Naval Security Enterprise Newsletter

2ND QUARTER FY 2016

INSIDE THIS ISSUE:

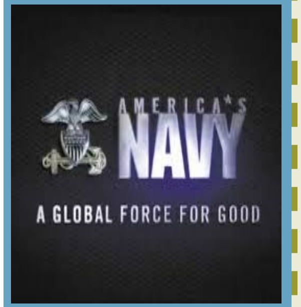
DUSN (P) Security Director's Corner

It's been a busy year already. This year's National Defense Authorization Act (NDAA FY16) directs the Department of Defense DoD to provide Congress several different reports concerning our implementation of the National Insider Threat (InT) Program standards and our efforts to improve execution of our Personnel Security mission. The provision of these reports to Congress falls right in line with Department of the Navy (DON), Navy and Marine Corps efforts to reach Initial Operating Capability (IOC) for DON and Service Insider Threat Programs by the end of FY16.

There are multiple requirements for achieving InT program IOC including building out an approved, effective Personnel Security Continuous Evaluation (CE) capability initially covering the cleared military, civilian and contractor workforce; User Activity Monitoring on at least one classified network; designing and building out component InT Analytic/Monitoring Hubs; information sharing and storage agreements aligned with existing privacy and records management laws/rules/regulations; effective interface between security, law-enforcement, counter-intelligence activities, commanders, Human Resources offices and installation support activities allowing us to identify, mitigate, and respond to potential insider threats. Getting InT right, with appropriate authorities and to standards, as quickly as possible is the main focus of effort in our office this FY.

In addition we continue working issues related to the Chattanooga shootings. Under guidance issued by the Secretary of Defense and Secretary of the Navy, the Services, military departments, and various DoD entities are pursuing improvements to physical security at off-installation sites, particularly recruiting offices and stations. We are working to improve mass-warning and notification capabilities across the Services and geographical locations. Everyone connected with DoD whose offices are in or near a geographic location of an active-shooter or other security event should be notified of the event so they can respond appropriately regardless of their service affiliation. We have worked successfully to improve guidance concerning arming of non-security/law enforcement personnel at off-installation locations where it makes sense to do so.

The White House announced the results of the Office of Personnel Management (OPM) Data Breach 90-day Review this month. As a result of the study the government will carve out the Federal Investigative Services Division and stand up the National Background Investigations Bureau (NBIB) and a more independent capability inside OPM. DoD will take over improving and providing data protection for the information technology capabilities that will support NBIB in the future. More on this as plans get implemented.



Information Security

The **ALNAV 001/16**, "Unauthorized Disclosures of Classified Information and Controlled Unclassified Information on DON Information Systems" was released early January 2016.

The ALNAV 001/16 strengthens responsibilities, identifies training and reporting requirements, and assigns actions to be taken by DON personnel as users on DON networks and information systems in the event of an electronic spillage (ES) or unauthorized disclosure (UD) of classified information and Controlled Unclassified Information.

The release of the ALNAV promulgated the approval of the DON ES Reporting Process which provides specific steps for commands to follow upon discovery of an ES of classified information on DON networks or information systems. The ALNAV 001/16 and associated references, including the DON ES Reporting Process are posted to the public key infrastructure (PKI) enabled DUSN(P) Information Security SharePoint Portal.

Click here to visit the DUSN(P) SharePoint portal for more information on Department of Defense DoD and Department of the Navy DON Information Security Program policy and reporting requirements. This website provides reminders and notices to assist Command Security Managers with some of their day-to-day security management responsibilities. Visitors requesting access to the portal must select the CAC email certificate.

"If you See something Say something."

Physical Security

Law Enforcement Officers Safety Act of 2004 (LEOSA)

The Department of the Navy (DON) will be coming forth with the Law Enforcement Officers Safety Act (LEOSA) program policy for the U.S. Navy and U.S. Marine Corps. In accordance with DoD Directive 5525.12, LEOSA implements sections 926B and 926C of Title 18, United States Code (U.S.C.) and incorporates section 1089 of Public Law 112-239 for (military and civilian) law enforcement personnel within the DoD who possessed statutory powers of arrest or authority to apprehend pursuant to section 807(b) of Title 10, United States Code (also known as article 7(b) of the Uniform Code of Military Justice).

