Naval Security Enterprise

Mission Statement:

"We will lead the Department of the Navy (DON) Security Enterprise to develop collaboratively and issue effective security policy; ensure comprehensive oversight of policy compliance; oversee and advocate for DON resourcing of the DON Security Enterprise; and promote cross-functional and enterprise-wide security integration."

Inside Newsletter:

From the Senior Director for Security

I really appreciated getting to meet many of you during my trips to New London, Pensacola and Region NW during the fall last year. I am amazed at the scope your work covers and the great relationships you have forged within the Security community and with those with whom you serve at your installations. Your questions at the Security Professionals Town-Hall meetings have been thoughtful. Thanks for your hard work and dedication.

Tracy Kindle (Security Education, Training and Awareness Branch Chief) and I continue to press you at the Town-Hall meetings to work through the Center for the Development of Security Excellence (CDSE) to gain a Security Professional Certification in the SPēD (Security Professional Education Development) Certification Program. By spring of 2016 DOD will have indexed all 080 positions to a certification level and certification will be mandatory across the Department of Defense. If you do not currently hold a certification please take the opportunity to get into a CDSE program now.

At the DON level we continue to shape the Naval Security Enterprise (NSE) – look for the SECNAVINST describing the NSE soon. Working with our DOD and interagency counterparts, we are building out the Insider Threat Program to comply with guidance from the President. DOD has rolled out the IMESA (Identity Matching Engine for Security and Analysis), part of the Physical Access Control Systems/Defense Installation Access Control programs. We continue to plan for the standup of the Defense Insider Threat Management and Analysis Center (DITMAC) and roll-out of automated continuous evaluation of the cleared workforce. Working with the Navy, the Marine Corps and DOD we are writing the first DON-level Operational Security policy instruction. Effectively protecting information is a constant effort and understanding the requirements to protect controlled unclassified and controlled technical information remains a big challenge.

In sum the security disciplines are in a state of change that is nearly constant –which makes your efforts even more important as you manage security programs for your commanders.

Because of the rate of change in security and the fact it's been three years since the Department of the Navy hosted a Security Managers' Symposium, we've planned a symposium for this spring. On page 6 you'll find information about our 2015 Symposium scheduled for 13-17 April in Leesburg, Virginia. The Symposium is your opportunity to find out about the many changes occurring in the security disciplines across the government and to engage with other Security Professionals from the Department of the Navy, DOD and other services to share questions and best practices. Look for the announcement in late January.

Happy New Year to you and your families. Every year brings new challenges and this year will be no different. I have confidence that all members of the security community will continue to press forward helping keep our people, our installations and our information secure.

Functional Community Management

Over the last seven months, the Mr. Bearor, COI Leader has made a concerted effort to meet as many of you in the community both civilian and military personnel as possible. Since last June he has visited, San Diego, Ca, Norfolk, Va, Mechanicsburg, Pa, Groton, Ct, Pensacola, Fl, and Navy Region NW. Thank you all for attending the briefing and providing him with your valuable feedback.

Although he has not visited all sites where we have personnel in the field protecting our National Security, he will make every attempt to keep you informed of the health of the community and address your professional security concerns.

Future site visits may include:

Kings Bay, Ga, Rota, Naples, Sigonella, Bahrain, Hawaii, Yokosuka, Sasebo, Okinawa, Guam.

Information on future Town Hall Meeting will be published in future newsletters and by your local command security personnel.

If you have an interesting security topic or event to share with the community, send the information to:

DON_SECURITY_SETA_US@NAVY.MIL

Tracy L. Kindle, COI Manager

Continuous Evaluation is important and mandatory!

SEE SOMETHING WRONG
DO SOMETHING RIGHT!

