



DEPARTMENT OF THE NAVY
COMMANDER
NAVAL EDUCATION AND TRAINING COMMAND
250 DALLAS STREET
PENSACOLA, FLORIDA 32508-5220

NETCSTAFFINST 5510.1E
N04
16 Oct 2024

NETC STAFF INSTRUCTION 5510.1E

From: Commander, Naval Education and Training Command

Subj: NAVAL EDUCATION AND TRAINING COMMAND HEADQUARTERS STAFF
INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.30C
(b) SECNAVINST 5510.36B
(c) SECNAVINST 5239.3C
(d) OPNAVINST 5530.14E
(e) SecEA Directive 3 of 12 June 2017
(f) DoD Instruction 5200.48 of 6 March 2020

1. Purpose. To promulgate the Naval Education and Training Command (NETC) headquarters (HQ) staff information and personnel security organization, assign responsibilities, and show organizational relationships. This directive supplements references (a) and (b) and applies to all military, civilian, and contractor personnel assigned to the NETC HQ staff.

2. Cancellation. NETCSTAFFINST 5510.1D.

3. Command Security Management and Responsibilities

a. Chief of Staff (COS)

(1) Overall responsibility for the effective implementation and management of the NETC HQ Information and Personnel Security program.

(2) Designate, in writing, the following security positions:

(a) Activity Security Manager (ASM). The ASM is assigned to the NETC N044 staff code. Reports to the COS for matters pertaining to the information and personnel security program for NETC HQ. The ASM duties are defined in enclosure (4) of reference (a) and enclosure (2) of reference (b).

(b) Assistant ASM (AASM). The AASM is assigned to the NETC N044 staff code. The AASM reports to the ASM. The AASM primary duties will be to administer the day-to-day requirements of the information and personnel security program for NETC HQ staff.

(c) Information System Security Manager (ISSM). The ISSM is assigned to the information technology division, NETC N6. Duties and responsibilities of the ISSM are defined in references (a) through (c).

1. Staff Communications Security Material System Responsibility Officer (SCMSRO). The SCMSRO is located in NETC N6 and is the primary advisor to the COS on matters concerning the security and handling of communication security information and hardware and associated records and reports.

2. Naval Nuclear Propulsion Information (NNPI) Control Officer. The NNPI Control Officer is located in NETC N6 and is the primary technical advisor for NNPI processed within NETC HQ and performs NNPI indoctrination and debriefs when required.

(d) Operations Security (OPSEC) Program Manager. The OPSEC manager is a full-time position assigned to the logistics division, NETC N4. The OPSEC manager acts as the focal point for all OPSEC matters and maintains a thorough knowledge of NETC operations and familiarity with NETC plans and procedures.

(e) Anti-terrorism (AT) Officer (ATO) and Physical Security (PS) Officer (PSO). The ATO and PSO are assigned to the NETC N0052 staff code. The ATO and PSO are the lead staff officers responsible to the COS on AT and PS matters. Duties and responsibilities for PS and law enforcement are defined in reference (d).

b. Assistant Chiefs of Staff (ACOS) and Special Assistants (SA). Responsible for the proper safeguarding and control of classified material within their assigned areas and will:

(1) Direct persons responsible for the security of classified material within their divisions.

(2) Ensure only authorized individuals, as described in paragraph 11 of this instruction, are granted access to classified and restricted spaces or have access to classified or sensitive material and information.

(3) Ensure personnel requiring access to the secret internet protocol router (SIPR) network (SIPRNet) complete and submit Office of the Chief of Naval Operations (OPNAV) 5239/14 (System Authorization Access Request Navy (SAAR-N)) and NETC 5510/6 (SIPR Access Request). Personnel must have a current annual cyber awareness challenge and derivative classification training certificate on file. Also, it is required to be indoctrinated into the North Atlantic Treaty Organization and sign a NETC classified access indoctrination brief.

(4) Ensure General Services Administration (GSA) security containers (safes and secure rooms) are properly secured when not in use. Standard forms (SF) required and responsibilities:

(a) NETC security will affix the SF 702 (Security Container Check Sheet) monthly to the top or side of the safe and to the outside secure room door or posted on the wall next to the door.

