DEPARTMENT OF THE NAVY
NAVAL SERVICE TRAINING COMMAND
2601A PAUL JONES STREET
GREAT LAKES, ILLINOIS 60088-2845

NSTCSTAFFINST 5510.l
N004
26 Jul 2022

NSTC STAFF INSTRUCTION 5510.l

From: Commander, Naval Service Training Command

Subj: NAVAL SERVICE TRAINING COMMAND STAFF INFORMATION AND PERSONNEL SECURITY REGULATION

Ref: (a) SECNAVINST-5510.30C
(b) SECNAVINST-5510.36B
(c) SECNAVINST 5239.3C
(d) OPNAVINST 5530.14E W CH3

1. Purpose. To promulgate the Naval Service Training Command (NSTC) staff Information and Personnel Security organization, assign responsibilities, and show organizational relationships. This directive supplements references (a) and (b), applies to all NSTC staff members (military, civilian, and contractor).

2. Command Management and Responsibilities.

a. Security Office. In this instruction, the terms Security Office or Security Office personnel are interchangeable and refer to one of the following positions:

(1) Security Manager. A collateral duty normally performed by the Administrative Special Assistant (N004). Appointed in writing and reports to Commander, NSTC (CNSTC) on matters of security but responsible to the Chief of Staff (COS) for administration of the Information and Personnel Security Program. The Security Manager's duties are defined in paragraph 2-3 of reference (a) and 2-2 of reference (b).

(2) Assistant Security Manager. A civilian position assigned to the N004A staff code. The Assistant Security Manager will be appointed in writing, and report to the NSTC Security Manager. The primary duties will be to administer the day-to-day requirements of the Information and Personnel Security Program for NSTC staff.

(3) Security Assistant. A civilian position assigned to the N004 staff code. The Security Assistant will report to the NSTC Security Manager. The primary duties will be to complete routine day-to-day Information and Personnel Security duties for the NSTC staff.

b. Information Assurance Manager (IAM). The NSTC IAM, appointed in writing, is assigned to the Information Technology (IT) Division (N6). Duties and responsibilities of the IAM are defined in references (a) through (c).

c. Division Directors and Special Assistants (DD/SA) are responsible for the proper safeguarding and control of classified material within their assigned areas and shall:

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

(2) Ensure only authorized individuals as described in paragraph 9 of this instruction are authorized access to classified/restricted spaces, or have access to classified or sensitive material/information.

(3) Ensure personnel requiring access to electronic classified material from the Secret Internet Protocol Router Network (SIPRNET) complete and submit OPNAV Form 5239/14 (SAAR-N), which is available from NSTC N6.

(4) Ensure classified material containers (safes) under their control are properly secured when not in use. Safe numbers, Open Secret Storage (OSS) area, responsible division, and room numbers:

(a) Safe number one, located in the Security Office (N004), room B-B36.

(b) Safe number two, located in the Flag Suite, in room 209.

(5) Ensure an unclassified inventory of all material in each safe is maintained outside of the safe. Provide the Security Manager or his designee an electronic copy of the inventory whenever changes are made.

(6) Ensure classified material security containers (safes and OSS) are properly secured using the following procedures:

(a) Affix Standard Form (SF 702) (Security Container Check Sheet) in a conspicuous location near all classified material containers.

(b) Ensure SF 702 is initialed by anyone, any time (regular workday, evening, weekend, or holiday) the security container is opened and 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) Post SF 701 (Activity Security Checklist) at the exit of all spaces/rooms containing classified containers and require the last person leaving the work space(s) to check off and sign the SF 701.

(1) Ensure all classified material containers are secure at the end of each workday. Certify each container is locked by initialing the SF-702 in the "Guard Check" block. If a security container is open but an authorized custodian is in the area of the container, the SDO will indicate such on NSTC Form 5511/1. Follow procedures in paragraph four of this

instruction if a security container is found open in an unoccupied space, or if classified material is left unattended.

(2) Conduct a visual inspection of the Protected Distribution System (PDS). The PDS visual inspection is required daily, to include weekends and holidays and 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. For a map of the PDS, contact the NSTC Security Office.

d. All Hands. Each NSTC staff are responsible for proper safeguarding of classified and/or sensitive information. They shall:

(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 or downloaded from the SIPRNET in the SIPR Media Log.

(3) Store all classified material in a classified material container listed in paragraph 3d(3) of this instruction, and destroy when no longer needed (paragraph 7 refers).

(4) Update the inventory list when adding or removing material from a classified security container and provide an electronic copy to the Assistant Security Manager.

3. Security Violations and Compromises.

a. Within NSTC Headquarters (HQ). If a classified container listed in paragraph 3d(3) is found unlocked in an unoccupied space, or classified material is found adrift in an unoccupied space, it will be immediately reported to the Security Office during working hours or the SDO after hours. The container and/or classified material shall be guarded until one of those officials arrives. Upon arrival, the Security Office Personnel or the SDO shall secure the classified material and follow the procedures outlined in Chapter 12 of 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 (i.e., 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 of 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 NSTC IAM Team, and to the chain of command. The Security Office will work with the NSTC IAM team to follow current guidance to report, contain, and clean the spillage.