Industrial Security Branch

DUSN (Policy) Industrial Security Branch is working with Defense Security Service (DSS) in accordance with the National Industrial Security Program (NISP) Classified Contracts System (NCCS) Operational Requirements Committee (NCCS ORC). The purpose of the NCCS ORC (further referenced ORC) is to establish an oversight committee responsible for requirements management. The ORC is responsible for the detailed requirements wring-out, design reviews, and validations of requirement implementation through testing. The ORC will approve, prioritize, and oversee the implementation of enhancements and modifications for the NCCS application resident on the Wide area Work Flow (WAWF) platform. The scope of the ORC is to manage the NCCS module whose function is to facilitate security classification guidance conveyed to contractors associated with the performance of a classified contract. The ORC shall consist of members of the Government Industrial Security Working Group.

Committee on Foreign Investment in the United States (CFIUS), CFIUS is a large function of the DUSN (Policy) Industrial Security Branch. CFIUS is an inter-agency committee authorized to review transactions that could result in control of a U.S. business by a foreign person (“covered transactions”), in order to determine the effect of such transactions on the national security of the United States.

Physical Security Branch

Asymmetrical Unmanned Aerial Vehicle (UAV) Threat and the Stand-off Weapons Defeat (SOWD) Program

***" Once the command of the air is obtained by one of the contended armies, the war must become a conflict between a seeing host and one that is blind."* — H. G. Wells, Anticipations of the Reaction of Mechanical and Scientific Progress Upon Human Life, 1902.**

Is it a bird?, is it a plane?…no it's your remotely controlled unmanned aerial vehicle (UAV) with super-hero like capabilities better known by their military noms de guerre: the Reaper, Predator, Heron, Global Hawk and Sentinel. Well, those are at least the good guys. But have you heard of the Dark Sword, Striker, Pterodactyl, Shahpar and Stork…probably not. The proliferation of UAV capability by adversaries such as China, Russia, Iran and Pakistan pose unconventional threats to our once unchallenged supremacy of the unmanned domain.

By definition, Unmanned Aerial Systems encompass a diversity of classifications which range from armed military drones to commercially off-the-shelf (COTS) purchased aircraft by recreational users. The term 'UAV' is representative of a class of air platforms known by different names: unmanned aircraft (UA), remotely controlled model aircraft (RCMA), remotely controlled aircraft (RCA), remotely piloted aircraft (RPA), and drones. In today's open market place, easily acquired technology.

Consequently, nefarious state-sponsored actors or ideologically inspired terrorist groups are employing UAVs or have the potential to use them in an, increasing and alarming, effort to conduct illicit activities against naval installations and missions both at home and abroad.
Current reporting indicates UAV use in smuggling narcotics and to conduct surveillance operations against law enforcement and military actions worldwide. Malign adaptation of this technology will only broaden over time in scope and scale.

Notwithstanding an ominous forecast, the Deputy Under Secretary of the Navy for Policy (DUSN (P)) Physical Security Directorate through the leadership of Branch Chief, Mr. Jeffrey Jones formed the counter UAV threat initiative called Stand-off Weapons and Defeat (SOWD) as part of the highly acclaimed Navy Physical Security Enterprise and Analysis Group (NPSEAG) program. The mission of this Stand-off Weapons Defeat Joint Integrated Product Team (JIPT) is to determine the best path forward to develop and deploy a family of countermeasures to defeat the various stand-off weapon (SOW) threats to Department of Navy (DON) assets.

The objective of this multi-service and multi-talented team is to produce a joint roadmap to guide the appropriate levels of research, development, test and evaluation (RDT&E) investments for a family of SOW countermeasures which can be integrated into a system of systems architecture which is expandable, extensible, and adaptable for all the operational environments of concern. This program highlights one of many unique initiatives spearheaded by the DUSN (P) Security Directorate in direct support of the nation's warfighters, now and into the future.

For more information contact Stand-off Weapons and Defeat (SOWD) POC:
Deputy Branch Chief, Mr. Clark W. Metz

Physical Security Branch Cont.