(b) Ensure SF 702 is initialed every time (regular workday, evening, weekend, or holiday) by anyone who opens the security container, and again when it is locked. A second person must verify the security container is locked and counter-initial the SF 702. If a second person is not available, the person locking the container must double check the container is secured and counter-initial the SF 702.

(c) NETC security will post a SF 701 (Activity Security Checklist) monthly to the inside wall at the exit of secure rooms and all spaces and rooms containing a safe(s). The last person leaving the work space(s) for the day is required to check off and sign the SF 701.

c. Staff Duty Officer (SDO). Perform end-of-day security checks to include:

(1) Use NETC 5511/1 (NETC SDO Daily Security Check List) to record end-of-day security checks. Turn the completed form in to the security office daily.

(2) Ensure all secure rooms and safes are secure at the end of each workday. Certify secure rooms and containers are locked by initialing the SF 702 in the "Guard Check" block. If a secure room or safe is open and an authorized custodian is in the area of the container, the SDO will indicate such on NETC 5511/1. Follow procedures in paragraph 6 of this instruction if a security container is found open in an unoccupied space, or if classified material is left unattended.

(3) Conduct a visual inspection of the protected distribution system (PDS). The PDS visual inspection is required daily, to include weekends and holidays. The visual inspection requires the SDO to walk the entire length of the PDS looking for signs of penetration, tampering, and any other anomaly causing a deterioration of protection safeguards. Contact the NETC security office (for a map of the PDS). NETC security will conduct the annual technical PDS inspections.

d. All Hands. All NETC HQ personnel (military, civilians, and contractors) are responsible for proper safeguarding of classified and sensitive information. They will:

(1) Ensure classified material received by any means, except from the SIPRNet, from within or outside the command is immediately delivered to the security office to implement control procedures.

(2) Log all material printed out or downloaded from the SIPRNet in the SIPR media log.

(3) Store all classified material in a GSA safe and destroy when no longer needed (refer to paragraph 9).

4. Foreign Travel

a. NETC HQ Civilian and Military Personnel

(1) Per reference (a), official foreign travel will be reported to NETC security by those individuals who have access

to classified information. NETC security will provide a foreign travel brief prior to your departure and a foreign travel debrief upon your return.

(2) Unofficial foreign travel will be reported to NETC security within 14 days of travel. The following pertains to unofficial foreign travel:

(a) Travel to Puerto Rico, Guam, or other U.S. possessions and territories is not considered foreign travel and do not need to be reported.

(b) Unanticipated border crossings into any foreign country not previously reported and approved, regardless of duration, are discouraged. However, if deviations occur from approved travel itineraries, you must report this event within 5 business days of return.

(c) Unplanned day trips to Canada or Mexico must be reported upon return from travel within 5 business days.

(d) When emergency circumstances preclude full compliance with pre-travel reporting requirements, you must, at a minimum, verbally advise your chain of command and the ASM or AASM of your emergency situation with all pertinent specifics prior to departure. Full reporting must be accomplished within 5 business days of return.

(e) NETC security will provide the traveler with a foreign travel brief, and NETC 5510/7 (Foreign Travel Notification) will need to be completed and returned to NETC security for reporting purposes in Defense Information Security System (DISS) per reference (e).

(f) The traveler is required to complete page two, Foreign Travel Debriefing, of NETC 5510/7 upon their return to close out their foreign travel, and forward to NETC security.

(g) For military personnel, an Isolated Personnel Report (ISOPREP) is required. NETC security will assist to ensure the ISOPREP is updated.

