



DEPARTMENT OF THE NAVY

U.S. NAVAL SUPPORT ACTIVITY

PSC 817 BOX 1

FPO AE 09622-0001

NAVSUPPACT NAPLES INST 5511.2K CH-1  
N93

**14 OCT 2014**

NAVSUPPACT NAPLES INSTRUCTION 5511.2K CHANGE TRANSMITTAL 1

From: Commanding Officer, U.S. Naval Support Activity, Naples,  
Italy

Subj: COMMAND PERSONNEL/INFORMATION SECURITY PROCEDURES

Encl: (1) Revised enclosure (1)

1. Purpose. To transmit new pages 2 and 3, which revise the requirements to attend the annual security training.

2. Action. Remove pages 2 and 3 of the basic instruction and insert enclosure (1).

A handwritten signature in black ink, appearing to read "D. W. Carpenter", is written over the printed name below it.

D. W. CARPENTER

Distribution:

NAVSUPPACT NAPLES INST 5216.4AA

Lists I through V

Electronic via NAVSUPPACT NAPLES web site:

[http://www.cnmc.navy.mil/regions/cnreurfswa/installations/nsa\\_naples/about/departments/administration\\_n1/administrative\\_services/instructions.html](http://www.cnmc.navy.mil/regions/cnreurfswa/installations/nsa_naples/about/departments/administration_n1/administrative_services/instructions.html)



## DEPARTMENT OF THE NAVY

U.S. NAVAL SUPPORT ACTIVITY  
PSC 817 BOX 1  
FPO AE 09622-0001

NAVSUPPACT NAPLES INST 5511.2K  
N1

- 7 JAN 2014

### NAVSUPPACT NAPLES INSTRUCTION 5511.2K

From: Commanding Officer, U.S. Naval Support Activity, Naples,  
Italy

Subj: COMMAND PERSONNEL/INFORMATION SECURITY PROCEDURES

Ref: (a) SECNAV M-5510.30, Department of the Navy (DON)  
Personnel Security Program  
(b) SECNAV M-5510.36, Department of the Navy (DON)  
Information Security Program

1. Purpose. To provide supplemental guidance to references (a) and (b). This instruction specifies command procedures for safeguarding classified and sensitive information and managing access to classified material. This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. NAVSUPPACT NAPLES INST 5511.2J.

3. Applicability. This instruction applies to all military, U.S. Federal civilian employees and contractor personnel assigned to U.S. Naval Support Activity (NAVSUPPACT), Naples, Italy and serviced commands regardless of the level of security clearance held. All command members must understand the proper procedures for safeguarding classified information and for reporting security violations.

4. Objective. To assign responsibilities and identify local procedures to be followed for protecting classified and sensitive information, and educating assigned personnel.

5. Responsibility. Maintaining security of sensitive information is the responsibility of all members of the Naval Service and civilian employees of the Department of the Navy. This instruction provides local guidance to enable assigned personnel to meet this requirement.

#### 6. Violations of this instruction

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

**14 OCT 2014**

b. Civilian employees and contractors 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.

7. Security Organization

a. The Commanding Officer (CO) NAVSUPPACT Naples is responsible for the effective management of the Information and Personnel Security Program.

b. The Command Security Manager (CSM) will be designated in writing by the CO and meet the requirements of reference (b). The CSM is the CO's principal advisor on information and personnel security and is responsible for management of the program. The CSM reports to the CO for functional security and administrative matters.

c. The Controlled Unclassified Information Officer is the CSM, unless otherwise designated in writing.

d. The Assistant Command Security Manager (ACSM) will be designated in writing by the CO and meet the requirements of reference (b). The ACSM is assigned the additional duty of Secret Control Officer (SCO). The ACSM/SCO is responsible to the CSM for assisting in administration of the program and for receipt, custody, accounting, and disposition of secret material (other than message traffic) in the command.

e. The Information Assurance Manager (IAM) will be designated in writing by the CO. The IAM will be responsible for command information assurance matters. The IAM will maintain the command's Information Assurance Program.

f. The Command Physical Security Officer (CPSO) responsibilities are assigned to the Security Department Head. The CPSO is responsible to the CO for physical security of all NAVSUPPACT Naples facilities per Security Standard Operating Procedures.