(3) The Security Office will initiate the Electronic Spillage Action Form (ESAF) OPNAV 5500/13. The NSTC I.AM will complete and submit the form in accordance with current Naval Network Warfare Command policy.

c. Reports of Violations and/or Compromises from other Activities. Reports of violations and/or compromise will be reviewed by the Security Manager and Staff Judge Advocate to ensure that the requirements of reference (b), Chapter 12 have been met. Disposition of the reports will be made per reference (b), Chapter 12.

d. Espionage. Contact with members of the NSTC staff by anyone attempting to obtain classified information or any other official information shall be immediately reported to Naval Criminal Investigative Service (NCIS) and the NSTC Security Office.

(1) Contact information for NSIC and NSTC Security Office:

(a) NSTC Security Office telephone: 847-688-4510 extension 247 or 153.

(b) NCIS is located onboard Naval Station Great Lakes, Great Lakes, IL in Building 2, telephone: 847-688-5655.

4. Preparation of Correspondence and Messages. Classified correspondence and messages will be properly marked and prepared per reference (b), Chapter 6. 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 & 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 Security Office for current guidance.

a. Original Classification Authority (OCA). Original classification is the initial decision to classify new technology/information. These decisions shall be made only by a designated OCA. CNSTC nor any other command officials in the NSTC domain have been assigned or delegated duties as an OCA.

b. Derivative Classification

(1) 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.

(2) All personnel with an active security clearance may perform derivative classification. However, all personnel who apply derivative classification markings must receive training on the proper application principles of Executive Order 13526 prior to derivatively classifying information and at least once every two years thereafter. Derivative classification authority for those who fail to complete training on derivative classification markings at least once every two years will be suspended. Contact the Security Office to obtain training.

(3) Information may be derivatively classified from a source document(s), or through the use of a 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 the pertinent classification markings to newly created documents, including the source of the derivative classification, declassification instructions, overall markings, and portion markings.

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

d. Authorized Spaces. Spaces/rooms with a SIPRNET computer are the only authorized spaces where classified material will be prepared at NSTC.

e. Electronic Storage

(1) 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 security containers (flash drives or thumb drives are not authorized). Classified material will never be stored on a non-removable hard drive.

(2) In order to store electronic classified material onto Removable Media devices, both the user and workstation's removable media device (e.g., CD-Writer, DVD-Writer, or other media storage device, excluding flash drives) must be authorized. A Removable Media Request (RMR) must be approved by NSTC IAM and NSTC Command Information Officer (CIO) in their duties as the NSTC Removable Media Representative.

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

5. Accounting and Control.

a. Incoming Mail. The NSTC mail clerks shall safeguard all incoming first class mail in transit from the U.S. Post Office to the NSTC mail room. NSTC mail room personnel will deliver all U.S. Postal Service (USPS) registered mail and General Services Administration (GSA) contract for overnight delivery (currently FEDEX) packages to the Security Office upon arrival at NSTC to determine if they contain classified material. If any classified material is received in any other office or division, it shall 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 a cleared individual will go to the Security Office to review the material and determine disposition.

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

c. Incoming Messages. Classified messages are received by the Security Manager or his designee via secure means from the Naval Computer and Telecommunications Area Master Station (NCTAMS). 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 Assistant Security Manager. The message will then be transmitted via the current authorized delivery method.

e. Removal from Security Containers. Classified documents not in security containers shall be kept under constant surveillance and placed face down or covered when not in use. Classified material shall be secured in locked security containers only those listed in paragraph 3d (3) will be used during the custodian's absence from the workspace. Co-workers will not be asked to safeguard classified material.

f. Classified Access for Visitors. Anyone requiring access to classified material while visiting NSTC HQ must have their command submit a Visit Request in the Defense Information System for Security (DISS). Visit request in DISS must be submitted to the Security Management Office (SMO) Code: N002105. The Security Office will validate the visitor's eligibility for access and advise the visitor's host.

g. Hand Carry Classified Material/Couriers. Removal of classified material from NSTC HQ buildings is prohibited except when authorized in writing by CNSTC, Executive Director, COS, HQ Flag Unit Commanding Officer, or the Security Manager. Authorization to hand carry classified material must be requested on NSTC Form 5521/2 (Courier Request). The DD/SA of the person making the request must acknowledge the requirement for the classified material to be hand carried on NSTC Form 5521/2. The completed NSTC Form 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 NSTC HQ with classified material, all material shall be delivered to the Security Office for inventory.