Department of Defense Lock Program

In 1992, based on Government requirements, FF-L-2740 and innovative engineering, the revolutionary X-07 lock was produced. It has been a DoD stalwart for safe-guarding high value and classified information over the past 22 years. A ground-breaking feature of the X-07 was that unlocking was accomplished electronically without aid of batteries or dependency on an external power source. Improvements in 1999 produced the X-08 version followed by the X-09 version in 2002 -- with the X-10 as the latest iteration.

While still in use, what has made the X-07 so popular; its time tested performance is now potentially its 'Achilles heel'. Industry lock experts recognize the X-07's length of service coupled with varying degrees of site to site usage, may have over-burdened its functionality beyond its reasonably expected lifetime. Moreover, we can expect to see additional issues in the future, so it's important for users to do preventative maintenance as recommended by the manufacturer.

What should I do to prevent a locking failure? DoD Lock experts are still assessing the impact, nevertheless, X-07s experiencing frequent (daily usage) should be tagged for replacement and resources identified, in fiscal year budgets, as part of a comprehensive life-cycle replacement program.

Are my X-07s going to be inoperable tomorrow? Perhaps not considered a major concern, but a situation you should be mindful of. If you have an X-07 with high use, perhaps recognize you've achieved 12 additional years past its government tested standard. A change may be prudent.

Who do I contact regarding my X-07? NAVFAC 1322 Patterson Ave. SE, Suite 100, Washington Navy Yard, D.C. 20374-5065, DoD Lock Program Technical Support Hotline (800) 290-7607, (805) 982-1212, DSN 551-1212 or send an email to Technical Support http://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock/OtherInformation/LockProgramContacts/RequestForm.html

United States Army Corps of Engineers
Protective Design Center
Security Engineering Training course
https://pdc.usace.army.mil/training/secengg

Personnel Security Branch

"Where is the Updated Personnel Security Manual?"

The latest edition of the Secretary of the Navy's Personnel Security Manual, SECNAV M-5510.30 completed in June 2006 will not be updated until the Department of Defense publishes the revised DoD Personnel Security Manual (DoD PSP Manual) issued by the Under Secretary of Defense for Intelligence.

The SECNAV Personnel Security Manual is evolving and changes to current policy will be rewritten in its entirety. The new manual will have a new look and follow the same structure as the DoD Manual.

The SECNAV Manual will only elaborate on specific policy unique to the department. It will not be a Standard Operational Procedural guide or a "How To" document.

Translation, the manual will be substantially reduced in size, no longer will it weigh you down, but provide relevant and up-to-date information.

While we wait on the DoD PSP Manual, some very important guidance has been released which affects operational procedures within Personnel Security:

- DoDI 5200.02, Personnel Security Program

- DoDI 5200.46 DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card.

The above DoD changes will be incorporated into the revised Department of the Navy Personnel Security Program Instruction, SECNAV 5510.30B and Department of the Navy Personnel Security Program Manual, SECNAV M-5510.30.

Serving Those who Serve our Country
DMDC
Personnel Security/Assurance
PSA Home | DCII | JPAS | SWFT
JPAS Login

Security Education, Training and Awareness (SETA) Branch

SECNAV M-5510.30 DoN Personnel Security Program Jun 2006, Chapter 2 Paragraph 2-3.1 & 2-3.3 requires every command in the Navy and Marine Corps eligible to receive classified information to designate a security manager in writing & for them to receive formal training. Seat Quota requests for the Naval Security Managers Course (NSMC), Course Identification Number: S-3C-0001 (CPD 925W Little Creek & 925X NASNI Coronado) are now available via eNTRS. The NSMC class schedule may be viewed on the CANTRAC, eNTRS or the Naval Security Enterprise on NKO. The CANTRAC (link) has been completely updated.

