Naval Security Enterprise Newsletter

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

This newsletter provides the wrap up from the Spring 2015 Naval Security Enterprise Symposium. I was very pleased with both the turnout and the enthusiasm from the more than 400 Security Professionals who attended the three-day event. I thought all the speakers from Mr. Bill Evanina, Director of the National Counterintelligence and Security Center (NCSC) to the closing keynote from Ms. Jodi Greene, Deputy Under Secretary of the Navy for Policy (DUSN (P)) were value added. I particularly want to thank those external organizations who provided such great support including the Office of the Under Secretary of Defense for Intelligence (OUSD(I)), the Defense Security Service (DSS), the Center for Development of Security Excellence (CDSE), DOD Consolidated Adjudication Facility, Naval Criminal Investigative Service (NCIS), the Cyber-Security Panel, the Personnel Security Appeals Board, and the staff here at DUSN(P) Security.

If you missed the event, take a look through this newsletter for links to the briefs and other information that can help keep you up to date.

Our office will continue to reach out to you and your leaders to talk about security, assess how well the Department is meeting its security missions, and stay engaged with you working on your concerns. Members of the Security Directorate, by agreement with the Office of the Naval Inspector General, will accompany select IG teams when they conduct inspection visits. Our subject matter experts will conduct several visits during FY16 to concentration areas to sit with security professionals so you can tell us how we can positively affect your problem sets. And I will continue to travel to meet you, let you know what we're working on and get your direct questions and feedback.

Lastly, you have no doubt heard of the breach of personnel data from various Office of Personnel systems. This is very worrisome on a number of levels and affects each of us. Each of you understands what data is on the SF86. Loss of the data may lead to identity theft and related problems – but could also give an adversary just the right information to target an individual for elicitation. We are working with DOD, the services, and NCIS on mitigation efforts. More to follow at - **http://www.secnav.navy.mil/OPMBreachDON**.

DON Security Symposium Presentations

The DoN Security Symposium Presentations are located on Navy Knowledge Online (NKO) in the Naval Security Enterprise (NSE) Community knowledge library. Here is a link to the NSE Community on NKO**: https://www.nko.navy.mil/group/naval-security-enterprise/naval-security-enterprise1.** You may have to log into NKO first for the link to work. Each page in the NSE Community has a link to a "How To" document that will guide you to the presentations. Please visit the knowledge library and review these great presentations, they are a wealth of knowledge. There are comment/suggestions web portals on the NSE. Please use them.

Security Education, Training, and Awareness (SETA) and Functional Community Branch

Symposium summary:

Indexing of Department of the Navy (DON) Security Position: This session provided participants an overview of the Department of Defense Security Accreditation and Certification Manual (DoDM 3305-13). This policy categorizes defense security positions in security functional tasks; identifies certifications applicable to personnel performing security functional tasks; establishes required language in security recruitment announcements; and the impact of indexing on the security workforce.

Preparing for Security Professional Education Development (SPēD) Certifications: This session provided participants with information required to take a SPēD certification exam; coordination with a Service Program Management Office; use of the Competency Preparatory Tools to help prepare for an exam; and the SPēD Certification Candidate Handbook.

SPēD Certification Maintenance: This session provided participants with a live demonstration on how to maintain a SPēD certification during the two-year certification maintenance period. This briefing included a step-by-step process for submitting the Certification Renewal Form. This session also included a discussion on the Defense Security Skills Standards document that brings together the DoD Security community's expectations of security practitioners.

Center for the Development of Security Excellence (CDSE) Outreach Exhibit: The CDSE set up an outreach exhibit where members in attendance could get a first-hand look at new security related products (i.e., security toolkits for use of mobile devices; FREE graduate level educational opportunities and security related training). See all the toolkits at http://www.cdse.edu/toolkits/index.html.

Five (5) most asked questions for SETA and Branch

1. Do I have to take a certification if I remain in my current position until I retire from government service?
Answer: No, however we highly recommend participating or obtaining a SPēD certification. If you move to another security position indexed to a SPēD certification, you will have to obtain the specified SPēD certification(s).

2. How long do I have to obtain a SPēD certification if I was selected for a position with a SPēD Certification requirement?
Answer: Two years.

3. What happens if I do not get my SPēD certification within the allotted time?
Answer: Your supervisory chain may take action to reassign you another positon where a certification is not required, or possibly take action to remove you from government service.

4. How long do I have to wait to retake an exam if I do not pass the first time?
Answer: 90 days

SETA and Functional Community Branch Cont.

5. What happens to my SPēD certification if I do not maintain 100 Professional Development Units (PDU) during the two-year maintenance cycle?
Answer: You will lose your current and other certifications you have obtained.

