Navy Pentagon, Rm 4E572
Washington, DC 20350

Acquisition Security
DON_SECURITY_ACQ@NAVY.MIL
Industrial Security
DON_SECURITY_IND@NAVY.MIL
Information Security
DON_SECURITY_INFO@NAVY.MIL
Insider Threat
DON_SECURITY_INSIDER_THREAT@NAVY.MIL
Personnel Security
DON_SECURITY_PERS@NAVY.MIL
Physical Security
DON_SECURITY_PHYS@NAVY.MIL
Security Education, Training and Awareness

Useful Links:

-Naval Security Enterprise on Navy Knowledge Online: https://www.nko.navy.mil/group/naval-security-enterprise/naval-security-enterprise1

- Department of The Navy, Security Executive: http://www.secnav.navy.mil/dusnp/Security/Pages/Default.aspx

- Department of The Navy, Security Education, Awareness and Training: http://www.secnav.navy.mil/dusnp/Security/Pages/SETACommMgmt.aspx

- Center for Security Development of Security Excellence: http://www.cdse.edu/index.html

- Center for Security Development of Security Excellence, My SPeD Certifications: https://i7lp.integral7.com/durango/do/login?ownername=dss&usertype=candidate

-Defense Security Service: https://stepp.dss.mil/SelfRegistration/