JPAS Account Requirements
The following are required:
- Letter of Appointment or Letter of Designation
- JPAS Personnel Security System Access Request (PSSAR) form completed signed and submitted
- Certificates of completion for Cyber Security Awareness Challenge/Security, Personally Identifiable Information & JPAS training commensurate to the sub-system and level of access (completed within the last year) must be submitted with the PSSAR. Reference: JPAS Account Management Policy Document Version 7.10 dated 12/05/2014 (link) JPAS main page; General Information; Account Manager Policy

Center for Development of Security Excellence

Security education, training, and professionalization for the Department of Defense and industry

CDSE Advanced and Graduate Courses
View current and upcoming offerings from the Education Division ▸

Security Professional Education Development (SPēD) Certification Program

Have you ever wondered how to obtain your SPēD certification? Over the next few quarters, information will be posted here to help you obtain and maintain your professional certification(s). The Defense Security Service (DSS) is the DoD Executive Agency responsible for helping DON personnel obtain and maintain one or multiple certifications.

To get started in the SPēD Certification Program click: http://www.cdse.edu/certification/faqs.html

To prepare to take a certification exam click: http://www.cdse.edu/certification/prepare.html

If you have any questions regarding your SPeD Certification Program, send us an email at: DON_SECURITY_SETA_US@NAVY.MIL

For more information on the SPeD certification program click: http://www.cdse.edu/certification/sped_what.html

2015 Security Manager Symposium

2015 marks the 19th Department of the Navy (DON) Security Manager Symposium. Over the past 18 years we've provided InfoSec, Industrial, and PerSec policy and guidance, which directly supports your command's security programs. This year we'll be adding PhySec & Acquisition Security to the list.

The conference will be held 13-17 April 2015 at the National Conference Center, Lansdowne, VA. Sessions will be held Tuesday - Thursday. Each day will focus on a general theme. Day 1 will focus on Policy and will have guest speakers from DoD/DON present to discuss recent and proposed changes to Policy. Day 2 will focus on Insider Threat with guest speakers from DoD, Cybersecurity, and NCIS. Afternoons will provide breakout sessions to discuss specific topics within each security discipline. Day 3 will focus on Security Education, Training and Certification as well as hands on workshops.

This year attendance is open to all DON Security Professionals, so please ensure widest dissemination. We are only able to accept 350 overnight guests, so pre-registration is highly encouraged. You may pre-register by sending an email to the conference organizer Mrs. Kate Fuster at the email address below. Pre-registering does not guarantee your reservation, but does ensure you receive immediate notification when registration opens.

Please send your pre-registration to don_security_enterprise_conf@navy.mil ASAP.   (Pre-registering means your leadership has verbally approved your conference attendance).

Also, please send us an email with any topics or training you would like to see covered at this year's symposium.

Naval Security Enterprise Branch

DUSN (Policy) Security Directorate will be promulgating an instruction in the second quarter of FY 15 delineating the scope, roles and responsibilities of the Naval Security Enterprise (NSE). This construct creates a framework to provide guidance to promote efficiency and facilitate consistent security policies and practices across the DON. It brings together policy makers and practitioners from all Naval security related disciplines in a manner that will facilitate continuing dialogue, identification of best practices and the ability to leverage common overhead.

DUSN (Policy) is an active participant in DoD and US interagency efforts to establish and implement a program to address insider threat. DON is working closely with the National Insider Threat Task Force (NITTF) to create a coordinated and integrated approach to address this difficult problem set. Security Directorate has already chaired two Naval Senior leadership sessions to solicit feedback and provide updates on Departmental insider threat efforts.   The Department is developing an implementation plan for release before the 3rd quarter of FY 15.

Operations Security (OPSEC) has been in the news quite frequently over the past several months. Press reports documenting alleged threats to families and service members by ISIS militants has reinforced DUSN (Policy) efforts to reinvigorate the Naval OPSEC program. For that last year, the Security Directorate has conducted a bottom-up review of OPSEC programs across the DON. Lessons learned and best practices identified during the review have been incorporated into several policy documents, including an upcoming SECNAV OPSEC instruction. This new policy document will focus on creating a program that permits accountability, enforcement, and oversight. It also stresses the importance of collaboration between OPSEC and public affairs professionals, sound social media policies, and enhanced OPSEC in contracting and acquisition.