On behalf of the Deputy Under Secretary of the Navy (Policy) (DUSN (P)) Security Directorate, I want to send a special thank you to **Mr. Brian Miller**, Chief, Training Division. Representing the Director of CDSE, Mr. Miller presented an excellent overview of the CDSE, which set the tone for the third day of the security symposium. I also want to thank other CDSE staff members for their outstanding support; **Mr. Boyd Crouse**, for presenting the “Preparing for SPēD certification session**; Mr. Ronald Adams**, for presenting the “SPēD Certification Maintenance session; and **Ms. Jill Baker, Mr. Keith Owens, and Mr. Scott Hill** for operating the security training, education and certification interactive exhibit. Lastly, I want to thank the participants of the security symposium for the candid feedback and their expertise during the question and answer sessions. In each session, we helped each other get the most out of each session, and without you, none of this would be possible. You make this program, and you make this program work.

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 ▸
Registration for the Spring 2015 Semester is now open!

REGISTRATION IS NOW OPEN FOR FALL SEMESTER GRADUATE LASSES THAT BEGIN ON AUGUST 24!

The Defense Security Service, (DSS) Center for Development of Security Excellence (CDSE) offers a variety of courses to US Government employees and Military Service Members.

No fee or tuition is charged for CDSE courses; however, some courses require students to obtain textbooks. In many cases your employing agency will pay for textbooks if you submit a SF 182 "Authorization, Agreement and Certification of Training" through normal channels.

CDSE courses are ideal continuing education to maintain your professional certifications.
You may earn 45 PDU's towards maintenance of your SPeD Professional Certification by completing one CDSE graduate course.

American Council on Education (ACE) college credit recommendations allow students who complete these CDSE courses to transfer credit towards completion of a Bachelor's or Master's degree at many colleges and universities.

Course descriptions and registration information can be found here: http://www.cdse.edu/education/courses.html

Each course is a semester long and requires a level of effort similar to a three semester-hour graduate course. This includes reading, research and writing assignments and participation in online learning activities.

Students may earn an Education Certificate by completing four courses in an area of concentration. Information about CDSE Education Certificates is found here: http://cdse.edu/education/certificates.html. An overview of the CDSE Education Program is found here: http://cdse.edu/education/index.html

Additional undergraduate and other security courses are found here: http://cdse.edu/catalog/index.html

If you would like additional information after visiting the CDSE website you may send your questions to CDSE.Education@dss.mil.

Information Security Branch

- **Topic:** Marking (*Presenter: Treva Alexander with DSS-CDSE*)
  - **Outline:** Provided policy requirements for marking, along with a practical exercise. Purpose of the workshop was to assist commands with conducting random sampling for marking compliance during their annual self-inspection, and identifying focus areas for initial or annual refresher training based on the results of their inspection.
    - **Primary focus question:** How do I identifying the most restrictive declassification date when derived from multiple sources with previously used declassification instructions (e.g., Originating Agency Determination Required (OADR), X4, Manual Review (MR), etc.).
    - **Answer:** Derivative markings shall use a calculated declassification date that is 25 years from the date of the document's origin, ***unless*** other guidance from the Original Classification Authority (OCA) is available. DoDM 5200.01, Volume 2, Enclosure 3, Section 9 refers. In the draft rewrite of the SECNAV M-5510.36 there will be a template to assist with calculating the most restrictive declassification date.

EXAMPLE:

Source 1: Declassify On: OADR, date of source: 1 August 1990
Source 2: Declassify On: X4, date of source: 18 October 1996
Source 3: Declassify On: MR, date of source 3 December 1992

Calculate 25 years from the date of the most recent document for the most restrictive declassification date. Using sources listed above, Source 2 is the most restrictive declassification date. Mark the derivative document "Declassify On: 20211018"

- **Topic:** DON Information Security Policy Overview (*Presenter: Bridget DelGrosso, DUSN(P) Security, Branch Chief, DON Information Security Policy*)
  - **Outline**: Provided current & pending policy changes: Policy Reminders: Initiatives (such as OCA/SCG Reduction Efforts, SAAR, etc.): Unauthorized Disclosures.
    - **Primary focus question:** What policy do we follow (DoD or Navy)?
    - **Answers:** Recommend commands refer to DoDM 5200.01, Volumes 1 through 4 for Information Security policy requirements, until the SECNAV M-5530.36 is updated. Check the SECNAV M-5510.36 for DON specific requirements that still apply (e.g. submission of waivers/exceptions, requests for classified meetings, authority to approve OCAs and requirements for requesting OCA, establishing Alternative Compensatory Control Measures, preliminary inquiry and JAGMAN investigation reporting requirements and format, etc.). Also, DON personnel must refer to DoDM 5200.01, Volumes 2 and 4 as the authoritative source for marking classified information and Controlled Unclassified Information (CUI) in correspondence vice SECNAV M-5216.5, DON Correspondence Manual (marking requirements are not current). DUSN(P) Security Directorate provided comments to the update of the SECNAV M-5216.5 to ensure compliance with DoDM 5200.01, Volumes 2 and 4.

