I am both grateful and humbled by the opportunity Ms. Greene, Deputy Under Secretary of the Navy (Policy) Department of the Navy, has given me to serve as your Senior Director for Security. I am especially appreciative of the opportunity to be working with such an expert group of individuals every day as we serve the Navy and Marine Corps. The noble cause of our profession, your individual and family sacrifices, and your dedication to the service of your country are an inspiration to me and make me want to match your professionalism every day. I recognize the immense responsibility that I have, and will work hard every day to fulfill my duties to you and the mission of the Navy and Marine Corps. I will do so in the most honest and effective manner I can. Mission success and your welfare will always be at the forefront of my decisions.

I must first thank the two pioneers who have gone before me, Ms. Kay and Mr. Bearor who have stood as two security sentinels that set a security and leadership standard in which we must all continue to strive to meet every day in every way. I stand on their shoulders now to make security inherently important to every aspect of the Navy and Marine Corps mission. I also want to thank Steve Ulate, Deputy Senior Director for Security for his superb support to the Security Directorate workforce during the six months he was the Senior Director for Security, Acting.

Lastly, I ask that each security professional, civilian or military take an active role in making the security mission relevant every day. Start or continue to improve your technical capabilities by getting your Security Professional Education Development certification(s). My office is standing by to support the community when needed. Click the picture below to send us your feedback and ideas.
Information Security

Applying Information Security Policy

**General safeguarding and destruction:** Personnel must keep classified information removed from storage under constant surveillance, covered with classified material cover sheets (Standard Form 703, 704 or 705) commensurate with the level of information when removed from a security container [or when retrieving a document from a classified printer in your workplace, draft documents, notes, worksheets, email printouts, etc.]. Additionally, personnel are reminded not to discuss classified information in public conveyances or places (e.g., train, plane, metro, bus, carpools, restaurants, common areas within the command such as vending machine areas, lunch rooms, kitchen areas, etc.) that permit interception by unauthorized persons. Classified material may not be opened or read in any area where it can be seen by unauthorized personnel. Destroy classified material when no longer required, including electronic storage media, to reduce classified holdings and the risk for loss or compromise of classified information. (Policy: DoDM 5200.01-Volume 3, Enclosure 2, Section 8; DoDM 5200.01-Volume 3, Enclosure 3, Sections 3 and 17; DONCIO msg 281759Z Aug 12, “Processing of Electronic Storage Media for Disposal.”)

For additional information on other topics, copy and paste this link into your internet browser: https://portal.secnav.navy.mil/orgs/DUSNP/Security-Directorate/Information-Security/SitePages/Home.aspx

Physical Security

**The DUSN (P) Physical Security Branch** provides policy, integration and oversight of several disciplines in the traditional security arena to include Physical Security, Law Enforcement, Antiterrorism/Force Protection (AT/FP), Key and Lock Control, Arms, Ammunition and Explosives (AA&E), Biological Select Agents and Toxins (BSAT), Critical Infrastructure Protection (CIP), and the Physical Security Enterprise Analysis Group (PSEAG). In their oversight role, the Physical Security Branch routinely participates in Security Site Assist Visits (SAV) to provide an objective external review of a command’s security program in order to provide guidance on processes, policies, and procedures to achieve compliance and develop a more effective security program. The team also regularly partners with the Navy Inspector General’s (NAVIG) Office during Command Inspections and Regional Area Visits in the health and compliance of security programs.

SAVs provide the command with an assessment of their current security posture, including recommendations for improving their plans, infrastructure, and program to meet standing requirements. SAVs also provides DUSN (P) Security with an opportunity to collect data in order to formulate more effective policy, advocate for resources, and establish a baseline understanding regarding the status of the Naval Security Enterprise.

For additional information on this article, copy and paste this link into your internet browser: https://portal.secnav.navy.mil/orgs/DUSNP/Security-Directorate/Physical-Security/SitePages/Home.aspx
Personnel Security

Extension of Periodic Reinvestigation Timelines to Address the Background Investigation Backlog

Effective immediately, Department of Defense (DoD) Components will implement the following actions to address the backlog:

The Office of the Under Secretary of Defense memorandum of 17 Jan 2017 states: Until further notice, Tier 3 Periodic Reinvestigations (PR) will continue to be conducted at ten year periodicity and Tier 5 PRs will be initiated six years after the date of the previous investigation (closed date) versus at the five year mark. This change in Tier 5 PR submissions will keep DoD Tier 5 PR within the current seven year reciprocity guidelines and will continue reducing the backlog. This change in periodicity will be reevaluated prior to December 31, 2017.