National OPSEC Program
Interagency OPSEC Support Staff
INTERAGENCY OPSEC SUPPORT STAFF

Acquisition Security Branch

Acquisition Security:

WHO WE ARE: The DUSN Policy Acquisition Security Branch serves as a liaison between the DASN RDA Technology and Program Protection (T&PP) office and DON Security Specialists performing Research & Technology Protection (RTP) functions.

TOP FY15-16 GOALS:

1) Review and identify policy gaps between the DoD Program Protection Plan Guidebook, DoD 5000 series and the DoD 5200.39. Provide a recommended path forward for possible development and implementation of DON-specific Program Protection policy.

2) Establish a well-defined, reciprocal relationship with RDA and SYSCOMs to explore a career-enhanced Security Specialist position in the Defense Security Enterprise. This position will exist to ensure security initiatives are identified and applied at the appropriate time within the Acquisition Life Cycle. This initiative requires:

- Effective alignment of security with Acquisition community.
- Leadership support and recognition of the importance of having Security Specialists (0080) embedded in Program Offices.
- Identification and training of appropriate skill set to support Acquisition activities

CURRENT FOCUS: Acquisition Security is currently working on the aforementioned DoD policy review and also evaluating how those policies are currently being implemented within the DON. We continue to work with OSD AT&L to ensure the policies are properly aligned with appropriate security requirements, and identified as early as possible in the Acquisition Life Cycle through working group participation and other security advocacy.

OTHER INITIATIVES: Acquisition Security is coordinating with OSD AT&L and the Defense Acquisition University (DAU) to develop a new ENG 160 Course. This course will include three new learning objectives that focus directly on security.

1. Given DoD Manual 5200.01 volumes 1-4, recognize the policy and criteria for classification of information and CUI identification.

2. Recognize the elements of identifying and protecting classified and unclassified information (include National Industrial Security Program Operating Manual (NISPOM) and DFARS).

3. Recognize the role of Defense Security Service (DSS) with respect to NISPOM and the related System Security Engineering (SSE) responsibilities.

CONTACT US: If you would like to know more about our exciting initiatives and/or have some relevant insights you would like to share, you are encouraged to contact us at DON_SECURITY_ACQ@NAVY.MIL.

Information Security Branch

The Information Security Branch has many projects underway, many of which are meant to help improve the overall posture of the program and assist the security professionals in the field. The specific topics addressed below are to provide you with situational awareness on some of the core projects completed or underway.

- **Mandatory Declassification Reviews (MDRs):** Realigned under Department of the Navy (DON) Administrative Assistant, Directives and Records Management Division effective 1 August 2014.
- **Update of SECNAV M-5510.36**: Update is still in-progress. The update will be a complete restructure and rewrite of the previous manual. The updated manual will have only 4 chapters vice 12. Each chapter in the updated SECNAV M-5510.36 will align with the DoD Information Security Program Manuals, DoDM 5200.01, Volumes 1 through 4. We will also cancel the OPNAVINST 5513 series of instructions and incorporate the requirements into the update of the SECNAV M-5510.36, along with a significantly improved format for DON security classification guides. The major overhaul of the manual is very time intensive, coupled with the daily demands and tasks, making it difficult to move the update forward in a more expeditious manner. So, Naval Air Warfare Center Weapons Division (NAWCWD) China Lake volunteered to TDY an asset for 8 weeks to DUSN (P) Security to assist with the update. Many thanks to NAWCWD! Target timeline for completing the draft re-write of the manual is end of CY 2015.
- **Classification Management Strategic Plan:** Developed to improve classification management issues for compliance with Executive Order 13526. Implementation of the plan has begun. One of the endeavors underway is validating compliance with training requirements for Original Classification Authorities (OCAs), and evidence they are exercising their authority.
- **Derivative Classifier Training:** Pushing for a change to the System Access Request (SAR) form for user access to a DON IT system. Specifically, wherein the Command Security Manager will have to validate an individual has completed the required Derivative Classifier training, prior to being granted access to a classified IT system. Also, looking to establish in policy a requirement to suspend a users access to a classified IT system, if the individual has not complied with the requirement to complete required Derivative Classifier refresher training every two years. Both endeavors require coordination with the cyber security community.
- **Marking Tool:** Identified requirements for an improved marking tool on SIPRNET, but will require multiple steps and funding to obtain approval for changes (if approved). The majority of personnel with access to SIPRNET have Classify for Outlook, which is a moderately adequate tool with limitations. The tools limited application, for use with email only, doesn't assist with marking documents on other core Microsoft applications (Word, Excel, and PowerPoint) that we often use. We have identified this as one, amongst many other requirements, for the capability and functionality of a marking tool. Availability of a tool that will meet our requirements list has to be identified. Again, funding and many other steps will be required to obtain the desired end product.
- **Realignment of Security Review:** Conducted and/or coordinated a security review of over 27K pages during FY14. This function does not align with our core mission of policy, and will be realigned to various offices. An ALNAV will be drafted to advise of this change.