Information Security Branch Cont.

- **Topic:** DoD Information Security Policy Overview (*Presenter: Ed Kaufhold, USD(I), Division Chief, Information Security*)
  - **Outline:** Key policy changes to DoDM 5200.01, Volumes 1-4: Status of CUI Final Rule & DoD Implementation of the Final Rule: CCRI Integration w/Traditional Security.
    - **Primary focus questions:**
      1. When will the new CUI framework to Executive Order 13556, Controlled Unclassified Information, be implemented?
      2. Is a Security Technical Implementation Guidance (STIGs) policy?
      3. What is the DoD portal to access new issuances?
    - **Answers:**
      1. The draft CUI Rule is out for public review and provides the federal government implementing requirements to the Order. The Final Rule is expected to be finalized early fall 2015. Information about the new CUI framework is available at http://www.archives.gov/cui/. Under Secretary of Defense (Intelligence) (USD(I)) will then issue DoD implementing requirements through an update of DoDM 5200.01, Volume 4. Estimated update of the Volume 4 is sometime in 2016, but full implementation within the DoD may take some significant time (e.g., updating software applications for compliance with marking requirements). DUSN(P) Security Directorate will only issue DON implementing requirements, if there is a specific DON requirement; otherwise, the DoD policy requirements will apply. Reminder, commands must follow current DoDM 5200.01, Volume 4 policy requirements for CUI, until the new CUI framework is implemented.
      2. DoDM 5200.01, Volumes 1 through 4 provides the implementing policy requirements for the Information Security Program not STIGs. Authority to set DoD Information Security policy rests with USD(I).
      3. Two part answer:
         - 1. DON issuances can be found at http://doni.documentservices.dla. mil/default.aspx**;** DUSN(P) Security website is available at http://www.secnav.navy.mil/dusnp/Security/Pages/Default.aspx and also contains copies or links to policy. Additional DUSN(P) Security Directorate policy is also posted at https://infosec.navy.mil/main/home?p=3-1&tab=3&folder=48 (PKI enabled website).
         - 2. DoD issuances can be found at http://www.dtic.mil/whs/directives/; USD(I) website for Information Security policy is available at https://intelshare.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/default.aspx (PKI enabled website).
- **Topic:** SECNAV M-5510.36 (*Presenters: Carmen Lanier & April Minor, DUSN(P) Security Action Officers, and Shari Belill, NSWCWD China Lake, Command Security Manager*)
  - **Outline:** Provided overview of the major changes underway to the update of the DON Information Security Program Manual (e.g., complete restructuring of the manual, self-inspection criteria, security classification guide format, new/updated exhibits, removal of Industrial Security chapter, etc.). Solicited recommendations/feedback from attendees for improving the guidance and/or exhibits: Open discussion – interactive format.
    - **Primary focus input:** Add language to address marking of media that has gone through a "trusted download" procedure; Requirement that the Command Security Manager (CSM) role is to be a full-time, "mission critical," position without other non-CSM duties; Add a column to the new security classification guide template for "original date" of classification for each element of information to better identify and track when the OCA made the original decision; Include most common marking deficiencies as important reminders for validating compliance with marking.

Information Security Branch Cont.

- **DUSN(P) Security Directorate, DON Information Security Policy position:** Will vet the recommendation regarding the role (full time – mission critical) of the CSM with the DUSN(P) Senior Director for Security. All other suggestions accepted. Two personnel from NSWC PC stepped up to assist with the update of the SECNAV M-5510.36. Many thanks!!

