Naval Security Enterprise Newsletter

3RD QUARTER FY 2016

INSIDE THIS ISSUE:

DUSN (P) Security Director's Corner

Security remains a hot topic across DoD. Just last week the Deputies Management Action Group (DMAG) chaired by the Deputy Secretary of Defense received a brief "Strengthening Defense Security" that discussed five separate security topics. The DMAG is the primary civilian-military management forum that supports the Secretary of Defense, and addresses top Departmental issues that have resource, management, and broad strategic and/or policy implications. This is good news for Security Professionals and shows the commitment of top leadership towards ensuring security remains a high priority. We continue to be affected by blowback from the OPM data breach. The backlog of investigations at OPM has grown to beyond 500K. Timelines to complete OPM investigations for all tiers are increasing and the "get well" plan extends into 2020. Make sure you do your part by ensuring that investigations and reinvestigations are initiated in a timely manner. I am excited about the upcoming Center for Development of Security Excellence (CDSE) 2016 Virtual Security Conference on 26 and 27 July 2016. Registration is now open and information/link is on page four. I also encourage each of you to register in the Security Directorate SharePoint website. This website should be your first stop when you have questions about executing your security responsibilities. Please see the link below. As I travel around to visit the Services I am extremely impressed by your dedication and hard work. Be the best resource you can be for your Commander by gaining and maintaining your Security Professional certifications via CDSE.

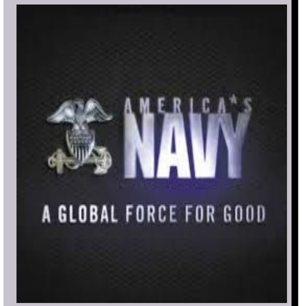
Website Registration

The DUSN (P) Security Directorate would like to encourage readers to register for the Security Directorate SharePoint website which is CAC enabled in order to receive the latest security announcements and updates posted on the website. The latest announcement is the Virtual DoD Security Conference which is scheduled for July 26-27, 2016. Register with the SharePoint website to receive upcoming registration updates click on the website icon:

Community Updates

The DUSN(P) Security Directorate would like to request security professionals submit noteworthy success stories or relevant articles that can be featured in future editions of the newsletter. We are looking for articles that highlight individual achievement (s) and team success within the Department of the Navy (DON). The Security Directorate would like to encourage more DON community involvement in order to facilitate better communication throughout the department. Members should feel free to send input (s) to the Security Education, Training, and Awareness Branch at: DON_SECURITY_SETA_US@NAVY.MIL

Information Security



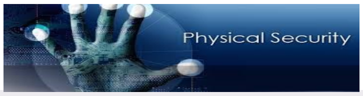
The **ALNAV 019/16**, "Acceptable Use of Authorized Personal Portable Electronic Devices (PPED) in Specific Department of the Navy Spaces" was issued 25 March 2016 (DTG 251830Z Mar 16). The ALNAV is a coordinated Deputy Under Secretary of the Navy Policy (DUSN(P)) Security and Department of the Navy (DON) Chief Information Officer message as part of the DON's cyber/traditional security partnership for the protection of national security information and information systems. It was primarily issued in response to requests for guidance on this matter from Security Specialists who attended the Mobility and Cybersecurity Panels at the DON Security Enterprise Symposium - April 2015. The ALNAV applies to all DON Sailors, Marines, civilians, and contract personnel; and, outlines the PPED capabilities permitted and not permitted in DON spaces where collateral classified information is processed, transmitted, stored, or discussed in order to allow PPED use while minimizing risk to DON information. The ALNAV does not prevent the Commanding Officer from issuing stricter policy in accordance with the needs of their commands. Definitions, additional requirements, potential consequences for non-compliance, and responsibilities are also outlined in the ALNAV. A copy of the ALNAV is posted on DUSN(P)) Security Directorate CAC enabled website to access the ALNAV **click here** under announcements. Members are encouraged to access the portal using their CAC and register to receive any updates, announcements, and additional information.

Physical Security

Physical Security Perspectives, Trends and Lessons Learned from Recent Security Assistance Visits (SAVs) and IG Inspections

How are you optimizing and adding value to your physical security program (PSP)? As with any security disciplines we want our PSP to be cost-effective, with leadership buy-in and not viewed as a hindrance to employees, but value-added. Deputy Undersecretary of the Navy for Policy (DUSN(P)), Security Directorate has made outreach to the Navy's security professionals, afloat and ashore, an actionable and collaborative experience. One way is through an emerging partnership with the Navy Inspector General (NAVIG), who frequently assesses commands as a staple of its core competency. This relationship has gleaned additional insight and value for our office as well. Our security professionals have visited HQ Commander Navy Installations Command (CNIC), HQ Naval Sea Systems Command (NAVSEA), Naval Education and Training Command, NAS Pensacola, NSA Mechanicsburg, NAS Norfolk and Naval Base San Diego thus far in 2015/16. Future SAVs and IG Inspections will continue.