Signed into law on July 22, 2004, LEOSA is intended to afford qualified active and retired law enforcement officers the privilege of carrying a concealed firearm in all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and all other U.S. possessions. By definition LEOSA is for personnel who were authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for any violation of law. Retired law enforcement personnel must have served a minimum of 10 years' service and will require annual qualifications in standards of training for firearms. Those who completed training qualifications and probationary periods of employment, but were separated due to a service-connected disability are also eligible for LEOSA enrollment. For more information please email the Physical Security Branch at:

DON_SECURITY_PHYS@NAVY.MIL

Personnel Security

The Office of Personnel Management (OPM) has implemented Tier 3 (T3) and Tier 3 Reinvestigation (T3R). T3 is the investigation required for positions designated as non-critical sensitive and/or requiring eligibility for access to Confidential or Secret information. T3R is the reinvestigation product required for the same positions. The Standard Form (SF) 86 is used to conduct these investigations. Tier 3 and Tier 3R investigations will be identified as T3 and T3R in OPM's databases. T3 investigations will be identified by case type code 64, and T3R investigations will be identified by case type code 65B.

The Tier 3, requested on the SF 86, is the minimum background investigation required for all military personnel, as well as civilians or contractors who occupy a non-critical sensitive position or have access to classified information.

A Tier 3 investigation must be submitted for military personnel who retire or separate from the military and become employed as a federal civil servant as a first time employee, unless the member was previously subject to a Single Scope Background Investigation.

Case type Tier3R, (Case Type Code - 65B), is requested if the subject requires a reinvestigation. Tier 3R, requested on the SF 86, is the periodic reinvestigation for military, civilian and contractor personnel who occupy non-critical sensitive positions or require access to classified information. The submission of SF 87 or electronic fingerprints is required, if previous results are not on file at OPM.

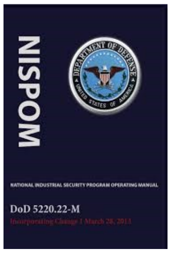
OPM no longer offers the Access National Agency Check with Inquiries (ANACI) and National Agency Checks with Law and Credit (NACLC). Additionally, per the Federal Investigative Standards, OPM will no longer offer the ANACI with an Enhanced Subject Interview (ANACI-P) product. **For additional information please email the Personnel Security Branch at:**

DON_SECURITY_PERS@NAVY.MIL

Industrial Security

Defense Security Service

The DUSN (P) Industrial Security Branch has been working with the Defense Security Service (DSS) Center for Development of Security Excellence (CDSE) to create the: Industrial Security Basics courses. The main course developed was the **Acquisition and Contracting** in the NISP course. The course consolidated the training curriculum for Industrial Security Databases and Systems eLearning courses which were all launched on January 11, 2016.


NISPOM
NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL
DoD 5220.22-M
Incorporating Change 1 March 28, 2013

These courses are significant as they are the first industrial security courses CDSE has developed specifically for the government security specialist. Not only are they available as individual courses, they are also being incorporated into an existing curriculum, Basic Industrial Security for the Government Security Specialist and the January 11, 2016 Industrial Security for Non-Security Government personnel was also launched. The courses provide students with a high-level overview of Industrial Security (IS) Basics, including the purpose and regulatory foundations of the NISP, the overall structure of the NISP, and the fundamental NISP roles and responsibilities. DSS Industrial Security Representatives (IS Reps), DSS Industrial Security Systems Professionals (ISSPs), DSS Counterintelligence (CI) Personnel, DSS Industrial Security Headquarters personnel and other DoD Security Specialists with Industrial Security responsibilities are the target audience.

Course information can be found at http://www.cdse.edu/catalog/elearning/ or contact don_security_ind@navy.mil.

Security Enterprise

Coming Soon: Identity Operations (IdOps) Charter and Instruction!

What is IdOps? It is the synchronized application of biometrics, forensics, and identity intelligence to establish identity, affiliations, and authorizations of an individual to deny anonymity to the adversary and to protect assets, facilities, and forces.