- **Topic:** Mobility (*Panel members listed below*)
  - **Outline:** There was an introduction of each discussion topic for varying panel members to discuss with interactive Q&A throughout with the audience. Topics: Why the traditional security community would care about mobility. Some areas of discussion included: Installing WI-FI hotspots on ships and how that may/may not affect classified spaces; Wireless policy (re: mobile device, laptops, etc. in classified spaces); Command Cyber Readiness Inspections (CCRI's) and the impact of mobile technology (re: is this adequately covered on the inspection checklist); Storing, processing, transmitting information (CUI or classified) on mobile devices; Mobile capability on travel (re: hotels); Bring your own device (BYOD) (protecting the information using personal device, spillages, etc.); C&A and what risk considerations are given to information, personnel, physical and industrial security during the approval process, etc. Open discussion – interactive format – two sessions of the workshop were held to permit maximum participation.
    - **Primary focus questions:**
      1. Is there a DON implementing policy to DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)?
      2. Are Fitbits authorized in spaces where classified information is processed?
      3. Are medical devices authorized in spaces where classified information is processed (e.g., hearing aid with blue tooth capability)?
    - **Answers:**
      1. There is no DON implementing policy to DoDD 8100.02 at this time. There is, however, USMC policy (Enterprise Cybersecurity Directive 005, Portable Electronic Devices, 12 March 2012 and USMC Enterprise Cybersecurity Directive 014, Wireless Local Area Networks, 15 November 2012), and a draft joint memo from DONCIO and DUSN(P) Security to provide policy guidance regarding use of DON issued wireless laptops in controlled areas. Commands must comply with DoDD 8100.02 available at http://www.dtic.mil/whs/ directives/ corres/pdf/810002p.pdf.
      2. Not a clear cut answer for spaces processing collateral classified information. Not all FitBits have the same capability. USMC must follow requirements referenced above. Recommend all others comply with command established policies or DoDD 8100.02 (e.g., assess the capabilities, determine the vulnerabilities, work collaboratively with the command Information System Security Manager and appropriate Authorizing Official (AO) (formerly the Designated Approving Authority or DAA). The AO will coordinate with the Certified TEMPEST Technical Authority (CTTA) to make a determination.
      3. DoDD 8100.02, para 2.5 addresses the requirements for medical devices. If the devices cited in the DoD policy don't apply and there are other associated vulnerabilities, follow recommendations in 2 above. USMC personnel must follow requirements in the policy cited above.

    - **General Comment:**
      In consideration of the above aforementioned questions, it was clear the DON is in need of a wireless policy. Functioning as the Navy mobility IPT chairman, Dan DelGrosso took this for action and will work with DON CIO, DUSN (P) Security

Information Security Branch Cont.

Directorate, HQMC C4 and OPNAV N2/N6 to develop said policy. Estimated start date is SEP 2015.

- **Panel Members:**
  - Dan DelGrosso (Facilitator/Technical Director PEO-EIS)
  - Russ Smith (DONCIO representative)
  - Jon Kling (SES/NAVSEA 08 CIO)
  - CDR (Sel) Bobby Carmichael (OPNAV N2/N6 representative)
  - Ray Letteer (HQMC C4 Cybersecurity Chief and USMC Authorizing Official)
  - Theresa Duvall (FCC, Office of the Navy Authorizing Official)

- **Topic:** SF 311 & Self-Inspection Reports (*Presenters: Carmen Lanier, DUSN(P) Security Action Officer and Shari Belill, NSWCWD China Lake, Command Security Manager*)
  - **Outline:** Presented the fiscal year 2013-2014 comparative data, trend analysis, and common data errors for each report. Provided recommendations for improving the data submitted by commands for both reports. Reviewed the draft guidance developed for the annual self-inspection report to assist CSMs with assessing their program, in order to better articulate findings/recommendations/best practices to their Commanding Officer and in formal reporting to DUSN(P) Security. Solicited recommendations/feedback for improving annual reports: Open discussion – interactive format.
    - **Primary focus input:** Add the marking sample matrix previously issued under CNO (N09N2).
    - **DUSN(P) Security Directorate, DON Information Security Policy position:** Accepted and will also be included in the rewrite of the SECNAV M-5510.36. *Just a reminder*, the Annual Information Security Self-Inspection report for FY15 will be issued July (estimated timeline). We will include the additional guidance for completing the report that was covered in this workshop. The guidance contains a list of additional questions in order to provide a comprehensive assessment of the items contained in the report. Use of the guidance and the additional questions embedded in that guidance is optional for the FY15 report.

- **Topic:** SSO Navy (*Presenter: Mark Lawton, SSO Navy*)
  - **Outline:** Provided an **o**verview of ever-changing organization structure as Naval Intelligence Activity (NIA), guidance on newly acquired (from Defense Intelligence Agency) Sensitive Compartmented Information Facility accreditation authority and program, and discussed common CSM – Special Security Officer (SSO) communication interface issues in the fleet, address laptop and Fitbit questions. (Contact Mark Lawton, for focus area questions and answers to determine appropriate authorized release of information presented).

Many thanks to all the presenters for their time, efforts, and expertise in supporting the DUSN(P) Security Enterprise Symposium - Information Security workshops. We also extend our appreciation to all the personnel who attended the Information Security workshops and provided not only their thoughts and ideas, but addressed their concerns and insightful questions. Understanding your challenges helps us with improving the policy.

Physical Security Branch

Symposium summary:

The core physical security theme centered on the relational requirements for a successful, relevant and holistic security program. Each presentation and the round-table discussion focused on the relationships, irrespective of service or echelon level, needed to forge adaptive and responsive programs. The intended goal for the three-day symposium attendees was to offer physical security insight at the Navy Secretariat and echelon one and two levels.