Information Security Branch Cont.

- **Unauthorized Disclosure of Classified Information and Controlled Unclassified Information on DON Information Systems**: Draft ALNAV for implementation of Deputy Secretary of Defense (DEPSECDEF) memo of 14 August 2014, Unauthorized Disclosure of Classified Information and Controlled Unclassified Information on DoD Information Systems completed. The DEPSECDEF memo addresses electronic spillages (ES), so an update to the current ES Reporting Process has been drafted as well, and will be promulgated with the issuance of the ALNAV. The draft ALNAV and the update to the ES Reporting Process are pending principal office review/comment, prior to final release by the Secretary of the Navy.
- **Replacement of Shipboard Security Containers:** Draft interim policy change completed. Outlines requirements for replacement of shipboard security containers used for the storage of classified information, with the new GSA Approved shipboard security container. Information on the new security container is available on the DoD Lock Program website at http://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html.
- **Executive Order 13556, Controlled Unclassified Information (CUI)**: Pending implementation. This is a freight train that is still on track, and will require some time to transition once implementing guidance is issued. In the meantime, compliance with requirements in DoDM 5200.01, Volume 4, Controlled Unclassified Information, must be adhered to, pending implementation of the Order. Learn more about the evolving changes to CUI at http://www.archives.gov/cui/.
- **Acquisition Security Database (ASDB) Site**: The DON Security Classification Guides (SCGs) posted to the ASDB will not be available after 23 January 2015, as part of the transition of the site from Space and Naval Warfare Systems Center Atlantic to the Defense Technical Information Center (DTIC). Copies of DON SCGs (less those with Distribution Statement F) can be obtained from the DTIC website at https://dtic.mil.

Secure Your Social Media Presence

Published, October 20, 2014

Attempted intrusions into DoD networks by spear-phishing or a social media based attack occur frequently. While it is legal to access social media sites from your DoD computer, there are precautions that you should take to make both your personal information and our government networks safe from attack. ...Click for Complete Article on DON CIO website

Naval Security Enterprise

Points of Contact:

Mailing Address:
Deputy Under Secretary of the Navy, Policy
1000 Navy Pentagon
Washington, DC 20350

Phone Number: 703- 601-0610

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:

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

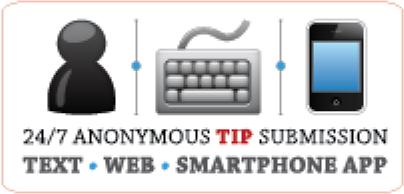
- **Department of The Navy, Security Executive**: http://www.secnav.navy.mil/ppoi/Security/Pages/Default.aspx

- **Department of The Navy, Security Education, Awareness and Training**: http://www.secnav.navy.mil/ppoi/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

- **Pearson Vue**: https://www1.pearsonvue.com/testtaker/signin/SignInPage/DSS



Click for the NCIS Reporting Brochure

Click for NCIS How to Report a Crime

SEE SOMETHING WRONG
DO SOMETHING RIGHT!