8. Security Education. The Command Information Security Education Program ensures personnel understand the need to protect classified information and have a understanding on the procedures to do so. Annual security education is required to be completed by all uniformed personnel (regardless of access to

**14 OCT 2014**

procedures to do so. Annual security education is required to be completed by all uniformed personnel (regardless of access to classified information) and civilian employees whose job position requires a security clearance. Department heads will identify their personnel security clearance and ensure they attend the annual requirement. In addition to the following minimum formal education requirements, a program of regular security awareness training will be provided by publication of notes in the Plan of the Week and security information posters.

a. The CSM or ASCM will provide an initial Security Orientation Briefing to all newly reporting personnel, identifying procedures for handling classified information and reporting security violations, and safeguarding Privacy Act data. The initial briefing will include execution of a Classified Information Nondisclosure Agreement (SF-312), if required. For military personnel the original SF-312 will be forwarded to BUPERS (PERS-312C). For civilian personnel the original will be filed by the CSM.

b. The CSM or ASCM will provide annual security training to **uniformed personnel and those civilian personnel whose job position** require a completed security investigation. The topics listed below are the minimum requirements to discuss.

- (1) Changes in security policies and situations.
- (2) Review of command security situation, vulnerabilities, violations, and areas of concern.
- (3) Changes that could affect command security posture.
- (4) Review of key security practices.
- (5) Reiteration of individual's responsibility and trust in being given access to classified national security information.
- (6) Obligation to protect classified information through proper safeguarding and limiting access to those with clearance, access, and need-to-know.
- (7) Counterintelligence reminders about reporting contacts and exploitation attempts.
- (8) Continuous evaluation/report requirements.

-7 JAN 2014

(9) Focus on recent security issues (not a repeat of other briefings).

(10) Completion of the annual refresher training for Security, OPSEC, and Personal Identifiable Information located in the Total Workforce Management System database.

c. The applicable Department Head (or designated subordinate) will provide personnel with specific security procedures for their assigned tasks.

d. The CSM will schedule and track annual Counter Intelligence training for all personnel with access to material classified Secret or above. This training will be provided by the local NCIS Field Office.

e. The CSM or ASCM will conduct security debriefs for detaching personnel and update JPAS appropriately. The CSM will debrief personnel who are terminating active military service or civilian employment, whose Limited Access Authorization is expiring, or whose security clearance is revoked for cause or administratively withdrawn. Upon completion of the security debriefing, personnel must read and execute the SF-312 and a Security Termination Statement (SF 5511/14). The original Security Termination Statement will be given to the member upon completion and a copy will be maintained by the CSM. All detaching member must check out with the CSM or ASCM.

#### 9. Foreign Travel.

a. All military and U.S. Federal employees assigned to NAVASUPPACT Naples are required to report foreign (outside of Italy) travel to the CSM or ACSM.

b. Personnel will use the Aircraft and Personnel Automated Clearance System (APACS) to obtain country (and theater, if required) clearance, prior to travel. This applies to official and unofficial travel.

c. The Anti-Terrorism/Force Protection Officer will perform foreign travel briefings and debriefings, if required.

d. It is the traveler's responsibility to ensure these requirements are met before travel. To aid in planning, leave and request chit routing should not be delayed for these requirements. The applicable Department Head will ensure that all requirements are met prior to actually departing for travel.

- 7 JAN 2014

e. All military, U.S. Federal employees, and contractors assigned to NAVSUPPACT Naples and serviced commands are required to have submitted a background investigation in order to hold a new generation Common Access Card (CAC) and to have access to Department of Defense Information Systems. Personnel who fail to complete the proper background investigation will have their access to the SIPR/NIPR suspended until the paperwork is completed and personnel security investigation is open. If personnel refuse to complete the appropriate background investigation, the result is the loss of their CAC Card.

f. CSM will designate an annual Security Cleanout Day. On this day, specific attention will be focused on disposition of unneeded classified and controlled unclassified information material. Departments that hold classified material will review items held and any unnecessary classified material should be destroyed.