OUSD (I) Physical Security Presentation: The session was an overview of the DOD Physical Security Policy and Programs by USD (I). The intent was to better inform the audience how policy is promulgated and to get their issues addressed. It also gave points of contact for the services and how to best stay engaged and be involved with the policy process. The focus areas were: access control, the rewrite of the Physical Security policy and other efforts for integration of physical and cyber realms. The long-term relationship building with information security was a key topic warranting further discussion and clarification.

DUSN (P) Physical Security Branch: Networks and strategic partnerships highlighted Day 1 and Day 3 presentations by Branch Chief, Jeff Jones. Core themes focused on building relational pillars of excellence and reemphasizing no security manager lives on their own island and they need to be more inclusive of other security professionals whom can support the program as well as baseline best practices. The PHYSEC Branch Chief touched on the associations needed for a robust Base Physical Security Plan. Additionally, Fiscal Year 15 priorities for the DUSN (P) Security Directorate were discussed, e.g. monitor Washington Navy Yards related actions and activities; policy promulgation – writing and publishing of a DON Physical Security Policy, DON SECNAVINST 5500.35 Physical Security Instruction; and lastly the Counter Asymmetrical Unmanned Aerial Systems (UAS) - DON is partnering with USD(I) to develop a collaborative whole of U.S. Government solution to the Unmanned Aerial Systems (UAS) threat that exists from violent extremists, foreign intelligence, criminal elements and other installation security concerns.

CNIC/USFF/OPNAV N46 Panel: This interactive round-table forum provided much needed cross talk from the policy originators and those that are tasked with its execution. The symposium attendees were able to ask direct questions affecting their day-to-day efforts to senior leaders with a broad range of expertise. This was a popular session among the attendees.

Physical Security Certifications: The purpose of this presentation was to provide an overview of the Physical Security Products and Services offered by the Center for the Development of Security Excellence (CDSE). It was an informative session which has the potential to strengthen everybody's physical security toolkit and knowledge base. In addition to the physical security blended learning, CDSE offers a wide variety of other instructional media in support of the DoD Information Security Program. This includes 'Security Shorts', which are targeted e-learning courses designed to be completed in less than 15 minutes; podcasts, which are audio-only based courses; and short training videos on various security processes and procedures.

Physical Security Branch Cont.

__Five (5) most asked questions for Physical Security__

1. Will DOD Lock Program send out lock SME representatives to installations?

(a) Yes. Please contact the DoD Lock Program Technical Support Hotline (800) 290-7607, (805) 982-1212, DSN 551-1212 to arrange for a site visit.

2. Department of the Navy Physical Security Policy is not tied into security and law enforcement performance measurements. What Instruction should I reference?

(a) Currently many DOD security and law enforcement policies are being rewritten and reviewed for inclusion. The 5200.08 revision will include duty performance standards.

3. NOSSA AA&E explosive arcs are not recognized by DoD for (RMAG) Risk Management Advisory Group? No known AA&E reference of RMAG facility type storage.

(a) Explosives magazine storage and explosive arcs should be referred and managed by the installation/command Explosive Safety Officer but shared with security professionals who manage those programs.

4. What is the DoD source reference for waivers and exceptions in physical security requirements?

(a) Directive-type Memorandum (DTM) 13-005, "Deviations from the Physical Security Program," April 25, 2013. *DTM 13-005 will be included in the to-be-revised DOD 5200 Physical Security Program.*

5. Once a 0080 description is indexed, will it be released for publication?

(a) Mr. Tracy Kindle is conducting 0080 indexing and it will be published by March 2016 and will include job certifications.

__Thank you Letters__

Roy Jusino

On behalf of the Deputy Under Secretary of the Navy (Policy) (DUSN (P)), Security Directorate, we thank you for your presentation on Physical Security – Department of Defense Lock Program at the 2015 Department of the Navy Security Enterprise Conference. Thank you so much for your professionalism and expertise. The symposium was a success due in large part to the proficiency of our guest speakers. The knowledge all of you communicated to our physical security customers at this year's symposium was tremendous.

Donna Rivera

On behalf of the Deputy Under Secretary of the Navy (Policy) (DUSN (P)) Security Directorate, we thank you for your presentation on Office of the Undersecretary of Defense (OUSD(I) Physical Security Program at the 2015 Department of the Navy Security Enterprise Conference. Thank you so much for your professionalism and expertise - the symposium was a success due in large part to the proficiency of our guest speakers. The knowledge you communicated to our physical security customers at this year's symposium was tremendous.

Physical Security Branch Cont.