(h) The traveler will need to report their travel to the ATO who will assist the traveler with the individual anti-terrorism plan and aircraft and personnel automated clearance system, if required.

b. NETC HQ Sensitive Compartmented Information (SCI) Eligible Civilian and Military Personnel. Those NETC HQ staff who have current SCI eligibility will be required to contact the Center for Information Warfare Training (CIWT) Special Security Officer (SSO) via e-mail (CIWT_SSO@us.navy.mil) to report official and unofficial foreign travel.

c. Contractor Personnel. Contractors are required to contact their facility security officer (FSO) to report all foreign travel.

d. Personnel are reminded of their responsibility to enter and exit the United States using a U.S. passport. It is a requirement to report the use of a foreign passport when traveling outside the United States.

5. Visitor Access and Visit Request

a. Visitors requiring access to classified areas onboard NETC HQ are required to have a visit request submitted in DISS from their government security management office (SMO), for federal civilians, and from the FSO for contractors, to SMO Code N000764 in order for NETC security to complete the visitor vetting and processing for access. Unannounced visitors will not be allowed entry into classified areas until their identity, security clearance eligibility, access level, and need-to-know are verified.

b. NETC HQ staff visiting other commands that require security clearance verification is required to submit NETC 5510/8 (NETC HQ Visit Request) to NETC security at least 3 working days prior to departure for processing.

c. NETC HQ staff who have a current SCI eligibility and require the use of SCI access for official travel are required to contact CIWT SSO for security clearance verification processing.

6. Security Incidents and Compromises

a. Within NETC HQ. If a security incident occurs, for example, if a safe or secure room is found unlocked in an unoccupied space, or classified material is found adrift in an unoccupied space, it will be reported immediately to the NETC security office during working hours or the SDO after hours. The container or classified material must be guarded until one of those officials arrives. Upon arrival, the ASM, AASM, or the SDO will secure the classified material and follow procedures outlined in reference (b).

b. Electronic Spillage. An electronic spillage is defined as data placed on an information system possessing insufficient security controls to protect the data at the required classification (e.g., secret information on an unclassified system). When an electronic spillage is discovered:

(1) Do not forward or attempt to delete the source of the electronic spillage. Immediately log off the computer (do not turn off or restart the computer) and disconnect the machine from the network.

(2) Report electronic spillages, whether initiated by NETC or by another command, immediately to the NETC security office, the NETC ISSM, and the chain of command. The security office will work with the ISSM to follow current guidance to report, contain, and clean the spillage.

(3) NETC ISSM will initiate and process OPNAV 5500/13 (Electronic Spillage Action Form) per current Naval Network Warfare Command policy. NETC security will report the spillage via DISS and ensure, at a minimum, that a security inquiry is conducted to determine if a preliminary investigation is required.

c. Reports of Violations or Compromises from Other Activities. Reports of violations or compromises will be reviewed by the ASM and Staff Judge Advocate to ensure that the requirements of reference (b) are met. Disposition of the reports will be made per reference (b).

d. Espionage. Contact with members of the NETC staff by anyone attempting to obtain classified or controlled unclassified information (CUI) must be reported immediately to the Naval Criminal Investigative Service (NCIS) and the NETC security office.

(1) NCIS in Pensacola, Building 3813, Naval Air Station, Pensacola, Florida, Phone 850-452-4211 or 224-772-9471.

(2) NETC Security Office, Building 628, Naval Air Station, Pensacola, Florida, Rooms 2-116 and 2-120, Phone 850-452-4015 or 850-425-2582.

7. Preparation of Correspondence and Messages

a. Classified Correspondence and Messages. Classified correspondence and messages will be properly marked and prepared per reference (b). Classification markings alert the holder to the presence of classified information and is a reminder for proper handling. It also enables the holder to understand exactly what is and is not classified. A properly marked document will identify the owner of the information (by letterhead or logo) and will indicate a date, overall markings (top and bottom), portion markings (each paragraph), source(s) of classification, the name of the person making the classification, declassification instructions, and any warning notices (if applicable). Contact the NETC security office for current guidance.

(1) Original Classification Authority (OCA). Original classification is the initial decision to classify new technology and information. These decisions will be made only by a designated OCA. Commander, NETC (CNETC) nor any other command officials in the NETC domain have been assigned or delegated duties as an OCA.