10. Classified Material Handling.

a. NAVSUPPACT Naples is not an Original Classification Authority (OCA), only a Derivative Classifier. Reference (b) Chapter 4 explains the associated duties. The CSM is responsible for routine questions of material classification.

b. Transmission and Transportation of Classified Material. Transmission refers to any movement of classified information or material from one place to another. Classified information will be transmitted either in the custody of an appropriately cleared individual or by an approved system or carrier. Classified information **may not be forwarded via guard mail.** Under no circumstances will classified material be mailed directly from departments. Hand-carry all classified material, which is to be mailed to the base Post Office. The Post Office will review classified material for proper marking, assign an accountable number and mail.

(1) The SCO will maintain a log of all classified material that is received or transferred out of the command. Records will be maintained for two years. Additionally, the SCO will retain copies of signed return receipts mailed back to originating agencies. All departments are responsible for notifying the SCO of material that they send or receive.

-7 JAN 2014

(2) Secret material will be covered by a receipt between commands and other authorized addresses. Failure to sign and return a receipt to the sender may result in a report of possible compromise.

(3) Receipts for Confidential material are required when transmitting to or from foreign address.

(4) Telephone Transmission. Classified information will not be transmitted over the telephone except via approved Secure Terminal Equipment (STE).

c. Safeguarding. Anyone who has possession of classified material is responsible for safeguarding it at all times and for locking classified material in appropriate security containers whenever it is not in use or under direct supervision of authorized persons per chapter seven of reference (b).

(1) Unclassified information may be collected to develop a clear picture of current and planned operations at sea and ashore, movement of personnel and equipment, force protection measures, and privacy act information. As this command is located in an overseas region, command members must be extremely vigilant in protecting unclassified material. All unclassified messages, schedules, and command correspondence must be shredded or otherwise destroyed before it is discarded. Command members must not discuss unclassified operations, duties or military functions with personnel who do not have a demonstrated need-to-know.

(2) Command members must report any unusual contacts or questions to the CSM.

d. Storage. Classified information, which is neither in use nor under the personal observation of cleared persons who are authorized access, must be stored in approved security container as prescribed in reference (b).

(1) Secret and Confidential material must be stored in a General Services Administration (GSA) approved container. GSA approved containers are clearly marked by a red label on a metal tag attached to the front of a container drawer.

-7 JAN 2014

(2) Each container used for the storage of classified material will be numbered and a master list maintained by the CSM. A Security Container Check Sheet, (SF 702) will be affixed to the outside of each container. The date, time and person(s) opening/closing/checking the container will be noted on the check sheet. The Security Container Information Form, SF 700, must be completed for each container and attached inside. The SF 700 envelope, containing each container's combination, must be delivered to the CSM. The CSM will maintain the master file of (SF 700) in a container of appropriate classification. One primary custodian and at least one alternate will be listed, along with their off-duty addresses and telephone numbers. A Maintenance Record for Security Containers/Vault Doors, OF 89, must also be completed and retained inside each container to record maintenance, repairs, damage, and periodic inspections. The CSM will conduct an inspection of all command security containers once every two years.

(3) The combinations to command security containers must be safeguarded. They will be released to only those command members who have a need-to-know the information contained in the material inside and are on the access list to the secure space.

(4) Acquisition of new security containers must be coordinated through the CSM in writing via memo. If the requirement cannot be met by relocating assets within a department or from other command departments, a new container will be procured. To relocate a security container, forward a memo to the CSM stating the container number, department, and old and new locations. To declassify a container, forward a memo to the CSM stating the container number, department, and that it contains no classified material.

e. NAVSUPPACT Naples is not authorized to store Top Secret material.

f. Marking. All classified material held at NAVSUPPACT Naples will be marked as prescribed in chapter six of reference (b). The CSM will assist command personnel in ensuring proper markings.