For additional information on this article, copy and paste this link into your internet browser: https://portal.secnav.navy.mil/orgs/DUSNP/Security-Directorate/Personnel-Security/SitePages/Home.aspx

Continuous Evaluation Realignment:

The Under Secretary of Defense memorandum of 19 December 2016 has realigned the Department of Defense Continuous Evaluation (CE) mission and CE Validation Cell resources from the Security Policy and Oversight Division to the Defense Security Service (DSS).

For additional information on this article, copy and paste this link into your internet browser: https://portal.secnav.navy.mil/orgs/DUSNP/Security-Directorate/Personnel-Security/SitePages/Home.aspx

Industrial Security

(NISP) Contracts Classification System Update:

SIGN UP to test the functionality of the National Industrial Security Program (NISP) Contracts Classification System (NCCS). NCCS will be deployed as the Enterprise Federal information system application supporting DoD and other Federal Agencies in the NISP by facilitating the processing and distribution of contract security classification specifications for contracts requiring access to classified information. For those who are involved with producing DD Form 254s (DoD Contract Security Classification Specification) for cleared contractors, being a volunteer tester of NCCS is a good opportunity to ensure familiarity with the system. NCCS establishes a centralized repository for the collection of classified contract security requirements and supporting data while automating the DD Form 254 processes and workflows. Over the next 12 months DSS will be working on a phased implementation with the DoD Components, the Federal executive branch agencies and cleared contractors. If you are interested in testing NCCS or accessing the system to see the functionalities, additional information can be found on the DSS website: http://www.dss.mil/diss/nccs.html


Enterprise Security

Insider Threat Update

The National Defense Authorization Act (NDAA) Fiscal Year (FY) 2017 significantly changes the definition of an insider threat to include workplace violence and incorporates an additional population of anyone that has, or once had, authorized access to information, a facility, a network, a person, or a resource of the DoD.

The DoD Insider Threat Management and Analysis Center (DITMAC) Reporting Memorandum was signed on 28 December 2016 mandating all 43 Department of Defense (DoD) Components to report information that meets the 13 reporting thresholds to the DITMAC. The DITMAC reporting thresholds include many of the same reporting criteria within the 13 adjudicative guidelines. The DITMAC reporting thresholds must be reported to the Department of the Navy Insider Threat Programs and the following offices will provide guidance on implementation:

DON Secretariat Insider Threat: Department of the Navy (DON) Assistant for Administration (AA); Operational Navy: Director of the Navy Staff (DNS) and Marine Corps: Deputy Commandant for Plans, Policies and Operations (DC, PP&O).

The DoDD 5205.16, Change 1 was signed on 25 January 2017. The Change 1 codifies the establishment and oversight of DoD Insider Threat reporting and information at the DITMAC. The DITMAC will: 1) Oversee the mitigation of insider threats to DoD resources; 2) Assess enterprise-level risks, recommend actions, oversee resolutions, and promote collaboration; and 3) Develop enterprise-level reporting thresholds, a repository for insider threat-related information and standards for the 43 DoD Insider Threat Programs based on law and policy requirements.

Send questions or comments to: DON_Security_Enterprise@Navy.mil

2018 DON Security Enterprise Symposium Survey

In early mid 2018 the DUSN (P) Security Directorate will host a Department of the Navy (DON) Security Enterprise Symposium. The symposium will have a similar format to the 2015 symposium. The symposium focus will be tailored towards hands on/how to sessions versus lectures. Speakers, topics and location will be announced at a later date. We are soliciting your feedback and input on the topics that you feel are most important to you. Let us know if you plan to attend and what your top three topics/areas of interest would be most beneficial. Send your input to the email inbox below: DON_SECURITY_ENTERPRISE_CONF@NAVY.MIL. Additional guidance is forthcoming as we get closer to confirming the date and location.
CONGRATULATIONS FROM THE
SENIOR DIRECTOR FOR SECURITY


Points of Contact:
Mailing Address:
Deputy Under Secretary of the Navy, (Policy), Security Directorate
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

Useful Links:
Department of The Navy, Security Executive:
National Counterintelligence and Security Center:
https://www.ncsc.gov/index.html
Information Security Oversight Office:
http://www.archives.gov/isoo/
Security Professional Education Development:
http://www.cdse.edu/certification/index.html
Security Training Education and Professionalization Portal (STEPP):
http://www.cdse.edu/stepp/index.html

*To access a website, copy and paste the link into your internet browser.