(2) Derivative Classification

(a) Derivative classification occurs anytime classified information is incorporated, extracted, paraphrased, restated, or generated in a new form. The duplication or reproduction of existing classified information is not derivative classification.

(b) All personnel with a national security eligibility (security clearance) may perform derivative classification. However, all personnel who apply derivative classification markings must receive annual training on the proper application principles of Executive Order 13526 prior to derivatively classifying information. Derivative classification authority for those who fail to complete annual training on derivative classification markings will be suspended. Contact the NETC security office to obtain training.

(c) Information may be derivatively classified from a source document(s), or through the use of a security classification guide. Those who perform derivative classification must be identified on the materials they derivatively classify by name and position or by personal identifier. Observe and respect original classification decisions and carry over to any newly created documents the pertinent classification markings, which include the source of the derivative classification, declassification instructions, overall markings, and portion markings.

(3) Working Material. Any material used to prepare classified correspondence or messages (e.g., drafts, notes, and computer disks) will be assigned the same classification as the document and must be stored and destroyed in the same manner as any classified material.

(4) Authorized Spaces. Secure rooms are the only authorized spaces where classified material will be prepared at NETC HQ.

(5) Electronic Storage

(a) Electronic classified material will only be stored on specifically designated and appropriately labeled classified removable media, to include removable hard drives, which can be secured in approved GSA security containers (flash or thumb drives are not authorized). Classified material will never be stored on a non-removable hard drive.

(b) In order to store electronic classified material onto removable media devices both the user and the workstation's removable media device (e.g., compact disc-writer, digital versatile disc-writer, or other media storage device, excluding

flash drives) must be authorized. Removable media request (RMR) must be approved by the ISSM and command information officer as the NETC removable media representative.

Note: The RMR process is not required when saving electronic classified material to the workstation's removable hard drive.

b. CUI. CUI is a marking for unclassified information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls, but does not meet the requirements for classification. CUI markings are only applied to information categories found on the CUI registry at <https://www.dodcui.mil/home/dod-cui-registry>. Prepare CUI correspondence per references (f).

8. Accounting and Control

a. Incoming Mail. The NETC mail clerk safeguards all incoming first-class mail in transit from the U.S. post office to the NETC mail room. NETC mail room personnel will deliver all U.S. Postal Service registered mail and GSA contract for overnight delivery (currently FEDEX) packages containing classified material to the security office. If other classified material is received by any other office or division, it must be delivered to the security office immediately. The security office is responsible for returning receipts received with classified material, assigning control numbers, preparing control sheets, and routing. The appropriate staff codes will be notified that classified material has been received and ready for review or pick-up. The security office will only release the material to a cleared individual with the need-to-know to review the material and determine disposition.

b. Outgoing Mail. Only security office personnel are authorized to mail out classified material from NETC HQ. They will assign serial numbers and ensure material is wrapped and marked per reference (b).

c. Incoming Messages. Classified messages are received by the AASM via secure means from the Naval Computer and Telecommunications Area Master Station. Incoming classified

messages will be delivered to the responsible code via SIPRNet email or held by the security office for appropriate staff personnel to review and determine a disposition. Classified messages will not be distributed during non-working hours unless they require immediate action.

d. Outgoing Messages. Classified naval messages must be prepared on a SIPRNet computer, printed, and then hand-routed to obtain the appropriate release signature. Once approved for transmission, deliver the paper copy of the message with the release signature and send the electronic version via SIPRNet email to the AASM. The message will then be transmitted via the current authorized delivery method.

e. Classified Material Removal from Security Containers. Classified documents not in security containers will be kept under constant surveillance and covered with the proper SF classified material cover sheet when not in use. Cover sheets SF 704 and 705, respectively, for secret and confidential material will be used. Classified material must be secured in GSA security containers during the custodian's absence from the work space. Co-workers will not be asked to safeguard classified material.

f. Reproduction of Classified Material. Classified material will not be reproduced without authorization of the security office. The only duplicating machine on which classified material may be reproduced is located in the Open Secret Storage room (2-139). Any classified material that is reproduced must be recorded and labeled (Copy 1 of 2, 2 of 2, etc.) on the original copy and reproduced copy and added to the inventory.