Richard Avery

On behalf of the Deputy Under Secretary of the Navy (Policy) (DUSN (P)) Security Directorate, we thank you for your presentation on Physical Security Certifications at the 2015 Department of the Navy Security Enterprise Conference. Thank you so much for your professionalism and expertise - the symposium was a success due in large part to the proficiency of our guest speakers. The knowledge you communicated to our physical security customers at this year's symposium was tremendous.

CAPT Joe Shipley, CAPT Matt Colburn, Mr. Ray Salamy, and Mr. Dave Speed

On behalf of the Deputy Under Secretary of the Navy (Policy) (DUSN (P)) Security Directorate, we thank you for your participation on CNIC/USFF/OPNAV 46 Panel Discussion at the 2015 Department of the Navy Security Enterprise Conference. Thank you so much for your professionalism and expertise - the symposium was a success due in large part to the proficiency of our guest speakers. The knowledge you communicated to our physical security customers at this year's symposium was tremendous.

Department of Defense Lock Program

(Click the logo to go to the DOD Lock Program)

Personnel Security Branch

Symposium summary:

The Personnel Security team focused on policy and the changing environment of personnel security programs and focus areas as a part of the Security Enterprise.

OUSD (I) Personnel Security Presentation:

- An overview of the DOD Personnel Security Policy and Programs including an update on completed instructions to include:
  - DoD Instruction 5200.02, DoD Personnel Security Program (PSP)
  - DoD Instruction 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)
- Focused overview of the process of obtaining policy and the history behind updating instructions and manuals
- Current draft policies under revision:
  - DoD Personnel Security Program, DoD 5200.2-R
  - DoD Personnel Security Program, DoD 5200.02
  - DoD Information Systems, DoDI 5200.jk
- Continuous evaluation and reporting requirements
  - A reminder of command roles and responsibilities for reporting behaviors of a security concern
- Ongoing discussion between OUSD(I) and the Director of National Intelligence on the issue of the Question 21, Psychological and Emotional health question, on the SF 86.

DoD Central Adjudication Facility:

- Addressed consolidation of the seven Central Adjudication Facilities and the DoD CAF ability to adjudicate favorable Suitability & HSPD-12 adjudications

SECNAV Council of Review Boards, Personnel Security Appeal Board:

- Reaffirmed their mission to adjudicate unfavorable personnel security determinations for the DON and is the final appellate authority for unfavorable personnel security determinations made by the DoD CAF.

Personnel Security Branch Cont.

Defense Logistics Agency, Defense Information Systems for Security (DISS):

- The DISS Family of Systems will enable an application of consistent standards and the reciprocal recognition of clearances through the implementation of the Case Adjudication Tracking System and Joint Verification System.

Top questions asked at the symposium:

1. **How do I obtain a CATS account?**

Answer: It is critical that all commands have access to CATS; an account can be obtained by contacting your Echelon II Security Manager with your request. They will approve your request for an account and forward your information to our office for account initiation. You will receive an email from the CATS team with instructions to set up your account. Additional assistance can be obtained from the CATS helpdesk or from your Echelon II Security Office.

2. **What investigation is required for military personnel to access systems?**

Answer: All military personnel, enlisted and officers, require the submission and favorable adjudication of a National Agency Check with Law and Credit as a minimum depending on rate, position, or duties.

3. **Why are eligibilities in JPAS being administratively withdrawn?**

Answer: In an effort to clean-up many "orphan" records in JPAS, the system will remove eligibility of a record which has no owing or servicing relationship, citizenship is listed as non-US citizen, and a separation date has not been entered on the record.

4. **How can the citizenship be changed in JPAS, when the record is showing non-US citizen?**

Answer: Since JPAS is a receiver of data from other systems, the member must first go to the servicing Personnel Servicing Detachment or Human Resource Office to ensure the personnel system has the correct information. This may require providing a copy of the birth or naturalization certificate.

5. **What is the minimum investigation required for HSPD-12?**

Answer: The National Agency Check with Written Inquiries and a favorable fingerprint check.

The Senior Director for Security and the Personnel Security Branch would like to extend thanks to Mr. Carl Kline, OUSD(I) Personnel Security Branch Chief, Mr. Daniel Purtill, DoD CAF Deputy Director, Mrs. Benita Jackson-Young, President, Personnel Security Appeals Board and to Mr. Michael Young, Defense Logistics Agency

Industrial Security Branch

Top Five Questions:

1. <u>What are some of the most common vulnerabilities and security violations that contribute to receiving a failed inspection?</u>
Persons without proper eligibility accessing classified, not reporting classified compromises, and un-cleared key management personnel.