The Security Directorate's long-term goal is to bridge the divide between the policy shapers and the commands implementing the latest guidance, so future policy can benefit from the familiarity and be better informed through cooperative dialogue from across the Naval PSP enterprise. Has your installation started a community of interest for PSP? If not, perhaps it's time to share knowledge and best practices while networking to make the community better. For additional information please email us at: DON_SECURITY_PHYS@NAVY.MIL



"If you See something Say something."

Personnel Security

NP2 Update:

New OPM/FIS Secure Portal (NP2)

As of April 4, 2016 the New NP2 Portal is up and running. DUSN(P) Security will no longer accept request for NC4 OPMIS Portal registration or reactivation of accounts.

At this time security personnel assigned to ships, without a Personal Identity Verification (PIV)/Common Access Card (CAC) 16 digit UPN's, that are currently out to sea (only) and can't upgrade their certificates need to be put on the two factors PIV/CAC authentication. Upon returning to Port ships security personnel users (only) will need to get an updated PIV certificate added to their certificate and be modified for PIV Authentication for access to NP2.

Please continue to submit NP2 request via the Echelon II Command Security Manager. OPM has a back log for in processing NP2 access account request. Please inform subordinate commands that delays will be between 8 - 10 days for a portal invite. OPM has added additional personnel to the Helpdesk to address the backlog of portal request.

DUSN(P) Security will continue to update the department on any changes regarding NP2.

Secure Web Fingerprint Transmission (SWFT) Plus Enrollment

The SWFT Plus policy/implementation plan is being developed and will be disseminated to the fleet upon completion. The directions for obtaining a SWFT Plus account and procedures for purchasing the required equipment will be included in policy. SWFT Plus implementation will give the DON the ability to use a web-based approach for enterprise capture, storage and transmission of electronic fingerprints to the Office of Personnel Management. Please send inquiries to the email address listed at:

DON_SECURITY_PERS@NAVY.MIL

Industrial Security

NISP Contract Classification System (NCCS). The National Industrial Security Program Contract Classification System (NCCS) provides a mechanism for creating and routing a DD 254 electronic equivalent form to and from the respective security offices/ organization of both the government and the prospective vendor.

Users: The CAC card will be mandatory for all NCCS users: Vendor/Contractor, Government Contractor and Government.

NCCS Benefits: Allows the DoD and Federal agencies to effectively monitor, manage and oversee contracted security requirements. The NCCS will be the repository for executed DD 254s between the Government and contractors.

The DD Form 254 paper contract process can be done electronically which alleviates untimely, inaccurate, duplicative, conflicting and unverifiable receipt. The Defense Security Service (DSS) is the functional owner of NCCS and will set the functional requirements for NCCS. DSS will also manage configuration control and required changes to the system.

The NCCS currently is in an Operational Acceptance Testing (OAT) phase that will carry through Summer 2016 with a planned implementation timeframe by end of CY 2016/Spring 2017.

SECNAV Industrial Security Policy Update. As of the 3rd QTR FY 2016 DUSN (Policy) Industrial Security Branch is in the process of writing the new SECNAV Industrial Security Manual. Progress on updates will be provided on a quarterly basis. For additional information please email us at:

DON_SECURITY_IND@NAVY.MIL

Enterprise Security

On 05 May 2016, the Secretary of the Navy issued SECNAVINST 3070.2 Operations Security, requiring robust implementation of the Naval Operations Security (OPSEC) program.

The SECNAVIST 3070.2 pertains to multiple fields of expertise, not just security professionals including: public affairs, information warfare, acquisition, and antiterrorism/force protection (ATFP). Current threats require we redouble our efforts combating the loss of critical information through enhanced collaboration between the OPSEC program manager, the security office, public affairs, information warfare, ATFP, and other security professionals. Exploitation of Internet based capabilities, publicly released information, and other UNCLASSIFIED, but potentially sensitive data, gives adversaries the ability to undermine our technological edge, threaten our personnel, and potentially compromise our operations.