g. Hand Carry Classified Material and Couriers. Removal of classified material from NETC HQ buildings is prohibited except when authorized in writing by the ASM, AASM, COS, executive director, or CNETC. Authorization to hand carry classified material must be requested on NETC 5521/2 (Courier Request). The ACOS or SA of the staff member making the request must acknowledge the requirement for the classified material to be hand carried on NETC 5521/2. The completed NETC 5521/2, along with the completed courier statement of understanding, will be turned into the security office for preparation of the courier letter or card. Upon the courier's return to NETC HQ with the

classified material, all material must be delivered to the security office for inventory. If the classified material was delivered to the courier's travel location, the signed receipt from the individual that accepted the classified material is required.

h. Classified Meetings. Classified discussions at conferences, seminars, exhibits, symposia, conventions, or other gatherings (hereafter referred to as "meetings") are only authorized when disclosure of the information serves a specific U.S. Government purpose. Classified meetings will only be held at a U.S. Government agency or a cleared Department of Defense (DoD) contractor facility with an appropriate facility security clearance where adequate physical security and procedural controls have been approved. Contact the security office to ensure adequate physical security and procedural controls are in place prior to any classified meeting.

i. Emergency Action Plan. Under emergency conditions, and time permitting, classified material must be secured in an approved GSA security container. If that is not possible, it will be kept in the possession of the custodian and delivered to the security office directly after evacuation of the building has been accomplished for accountability. Safety of life is of paramount importance and takes precedence over securing classified material. Emergency conditions include a bomb threat, fire, civil disturbances, natural disasters, prolong abandonment of the building, etc.

9. Destruction of Classified Material

a. Under Normal Conditions. Only security office personnel are authorized to destroy classified material (paper) and classified hard drives. Destruction will be accomplished by shredding per the provisions of reference (b) and via Jackhammer located on CIWT, respectively. For unclassified hard drive destruction, you are required to make arrangements with the NETC N6 Saufley team for proper disposal.

b. Under Emergency Conditions. In the event of an emergency, all classified material will be stored, to the greatest extent possible, in a GSA approved security container.

c. Classified Clean-out. All classified material held at NETC HQ must be reviewed at least annually to determine the requirement for its continued need to be maintained. The security office will coordinate an annual classified material clean-out day to review and destroy any material no longer required. This also includes CUI material.

10. Control of Combinations. Combinations to classified material containers and changes thereto are controlled by NETC security.

11. Personnel Security

a. Security Clearance Eligibility and Access

(1) Only those persons whose regular assigned duties require access to classified or sensitive material based on a need-to-know will be granted access.

(2) All military members will be assigned secret access for assignment as SDO. Higher levels of access are only authorized for military members filling billets with a functional area code (FAC) "Q" on the activity manning document (AMD).

(3) Civilian positions must be properly coded as non-critical sensitive (CS) for secret access, or CS for top secret access before access will be granted.

Note: Non-CS must also be used for civilian positions requiring access to any sensitive type information, even when access to classified information is not required.

(4) Contractors must have the highest level of classified access authorized listed in the contract's statement of work, and there must be a completed DD 254 (DoD Contract Security Classification Specification). The contracting officer's representative (COR) is responsible for the completion and signing of the DD 254. However, consultation with the NETC security office on security issues and procedures when completing the form is required. CORs will provide a copy of completed DD 254 to the NETC security office.

b. Administrative Withdrawal of Access. Per reference (a), access to classified material will be administratively withdrawn from persons whose current duties do not require a need-to-know or access.

c. Common Access Card (CAC). Prior to CAC issuance, including contractors, a background investigation must be submitted to Defense Counterintelligence and Security Agency (DCSA), with favorable fingerprint results received. Due to the length of time this process can take, background investigations may be initiated prior to a member's actual start date. Should it be desired to bring a new employee onboard pending completion of the required investigation, an interim CAC may be granted as long as the employee has a favorable review of their SF 86, proof of U.S. citizenship, background investigation submitted to DCSA, and a favorable fingerprint check. Supervisors should contact the security office as soon as new employees are identified.