2. <u>What will be the new NID process per DSS?</u>
DSS is responsible for proposing NIDs on behalf of GCAs, to include the U.S. Navy. Once the DSS proposal has been communicated to the GCA, the GCA has 30 days to respond affirmatively or negatively.
To begin the process of getting a DSS NID proposal, the Program Office must send to DSS (at NID@DSS.MIL) a copy of (1) the DD-254, (2) a description of the technology involved, and (3) some kind of statement verifying the accesses required by the contractor. If COMSEC is involved, Program Office will also need to provide a COMSEC list.

3. <u>What are the timelines for NID processing?</u>
DSS contacting GCA once NID is received: Same Day
Program Office Response to DSS: 5 days
DSS recommendation and communication to GCA: 20 days
GCA Communicate Decision to DSS: 30 days
If CA involved, DSS to CA: Same Day

4. <u>What is the expected release time of the National Contract Classification System (NCCS) new DD Form 254 database?</u>
The expected release time is Mar 2016 (tentative).

5. <u>What are the two SAP policy volumes?</u>
DoDM O-5205.07, Volume 3, "DoD Special Access Program (SAP) Security Manual: Physical Security "dated April 23, 2015. (When user selects this policy issuance, the screen will advise that it is a controlled document and that access requires a DoD PKI certificate.)
DoDM 5205.07, Volume 4, "Special Access Program (SAP) Security Manual: Marking" dated October 10, 2013

<u>Industrial Security</u>
OUSD (I) Industrial Security Presentation: This session provided an Industrial Security Policy overview. This presentation intent was to inform members about the National Industrial Security Program, Industrial Security Policy for Government Activities, Revision of the DD Form 254, Executive Order (EO) 13691 and Amendment of NISP EO 12829, Industrial Security Requirements for Contractors and to answer any questions that attendees have.

Industrial Security Branch Cont.

Ms. Heil OUSD(I) presentation provided the purpose of the NISP, ensuring agencies implementing directives are consistent with the NISP. Ms. Heil informed attendees' on current existing policies, pending policies that are currently being re-written and the status of the DoDM 5220.22, Volume 2.

The presentation included the procedures for exception to policy, roles and responsibilities of the National Industrial Security Program Policy Advisory Committee (NISPPAC) and Directive Type Memorandum (DTM-15-002) NID/FOCI process.

Defense Security Service

Defense Security Service (DSS) Presentation: This session provided information to attendees about the Defense Security Service (DSS) in relation to Industrial Security. Mr. Scott Dublin and Mr. Jamaar DeBoise (Industrial Security Specialist) enlightened attendees on the DSS Mission, (i.e. administering the NISP, supporting national security and the warfighter and oversee the protection of U.S. and foreign classified information in the hands of industry.

DSS presentation also included Executive Orders, DoD Directives and administering programs for DoD and 28 other Federal agencies. The main topics of discussion were on Facility Clearances (FCLs) and how the loss of FCLs can affect an overall contract being worked in that facility, also the most common security vulnerabilities that can cause the loss of an FCL.

Once the presentations were completed, the question and answer session were of great quality. Questions were asked and all presenters were able to answer questions to the satisfaction of attendees. Actually the Q&A session was so good the presenters actually stayed around and continued to answer questions that anyone had.

Thank you Letters

Ms. Valerie Heil

On behalf of the Deputy Under Secretary of the Navy (Policy) (DUSN (P)) Security Directorate, we thank you for your presentation on Industrial Security – OUSD (I) at the 2015 Department of the Navy Security Enterprise Conference. Thank you so much for your professionalism and expertise - the symposium was a success due in large part to the proficiency of your presentation. The knowledge you communicated to our Industrial security customers at this year's symposium was tremendous.

Mr. Scott Dublin/Mr. Jamaar DeBoise

On behalf of the Deputy Under Secretary of the Navy (Policy) (DUSN (P)) Security Directorate, we thank you for your presentation on Industrial Security – Defense Security Service at the 2015 Department of the Navy Security Enterprise Conference. Thank you so much for your professionalism and expertise - the symposium was a success due in large part to the proficiency of your presentation. The knowledge you communicated to our Industrial security customers at this year's symposium was tremendous.

Naval Security Enterprise Branch

Symposium summary:

An effective OPSEC program requires leadership buy-in, starting with the Commanding Officer, and the OPSEC Officer has the responsibility to implement the OPSEC process in order to protect the command's unclassified Critical Information and its personnel. OPSEC is primarily an operational program, but holistically looks at an organizations security programs.

The Navy's OPSEC Support Team (NOST) tailored a brief specifically designed for command leaders and security professionals, covering the OPSEC process and implementing OPSEC into the daily routine. The brief primarily covered the vulnerabilities associated with the latest technologies and avenues to mitigate those vulnerabilities. The high-impact, fast paced brief discusses how we all possess critical information, discusses the various threats among us, to include the recent ISIL on-line threats, demonstrates some to the vulnerabilities and provides recommended countermeasures.