The OPSEC policy includes two useful resources: a self-inspection tool and a DON Critical Information List (CIL). The self-inspection tool facilitates an internal assessment of compliance with DOD and DON standards, and provides higher level Commands the ability to evaluate the effectiveness of subordinate programs. The DON CIL provides an overview of what the SECNAV considers "critical information" across the Department. Each Command is still expected to develop their own CIL based on local and specific operational threats.

The Department has designated two OPSEC support capabilities, the Naval OPSEC Support Team (NOST) located at Navy IO Command Norfolk, and the Marine OPSEC Support Team (MOST) located at the Marine Corps Information Operations Center Quantico. Both OPSEC organizations provide excellent reach-back support to the operating forces.

Specifically, the NOST is responsible for the Navy OPSEC Program Manager course (CIN: J-2G-0966) and development of annual training hosted on NKO and Marine Net. They also provide program assistance, awareness resources, assessment and planning support, and various briefs and presentations upon request. The NOST can be reached via any of their websites to include http://www.Facebook.com/NavalOPSEC, the OPSEC link on the Navy's Homepage or by emailing the team at opsec@navy.mil.

The MOST conducts external OPSEC assessments (surveys) of Marine Corps units and supports unit signature management profile analyses; provides operational and tactical level OPSEC expertise to Marine Corps Forces; advocates for and coordinates OPSEC training to meet Marine Corps training requirements; and supports OPSEC program development. The MOST can be reached via the OPSEC link on the MCIOC Homepage or by emailing the team at OPSEC@usmc.mil.

Acquisition Security

Acquisition Security/Program Protection Training Opportunity

Air Force Life Cycle Management Center hosts a quarterly 3-day Acquisition Program Protection Planning (PPP)

This course is designed for Program Managers, System Engineers, and Security Staff in developing and executing acquisition program protection efforts. The course covers all interrelated processes, to include identification of Critical Components, AQ Intel/Cyber Security Threats, Anti-Tamper, Cyber Security Risk Management, Supply Chain Risk Management, Counterfeit Prevention, Foreign Disclosure, and countermeasures development.

Course Dates/Location: 23-25 Aug 2016//WPAFB

REGISTRATION: Registration is limited and processed in the order received via Program Protection Planning site. Click this link for specific course details and to view future course dates: https://www.milsuite.mil/book/groups/acquisition-program-protection-planning

(you must click "join" in the top-right corner).

CONTINUING EDUCATION: You will receive 45 SPēD Professional Development Units toward your certification (s) renewal. **For more information email: DON_SECURITY_ACQ@NAVY.MIL**

Security Education, Training, and Awareness

HOT!!! New Security Assistant Training Resources. The Center for Development of Security Excellence (CDSE) has released a performance support toolkit and curricula for the Security Assistant. The target audience (Security Assistant) is defined as the non-career, non-security personnel responsible for conducting security activities as a collateral or additional duty within the Information and Personnel Security areas.

The toolkit will quickly point personnel who are responsible for conducting security assistant related activities to the resources needed. Do you have a question about how to do something or need information about a topic in the Personnel, Information, or Contracting areas? The information security curriculum is intended for personnel who are responsible for conducting security assistant activities in Information Security. This curriculum consists of eLearning courses and shorts which will provide an overview of the Information Security Program, to include marking, protecting, handling and disposing of classified information. The curriculum also provides unauthorized disclosure and reporting requirements.

The personnel security curriculum is intended for personnel who are responsible for conducting security assistant activities in Personnel Security. This curriculum consists of eLearning courses and shorts which will provide an overview of the Personnel Security Program, the Adjudication Process, the new Revised Federal Investigative Standards (FIS), adverse information reporting and the Joint Clearance and Access Verification System (JCAVS) levels 7, 8, and 10. To access the Security Assistant Toolkit and curriculum click here.

2016 DoD Virtual Security Conference Defense Security Service announced the 2016 DoD Virtual Security Conference **REGISTRATION IS OPEN**. The conference will occur July 26-27, 2016 using the Adobe Connect Platform. Registration is open to 2,000 DoD civilian and military security personnel. Participants will have the opportunity to learn from DoD leaders and experts about security policy updates and best practices in the areas of Operations, Insider Threat, and Information Security. To register click here. ←

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
Enterprise Security
DON_SECURITY_ENTERPRISE@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

AMERICA'S NAVY
A GLOBAL FORCE FOR GOOD.™

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 SPēD Certifications:

https://i7lp.integral7.com/durango/do/login?ownername=dss&usertype=candidate

-Defense Security Service:

https://stepp.dss.mil/SelfRegistration/Login.aspx