d. Access by Foreign Visitors. Visits by foreign nationals (FN) and representatives of foreign governments, foreign industry, or international organizations must be approved, and the disclosure authority determined, for each visitor. A FN is defined as anyone who is not a citizen or national of the United States, holds a green card, is an immigrant or resident alien, or works for a foreign owned company. In order to obtain access to Department of the Navy (DON) official information, the FN must contact their embassy to start a foreign national visit request. Official requests must be submitted by the applicable foreign government on the FN's behalf certifying the visitor's national clearances and need-to-know.

e. SCI. Access and briefings for persons who require SCI access will be processed by the CIWT SSO. Only military and civil service billets with a FAC "Q" on the AMD will be authorized SCI access.

f. Continuous Evaluation Program (CEP). By definition, CEP involves the uninterrupted assessment of a person for retention of a security clearance eligibility or continuing assignment to sensitive duties. This ensures a high standard of conduct and that questionable conduct or activities are promptly reported for adjudicative assessment. Per references (a) and (e), individuals must report to their supervisor and security office

and seek assistance for any incident or situation which could affect their continued eligibility for access to classified information or sensitive information. Co-workers have an obligation to advise their supervisor and security office when they become aware of information with potential security clearance significance.

g. Security Education and Training

(1) Orientation Briefings. At check-in, all NETC staff personnel will receive a security orientation briefing by the security office.

(2) Debriefings. The security office will debrief persons who have had access to classified material prior to their departure from federal service. Individuals must read and execute an OPNAV 5511/14 (Security Termination Statement) at the time of debriefing.

12. Violations of the Provisions of this Instruction

a. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice, or criminal penalties under applicable federal statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this instruction.

b. Civilian employees are subject to criminal penalties under applicable federal statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this instruction.

13. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON Assistant for Administration, Directives and Records Management Division portal page at [https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved %20Record%20Schedules/Forms/AllItems.aspx](https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx).

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager.

14. Review and Effective Date. Per OPNAV Instruction (OPNAVINST) 5215.17A, NETC will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, DoD, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 (Review of Instruction). This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

15. Forms

a. The following forms are available for download from the NETC public web site (<https://www.netc.navy.mil/Resources/NETC-Directives/>):

- (1) NETC 5510/6 (SIPR Access Request)
- (2) NETC 5510/7 (Foreign Travel Notification)
- (3) NETC 5510/8 (NETC HQ Visit Request for Official Travel)
- (4) NETC 5511/1 (NETC SDO Daily Security Check List)
- (5) NETC 5521/2 (Courier Request)

b. The following forms are available for download from the GSA forms library web site (<https://www.gsa.gov/reference/forms?footer>):

- (1) SF 701 (Activity Security Checklist)
- (2) SF 702 (Security Container Check Sheet)
- (3) SF 704 (Secret Cover Sheet)

(4) SF 705 (Confidential Cover Sheet)

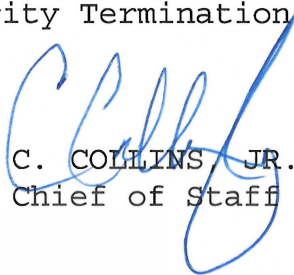
c. The following form is available for download from the Washington HQ Services public web site (https://www.esd.whs.mil/Directives/forms/dd0001_0499/): DD 254 (DoD Contract Security Classification Specification)

d. The following forms are available for download the Naval Forms Online web site (<https://forms.documentservices.dla.mil/order>):

(1) OPNAV 5239/14 (System Authorization Access Request Navy (SAAR-N))

(2) OPNAV 5500/13 (Electronic Spillage Action Form)

(3) OPNAV 5511/14 (Security Termination Statement)


C. COLLINS JR.
Chief of Staff

Releasability and distribution:

This instruction is cleared for public release and is available electronically on the NETC public web site (www.netc.navy.mil) or by e-mail at netc-directives@us.navy.mil.