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 shall 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 the appropriate security container. If that is not possible, it will be kept in the possession of the custodian and delivered to the Security Office as soon as possible after successfully evacuating the building. Safety of life is of paramount importance and takes precedence over securing classified material. Specific scenarios:

(l) Bomb Threat. Store all classified material in a proper container after searching the container for suspicious items. Lock the container and mark it as having been searched.

(2) Fire. If time permits, store classified material in a proper container and lock it prior to evacuation. If not, keep the material in your possession and out of sight of other persons until authorized to return to the building. The material will then be taken directly to the Security Office for inventory.

(3) Civil Disturbances and Natural Disasters with No Advance Warning. Make an effort to the maximum extent possible with respect to protecting classified material.

(4) Anticipated Civil Disturbances and Natural Disasters of Anticipated Short Duration. Store confidential material in an appropriate container and lock it prior to taking shelter or evacuating the building. Take secret material to the Security Office. Upon return to normal conditions, retrieve and inventory all secret material.

(5) Anticipated Prolonged Abandonment of the Building. Deliver all classified material to the Security Office.

6. Destruction of Classified Material.

a. Under normal conditions, only Security Office personnel are authorized to destroy classified material. Destruction will be accomplished by shredding per the provisions of reference (b), Chapter 10. The only authorized equipment for shredding classified material at NSTC in Great Lakes is in the Security Manager's Office, room B-B36.

b. Classified Clean-out. All classified material held at NSTC 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.

7. Control of Combinations. Combinations to classified material containers and changes thereto are controlled by the Security Office personnel.

8. Personnel Security.

a. Security Clearance/Access.

(1) Need-to-Know. Only those persons, whose regular assigned duties require access to classified or sensitive material on a need-to-know basis, as determined by their DD/SA will be granted access.

(2) Access Request. Requests for classified access and Information Technology level designation will be made to the Security Office on NSTC Form 5521/1. CNSTC, COS, The HQ Flag Unit Commanding Officer, and the Security Manager are the only NSTC staff authorized to grant access to classified material. Access to classified material will not be authorized until approval is granted.

(a) All military members will normally 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).

(b) Civilian positions must be properly coded as Non-Critical-Sensitive (N-CS) for secret access, or Critical- Sensitive (CS) for top secret access before access will be granted to the incumbent per reference (a), Chapter 5.

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

(c) 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, Department of Defense Contract Security Classification Specification Form. The Contracting Officer Representative (COR) is responsible for the completion and signing of form DD-254. However, consultation with the Security Office on security issues and procedures are required when completing form DD-254. CORs shall provide a copy of the completed DD-254 to the Security Office.

(d) IT positions require an appropriate level of background investigation prior to authorized access. These positions must be properly coded as either IT Level I or II on NSTC Form 5521/1, per reference (a), Chapter 5.

(e) Per reference (a), civilian positions with a position designation code of Non-Sensitive are required to be designated IT level III and requires rigorous IT controls to preclude visual access to information protected under the Privacy Act of 1974, proprietary data, and other protected sensitive information.

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

b. Common Access Card (CAC). Prior to a CAC being issued to anyone, including contractors, a background investigation must be submitted to Office of Personnel Management (OPM), with favorable fingerprint result received. Since this process can result in

new employees not obtaining a CAC for weeks, and could take several months, background investigations may be initiated prior to a member's actual start date. Supervisors should contact the Security Office as soon as new employees are identified.

c. Access by Foreign Visitors. Visits by foreign nationals (FNs) and representatives of foreign governments, foreign industry, or international organizations must be approved, and the disclosure authority determined, for each visitor. An 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 (FNVR). Official requests must be submitted by the applicable foreign government on the FN's behalf (normally the foreign government's Washington, D.C. embassy) certifying the visitor's national clearances and need-to-know.

d. Continuous Evaluation Program (CEP). By definition, CEP involves the uninterrupted assessment of a person for retention of a security clearance 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. According to reference (a), Chapter 10, individuals must report to their supervisor or appropriate security official 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 or appropriate security official when they become aware of information with potential security clearance significance.

e. Security Education and Training.

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

(2) On-the-Job Training (OJT). OJT will be given by the Security Office to personnel at the time classified access is formally granted, prior to the person actually accessing any classified information, and on an "as required" basis for personnel in the performance of their duties.

(3) Debriefings. The Security Office will debrief persons who have had access to classified material prior to their departure from federal service per paragraph 4-11 of reference (a). Individuals must read and execute a Security Termination Statement (OPNAV 5511/14) at the time of debriefing.

9. Forms Availability. All forms listed in this instruction are available from the Security Office.

10. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of September 2019.

11. Review and Effective Date. Per OPNAVINST 5215.17A, NSTC will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using

OPNAV 5215/40 Review of Instruction. This instruction will automatically expire ten years after effective date unless reissued or canceled prior to the ten-year anniversary date, or an extension has been granted

JENNIFER S. COUTURE

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via Department of the Navy Issuances Web site,