Through short-take video clips and current real-world examples, the NOST demonstrated how important OPSEC is in our daily activities both on and off duty. Whether an engineer designing a weapon system or a public affairs officer charged with projecting information, each of us has a role in protecting critical information and practicing good OPSEC.

The well attended discussion, resulted in a number of questions, mainly focused on how to develop an effective posture in a resource constrained environment.   Presenters responded that OPSEC culture and practices do not require a tremendous investment, however management and oversight is essential for effective implementation. They explained that leadership has to decide how much risk they wish to assume and allocate resources accordingly.

DUSN(P) would like to thank Mr. James Magdalenski, Director of the Naval OPSEC Support Team (NOST) for this valuable contribution to the deliberations.

Executive Order (E.O.) 13587 direct all executive branch department and agencies that have access to classified information to implement an insider threat detection and prevention program. The purpose of the Program is to deter, detect and mitigate insider threats. The Department of the Navy (DON) established an Insider Threat Program, SECNAVINST 5510.37. Mr. Tony Simmons, DON Insider Threat Program Manager briefed the current state of the program. The DON Insider Threat Program Implementation Plan is in draft, and aiming to have the Agency Head signature by 4th quarter 2015.

Acquisition Security Branch

Symposium summary:

The Acquisition Security Branch offered two sessions for updates on the state of DON Acquisition Security Policy. Kate Fuster, Acquisition Security Branch Chief for DUSN Policy, provided an update to her office's current and future initiatives. Grant Merkel, SPAWAR Research Technology Protection Lead, provided an overview brief of acquisition security and how it aligns with industrial and information security. Mr. Merkel also provided insight to why cross-discipline cooperation is critical to technology protection for RDT&E and Acquisition (RDA) efforts. Kerry Moore, NAVSEA Research Technology Protection Lead, was also on-hand to assist in the discussions.

I would like to thank Mr. Merkel and Mr. Moore for their significant input and participation. Their support to the conference was just the latest example of their continued efforts to deliver Acquisition Security expertise and solutions to their respective commands, often with little or no DON Policy to direct and/or empower them.

The following topics were included in the session discussions:

- Acquisition Security is a new concept for many security professionals. It is accomplished through a collection of security assessment and related countermeasures taken by Programs and Projects to systematically protect Critical Technologies and also their associated Critical Program Information (CPI). Some of these measures may include: Operations Security (OPSEC), Anti-Tamper (AT), Threat Assessments, Security Countermeasures, Foreign Military Sales (FMS), and Supply Chain Risk Management (SCRM). A Program Protection Plan (PPP) serves as the core product that aligns these assessments and measures in a common, goal-driven process.

- There are currently several Security Specialists located in each SYSCOM designated as Research & Technology Protection (RTP) Representatives. These RTP Leads are working directly with our office to forge a new path for Acquisition Security initiatives. In March 2015, DUSN Policy Security Directorate and DON CIO Co-Chaired a SYSCOM Security Study that resulted in a clear need for Acquisition Security Policy. The findings presented that DON RTP Leads follow DoDI 5200.39 and DoDI 5200.44, but lack DON implementation guidance for a consistent horizontal approach enforceable by policy.

- Currently, DASN (RDT&E) Technology and Program Protection (T&PP) Office performs the role as lead for ASN(RDA) and DON on all program protection matters. DUSN(P) is working with DASN(RDT&E) to better define program protection roles so that the DON is better focused on policy and oversight for program protection. This effort was recently codified in the SECNAVINST 5500.36, as it describes the Naval Security Enterprise responsibility for providing central oversight and governance to CPI protection, Mission Assurance and Critical Infrastructure Protection. This shift will have little effect on RTP Leads as their primary mission remains the same. The RTP Leads shall act as the process owners for CPI (DoD 5200.39) and CA (DoD 5200.44). The RTPs shall continue to assist the programs with their Critical Program Information (CPI) Identification and Criticality Analyses (CA) of Critical Components, Threat Assessments and shall ensure additional security countermeasures are identified when needed.

A helpful analogy may be to observe the Acquisition Security personnel role, particularly as it pertains to CPI protection, as the conductor of a program protection orchestra. The conductor doesn't need to be a master of each instrument. He/she does need to know all the players and how they should complement each other and fill their role, so the ultimate product is the beautiful piece of music. It is the goal of this office to document that process and provide authoritative guidance to allow a robust, consistent program protection capability within the DON.

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
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/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

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

Continuous Evaluation is important & mandatory!

SEE SOMETHING WRONG
DO SOMETHING RIGHT!

Click for the NCIS Reporting Brochure
Click for NCIS How to Report a Crime