data collection and analysis plan. The CPTD exercise is part of United States Fleet Forces Command (USFFC) and Navy Warfare Development Command (NWDC) Fleet Experimentation Program (FLEX).

The Navy-Physical Security Enterprise and Analysis Group has worked closely with OPNAV, USFFC N042/FP, CNIC N3AT/N36X, NWDC, and other senior Navy security stakeholders in planning this exercise and I hope to see many of you in San Diego.

This is a busy time for the Naval Security Enterprise. The Office of the Under Secretary of Defense (Intelligence) is leading a Cross Functional Team dedicated to reviewing the end-to-end personnel vetting enterprise and also work to find solutions to the Personnel Security Investigation backlog.

I understand that the backlog is creating difficulties across the Department of the Navy for operational units, bases, stations, warfare centers, and our private sector industrial partners. I would like to assure you that this issue has the full attention of the Department of the Navy’s leadership and Dr. Livingston or I will provide a progress update in our next newsletter.

I am looking forward to attending the upcoming CITADEL PROTECT Technology Demonstration (CPTD) to be held at Naval Base San Diego, Ca from 11 to 15 SEP 2017. The CPTD will be integrated into a CNIC sponsored CITADEL PROTECT exercise designed to assess shore/afloat Anti-Terrorism/Force Protection integration and readiness.

The new technologies will be incorporated into field training exercise events and the effectiveness of each technology will be assessed to a set of established standards in conjunction with a data collection and analysis plan. The CPTD exercise is part of United States Fleet Forces Command (USFFC) and Navy Warfare Development Command (NWDC) Fleet Experimentation Program (FLEX).
Information Security

Department of the Navy (DON) Alternative Compensatory Control Measures (ACCM)

ALL requests to use ACCM must go to the DUSN (P) via DUSN (P) Security for review and approval. Contact Information Security Branch at DON_INFOSECURITY@navy.mil for additional questions on ACCMs. A new SECNAV Instruction on DON ACCM policy has been developed and is in the DON Tracker system for staffing and signature by the SECNAV. There are 11 appendices to this instruction to assist the command with requests, management and oversight of ACCM(s). Fiscal year 2018 ACCM Inspection schedule is under development and will be published to all DON commands with approved ACCMs in September 2017.

Waivers and Exceptions
Waivers and/or exceptions to Information Security policy request(s) - If and when a condition exist which prevents compliance with a specific standard, or costs of compliance exceeds available resources for requirements in Volumes 1-4 of the DoDM 5200.01 or the SECNAV Manual 5510.36, the Commanding Officer must submit a written request for a waiver or exception via the administrative chain of command to the DUSN (P) Security Directorate and forward via the DON tasking system (i.e., DON TRACKER). The required formats and information for submission of a waiver or exception can be obtained by emailing the DUSN (P) Security, Information Security Branch at: DON_SECURITY_INFO don_security_inf.fct@navy.mil.

Physical Security

Naval Criminal Investigative Service Security Training Assistance and Assessment Team (STAAT)

Mission is to provide training and vulnerability assessments in support of NCIS Director’s overall strategic priority of Preventing Terrorism, Protecting Secrets, and Reducing Crime.

STAAT is comprised of Physical Security Specialists (GS-0080) who have a variety of backgrounds which includes former Navy SEALs, Police Officers/Federal Agents, Active Duty Military Officers/Enlisted with extensive security experience. STAAT supports the Navy and Marine Corps, in an AOR covering over 900 ports and airfields in 65 countries, conducting: Port Assessments (PA), Airfield Assessments (AA), Physical Security Survey (PSS), Military Working Dog Certification/Assessments, Naval Inspector General (NAVIG) Command Inspections, Force Protection Readiness Reviews (FPRRs), Pre-arrival Port Security Assist Visits, Physical Security/Law Enforcement Assist Visits, Military Sealift Command Individual Ship Assessments (MSC-ISA), Hotel and Liberty Venue, School, Humanitarian, Courtrroom Assessments, and Route Analysis.

STAAT also instructs Security First Responder Course, Active Shooter Response Course, Surveillance Detection, Antiterrorism Officer Course Level II, and Naval Physical Security Course. It also conducts Inter-Operability Seminars in Detection of Installation Surveillance, Maritime Interdiction Operations, Law Enforcement Techniques, Protective Service Operations, and Incident Response to Terrorist Bombing. STAAT’s main staff and largest detachments are located on the North Island Naval Air Station, San Diego CA (STAAT PAC) and Joint Expeditionary Base Little Creek/ Fort Story, Virginia Beach VA (STAAT LANT).

To request STAAT assistance contact: STAATLANT: Mr. Lawrence Fiorillo at lfiorillo.lo@ncis.navy.mil STAATPAC: Mr. John Pasalich at or john.pasalich@ncis.navy.mil.
**Personnel Security**

**Standard Form 86**

The 2017 Standard Form (SF) 86 will be enabled in e-QIP on Sunday, 30 July 2017. The form revision was a collaborative effort with significant input from stakeholders across the National Security Community. Supporting documentation to include Draft Screenshots, a Draft Content Guide and other functional materials have been updated in the NP2 Public Library for public reference.