Why is it important to develop a charter and instruction for IdOps? Simple, it is important to develop a charter and instruction for IdOps as a means for the Department of the Navy to define and establish roles and responsibilities for validating a person's unique identity. Some of the unique ways we use biometrics: (1) The Defense Manpower Data Center uses fingerprint technologies to validate who you are when you are issued and reissued your Common Access Card (CAC) to access DoD facilities and computer networks. (2) Fingerprints are collected for Background Investigations and Personnel Security Investigations to validate a person's identity and to conduct a criminal check through the FBI fingerprint repositories. (3) We use eye scan technologies, collect fingerprints and DNA to validate or discover the existence of unknown potential threat actors and connect individuals to other persons, places, events, materials, and characterizing their level of potential threats to US.

What is next? The IdOps Charter will formally establish the IdOps Working Group under the Navy Security Enterprise (SECNAV Instruction 5500.36). The IdOps Working Group will report to both the Advisory Group and the Executive Committee. More to follow!

Acquisition Security

Better Buying Power Principals (BBP) defined by the Honorable Mr. Frank Kendall, Under Secretary of Defense for Acquisition, Technology, and Logistics. For today's article, I want to focus on Principal number 10.

Principle 10: We should have the courage to challenge bad policy. Deming' 8 of 14 points states that successful organizations "drive out fear." He meant that a healthy organizational culture encourages members to speak out and contribute ideas and inform management about things that are not as they should be. We should not be afraid to speak up when we see bad policy, or policy applied too rigidly where that clearly isn't the best course of action. We should not be afraid to offer creative ideas or to challenge conventional wisdom, and we should encourage others to do so as well. None of the BBP initiatives, or their more detailed implementation guidance, are intended to apply in every possible situation. All of us should be willing to "speak truth to power" about situations in which policies simply are not working or will not achieve the intended result. The annual PM Program Assessments that I started last year and included in BBP 3.0 proved to me that the chain of command has a lot to learn from the very professional people on the front lines of defense acquisition. This applies to all the professionals who support or work for those PMs also. Continuous improvement comes from the willingness to challenge the status quo.

The Principles Suggested by 24 Acquisition Experts

Principle 1: Continuous improvement will be more effective than radical change.
Principle 2: Data should drive policy.
Principle 3: Critical thinking is necessary for success; fixed rules are too constraining.
Principle 4: Controlling life-cycle cost is one of our jobs; staying on budget isn't enough.
Principle 5: People matter most; we can never be too professional or too competent.
Principle 6: Incentives work—we get what we reward.
Principle 7: Competition and the threat of competition are the most effective incentives.
Principle 8: Defense acquisition is a team sport.
Principle 9: Our technological superiority is at risk and we must respond.
Principle 10: We should have the courage to challenge bad policy.

Security Education, Training, and Awareness

SPēD Certification Maintenance Changes: Staying current with your certifications is an ongoing requirement and there have been a number of positive changes to the certification maintenance process. First, there is only one certification renewal form (CRF) to use in order to submit your professional development units (PDUs). Second, you only need to maintain one certification and that is your most recently conferred core (SFPC, SAPPC, SPIPC) certification. You must attain **100** professional development units (PDUs) altogether, regardless of the number of certifications you have. Third, you have a specific two-year certification maintenance cycle with start and end dates. Example, if your certification renewal expiration date for your most recent core certification is June 30, 2016, and you submit your 100 PDUs, your new expiration date will be June 30, 2018. Once you attain 100 PDU's within your maintenance cycle and submit your certification renewal form (CRF), your certification status will continue to indicate "certified." The Center for the Development of Security Excellence (CDSE) recommends submitting your CRF no earlier than 180 days prior to your certification (s) expiring. For additional information on SPēD Certification Maintenance, click here.

CDSE LINK

CDSE Hosts:

Registration Now Open!

DITMAC and the DoD Insider Threat Program Webinar on 3/7/16 at 12pm

Join the Defense Insider Threat Management Analysis Center for a live discussion of their role in the DoD Insider Threat Program.

NEW DATE!

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

Email Addresses:

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
DON_SECURITY_SETA_US@NAVY.MIL

Useful Links:

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/Login.aspx