-7 JAN 2014

g. **Reproduction.** Reproduced copies must be afforded the same security control as the original and must indicate classification, any special markings, and must be remarked if markings do not copy clearly. Copies must be on a copier which is authorized to reproduce classified information. Only the CSM or the Executive Officer may authorize reproduction of Secret material. Confidential material may be reproduced, if authorized by the Department Head (DH). After completion of copying:

(1) Check the surrounding area for classified material and ensure the original and all copies have been removed.

(2) Check for stuck copies in the event of a malfunction.

(3) Run two pieces of blank paper through the copier on completion.

(4) Check paper path and any bins to ensure no copied pages are left in the copier.

h. **Inventory** will be conducted semiannually or, as directed by the CSM. When completed, the department will prepare and sign a full list of Secret material accounted for and notify the CSM of inventory results.

i. **Destruction.**

(1) Secret. Department security point of contacts will report the destruction of secret material, by memorandum or OPNAV Form 5511/12, to the CO for retention by the CSM. The memorandum or form will completely identify the material which was destroyed and how it was destroyed. Additionally, the inventory will completely identify all classified material which is retained.

(2) Confidential. There is no requirement to record destruction of confidential material. The cognizant DH may forward a record of the destruction to the CSM, if deemed warranted.

(3) Departmental security point of contacts will ensure that procedures are in effect to ensure that classified material is properly stored at the end of each workday.

-7 JAN 2014

(a) All classified material is stored in a locked security container.

(b) No classified material has been inadvertently discarded in wastebaskets.

(c) Space is properly secured, all windows and doors locked.

11. Access and Visit Procedures. All command personnel are responsible for assuring that classified material within their cognizance is made available only to those having the proper clearance and need-to-know has been firmly established. Personnel must ensure that unauthorized persons do not gain access to classified information by sight, sound or other means. Classified information will not be discussed with or in the presence of unauthorized persons.

a. Before authorizing a command member or visitor access to classified material, verify the level of authorized security clearance with the CSM or ACSM and ensure that the individual has a need-to-know of the information.

b. Notify the CSM of any visitors who may require access to classified information by having originating organization submit all visits through JPAS.

c. Disclosure of classified material to Foreign Nationals is tightly controlled and the CSM will liaison with outside foreign disclosure officers before releasing material.

d. It is incumbent on all command members to ensure that unauthorized persons are not permitted access to any command spaces. Suspicious activities must be reported to the NAVSUPPACT Naples Security Dispatch at DSN: 314-626-5638/9.

12. Requesting and Granting Clearances. Clearance and access are based on the results of background investigations leading to personnel security determination completed by the Department of the Defense Central Adjudication Facility (DODCAF) and reported in JPAS. All military, U.S. Federal employees, and contractors assigned to NAVSUPPACT Naples and serviced commands are required to complete a background investigation or re-investigation for proper eligibility.

-7 JAN 2014

a. Need-to-know is a determination that a prospective recipient has a requirement for access to, knowledge of, and possession of classified information in the official performance of their duties.

b. Clearance eligibility is an administrative determination by DODCAF that an individual is eligible for access to classified information of a specific classification category. The CSM will verify eligibility in JPAS. If the individual must complete the required paperwork for a background investigation, the CSM will identify the requirements, notify the DH and provide assistance. Failure to complete a required investigation or re-investigation is dereliction of duty and punishable under the UCMJ for military personnel. Civilian employees are subject to administrative sanctions of applicable Federal Statutes.

c. Access is the ability and opportunity to obtain knowledge or possession of classified information. Access is granted to permit an individual to perform duties of a particular billet at a particular command. Access is granted by the CSM and will be withdrawn upon detachment from this command or if the individual no longer requires access. If an individual changes duties within this command and no longer requires access at the level granted, the DH must notify the CSM immediately. Personnel access will be recorded in JPAS.