When the SF 86 is deployed, the National Background Investigation Bureau (NBIB) will disable the 2010 SF 86 at the same time. This will ensure all new initiatives are being requested on the 2017 SF 86 only. Requests that were initiated on the 2010 form prior to 30 July will continue to run their course and agencies will be able to release those requests to NBIB, they will be accepted and processed. NBIB will continue to process the 2010 SF86 for a period of time, which will be determined by case ingest numbers.

Once it is determined that the ingest numbers are at a minimal state, NBIB will turn off the 2010 SF 86 and any remaining cases will be terminated. NBIB will provide a notice to agencies with the date that the 2010 SF 86 will be turned off.

Also, the NBIB updated the INV 15 - Requesting NBIB Personnel Investigations document. Section 5.5 provides guidance on the submission of applications or resumes stating: “An application or résumé should only be submitted to NBIB when there is a substantive discrepancy between the application/résumé and the Standard Form, and the commander needs that discrepancy addressed during the investigation.” The Federal Investigation Notice No. 17-6 has additional information.

**Industrial Security**

**NISP Contract Classification System (NCCS)**

The latest version of NCCS (v5.10.1) deployed in June 2017. Among other improvements, the new release integrates a workflow process for receiving, submitting and approving National Interest Determinations, provides enhanced attachment handling, program information, data encryption and establishes a library with role based access protections.

User and technical testing was completed in May/Jun and the system is fully operational. To view new requirements see the NCCS site https://awfraid.nit.disa.mil/nccswbt/.

The Defense Security Service continues to implement NCCS in a phased approach. The phases are as follows: Phase 4 ends August 2017 Phase 5 - September to December 2017 Phase 6 - January to April 2018.

Currently there are 18 agencies and 51 industry who have registered in NCCS as of July 27, 2017.

DUSN (P) Security Office highly encourages program offices to contact DSS to begin implementation ICO NCCS as this system will be the new way of completing the electronic DD Form 254.

The National Insider Threat Task Force (NITTF) Mission

The primary mission of the NITTF is to develop a Government-wide insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies.

‘Any Given Day Video’

The NITTF produced Insider Threat video, ‘Any Given Day’, is now active on the unclassified website. Any Given Day was produced for departments and agencies to enhance their insider threat education and awareness efforts. Key messaging includes countering a negative “big brother” connotation and highlighting the balance between collecting information and privacy concerns. NITTF encourages the inclusion of this video into your existing training plan for your workforce.

You can access it directly by visiting the NCSC / NITTF webpage: https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

DoD Lock Program Website has Changed

The DoD Lock Program website has changed to a secure server as required by The White House Office of Management and Budget (OMB) Memorandum M-15-13. Our website is still public; the only difference is you will see “https” instead of “http” in the website address (URL). If you are using a DoD furnished computer, you should not be affected. DoD computers should have the appropriate DoD security certificates installed on them.

If you do encounter a security warning when navigating to the DoD Lock Program website (https://www.navfac.navy.mil/locks), you should install the latest DoD security certificate in your browser settings. Be assured that our website is safe. These warnings appear because your browser’s settings do not have the DoD security certificate installed. Note:

You may have to repeat this process over time because the DoD will issue new security certificates periodically.

The warnings will vary based on the type of browser you use. First, it will notify you that the site’s certificate is not valid or it cannot be recognized. Then it will give you options, for example:

“Continue to this website.” Although this option is not recommended, it allows you to continue safely.
SPēD Update
The SPēD Certification Program released new Security Fundamental Professional Certification (SFPC) and Security Assess Protection Professional Certification (SAPPC) Competency Preparatory Tools (CPTs) and updated Candidate Handbook on Aug. 8, 2017.

The new CPTs include updated materials including Cyber Skills content. The new SFPC and SAPPC assessments including Cyber content are scheduled to be published live for testing on 2 October, 2017.

Current SFPC Security Clusters are as follows:

- Information Security: 31%
- Personnel Security: 28%
- Physical Security: 10%
- Industrial Security: 13%
- General Security: 18%

Current SAPPC Security Clusters are as follows:

- Information Security: 31%
- Personnel Security: 28%
- Physical Security: 10%
- Industrial Security: 13%
- General Security: 18%

The information above will be reflected in the SPēD Certification Program CPTs and Candidate Handbook.

If new CPTs are not visible, you will need to refresh your internet cache. To do this, press the control- and alt keys then click- refresh simultaneously (the refresh circle in the address line of your browser). You also may need to update your flash cache.

To do this, click the window icon to access your control panel. Select the settings icon. Then search for the word “Flash” in the search box. Select “Flash Player”. Click “Delete All” box. Then click “Delete Data”. If that does not work, then try accessing in a different browser (other than Internet Explorer). Refer to the following web pages for information about Cluster changes: http://www.cdse.edu/certification/index.html

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_INT.FCT@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

Newsletter Editors: Tracy L. Kindle and Terrance McGowan

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/iOS/

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.