13. Continuous Evaluation. The CSM will continuously evaluate individuals with access to classified information and will report questionable or unfavorable information and/or other security clearance and access-related information to the chain of command and DODCAF. Questionable information will be submitted to DODCAF via JPAS. DODCAF will determine if the information affects continued eligibility for access to classified information. Continuous evaluation relies on all members of the command to recognize and report questionable or unfavorable security information. All assigned personnel must:

a. Report any known or suspected security violations to the CSM at DSN: 314-626-5397 or the ACSM at DSN: 314-626-5408.

b. Report to the CSM if you had any contact with foreign nationals attempting to gain unauthorized access to classified material. Additionally, report to the CSM and chain of command any continuing, close relationship (shared living quarters) or intentions to marry a foreign national. The CSM will be

- 7 JAN 2014

included in routing, for information only, on all marriage packages routed by service member. The request confirms intention to marry and the CSM will report this request to DODCAF. Reporting shared living quarters with a foreign national is the responsibility of the service member or civilian employee. Failure to report cohabitation with a foreign national reflects upon the trustworthiness and integrity of the individual and is punishable under the UCMJ and will be reported to DODCAF.

c. Ensure that any person seeking access to classified material has a bona fide need-to-know.

d. Practice telephone security, assuming that everything said is monitored, especially when using mobile phones and International Marine/Maritime Satellite (INMARSAT). Use secure means such as a Naval message, secure fax or registered mail to transmit classified material.

e. Ensure individual behavior is consistent with the expected level of trustworthiness, loyalty, reliability, and judgment of persons granted access to classified material.

f. Adhere to the specific procedures for handling, controlling, safeguarding, and using classified material that is identified in this instruction. Any questions about proper handling of classified material may be directed to the CSM.

14. Inspections. The CSM will schedule two different annual internal security reviews, ideally one every six months. Command inspectors will not be the CSM or ACSM and will be E-8 or above. They will utilize the Security Inspection Checklist from references (a) and (b). One inspection focuses on Information Security and the other focuses on Personnel Security. The results will be forward by formal memorandum to the CO via the CSM. The results of the inspections will be maintained by the CSM for two years. EKMS inspections and assist visits will be coordinated by the servicing EKMS account.

15. Security Discrepancies. A security discrepancy could be, but not limited to: loss, possible loss, compromise, or unauthorized disclosure of classified material.

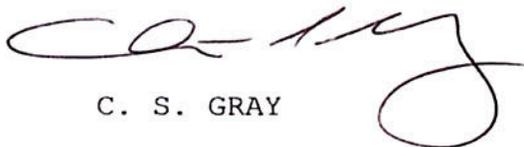
a. Any individual assigned to NAVSUPPACT Naples who becomes aware of a security discrepancy or suspected compromise will immediately notify his supervisor and the CSM or CO.

- 7 JAN 2014

b. In the case of lost or misplaced material, the person in charge of the material will immediately notify his supervisor and initiate a thorough search, reporting the results of the search to his supervisor and the CSM. The cognizant department head will prepare a report of the circumstances surrounding the loss.

c. The CSM will provide the CO with a recommendation regarding any command investigation or outside agency involvement. The cognizant department head will provide direct support to the CSM during and after the investigation. The CSM will ensure results are reported per chapter 12 of reference (b).

d. Compromises, whether intentional or negligent, are punishable under the UCMJ in the case of military personnel. Civilian employees and contractors are subject to criminal prosecution and administrative sanctions under the appropriate federal statutes.

  
C. S. GRAY

Distribution:

NAVSUPPACT NAPLES INST 5216.4AA

Lists: I through IV

Electronic via NAVSUPPACT NAPLES web site:

[https://www.cnic.navy.mil/regions/cnreurafswa/installations/nsa\\_naples/about/departments/administration\\_nl/administrative\\_services/instructions.html](https://www.cnic.navy.mil/regions/cnreurafswa/installations/nsa_naples/about/departments/administration_nl/administrative_services/instructions.html)