



DEPARTMENT OF THE NAVY
NAVAL DENTAL CENTER
2310 CRAVEN ST.
BOX 368147
SAN DIEGO, CALIFORNIA 92136-5596

ORIGINAL

file

NAVDENCENS DIEGO INST 5510.2C
012
27 FEB 1996

NAVDENCEN SAN DIEGO INSTRUCTION 5510.2C

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) OPNAVINST 5510.1H

Encl: (1) Personnel Security Check in Procedures

1. Purpose. To set forth procedures for the receipt, control, safeguarding, and dissemination of classified material and to provide direction on the Information and Personnel Security Program (IPSP) for military and civilian personnel within Naval Dental Center, San Diego. Enclosure (1) provides check in procedures for personnel security.

2. Cancellation. NAVDENCLINICINST 5510.2B.

3. Definitions

a. Clearance. An administrative determination by competent authority that an individual is eligible for access to classified information of a specific classification category.

b. Access. The ability and opportunity to obtain knowledge or possession of classified information. An individual does not have access to classified information merely by being in a place where such information is kept, provided the security measures which are in effect prevent him from gaining knowledge or possession of such classified information.

c. Need to Know. The necessity for access to, knowledge of, or possession of classified information in order to carry out official military or other governmental duties. Responsibilities for determining whether a person's duties require access to classified information and whether authorized to receive it rests with the possessor of the classified information and not with the recipient.

4. Responsibilities

a. Security Manager (SM). A member of the command possessing a TOP Secret or Interim Top Secret security clearance shall be assigned by the Commanding Officer as the Security Manager. The SM shall:

Naval Dental Center, San Diego

TOL

NAVDENCENS DIEGO INST 5510.2C

27 FEB 1996

(1) Ensure that all personnel who are to handle classified material are appropriately cleared and instructed in accordance with reference (a).

(2) Develop and administer the Command's Information and Personnel Security Program (IPSP) in compliance with reference (a) and CINCPACFLT directives.

(3) Oversee and coordinate information security education requirements in accordance with reference (a).

(4) Conduct inspections to evaluate the effectiveness of the IPSP within the command.

b. Top Secret Control Officer (TSCO). The Executive Officer is hereby assigned as the Top Secret Control Officer.

(1) The TSCO shall hold a final Top Secret clearance as approved by the Department of the Navy, Central Adjudication Facility (DON CAF).

(2) This command does not have the capability of storing Top Secret materials. Once notified by the Communications Center of a Top Secret message, the Top Secret Control Officer will go to the Communications Center to review the message.

(3) In the event that the material needs to be utilized at the dental clinic, the TSCO will ensure that the material and information is accounted for, transported, disseminated, safeguarded and returned to the Communication Center for storage in accordance with reference (a).

c. Classified Material Control Officer (CMCO). The Head, Personnel Administration Department is hereby assigned as the Classified Material Control Officer. The Assistant Head, is hereby assigned as the Classified Material Control Assistant. The CMCO and CMCA shall:

(1) Be responsible for the security and proper handling of classified material in accordance with reference (a).

(2) Ensure classified material is locked in storage containers/areas approved by reference (a).

(3) Ensure inventory of classified material is performed in accordance with reference (a), periodically and reported to the SM.

27 FFB 1996

(4) Ensure classified materials are destroyed in accordance with reference (a).

(5) Ensure proper administrative processing of all required documentation for clearance and access actions, service record entries, security briefing and termination statements.

(6) Maintain a roster of personnel authorized access to classified material.

d. Internal Review Officer. The Command Evaluation Coordinator shall conduct an annual review of the IPSP.

e. Command Duty Section. The duty section shall perform a security check of the CMCO's office prior to 2400 daily, and properly complete the Activity Security Checklist (ASC) which will be retained for 90 days.

f. Users of Classified Materials. All users of classified materials will be familiar with reference (a) and with the procedures set forth herein.

5. Procedures for Granting of Clearance and Access. All personnel who receive, prepare, or have access to classified information, shall be cleared in accordance with reference (a).

a. Military Personnel

(1) Supervisors must determine the level of clearance and access required of their assigned personnel and request the same from the Security Manager (SM). A complete justification, based on the work performed and the individual's need to know, shall be submitted with the request for clearance and access.

(2) Authority to grant individual final clearances rests with the Department of the Navy Central Adjudication Facility (DON CAF).

(3) The CMCO will cause the OPNAV 5510/413 Personnel Security Action Request to be completed, forwarded to DON CAF and will ensure the service member is given a security briefing and that documenting papers are completed.

(4) Provided the required investigation has been completed and no contraindications to clearance are known, interim clearance and access may be granted by the commanding officer, pending final approval by DON CAF.

27 FFB 1996

b. Civilian Personnel

(1) Except under extraordinary circumstances, clearances will not be authorized for any civilian employee whose position description (PD) does not indicate the position as "critical sensitive" or "non-critical sensitive" as defined in reference (c). PDs for which these designations are requested must be submitted for approval to the SM. The description of duties must clearly show the need for clearance and access to classified material.

(2) The Naval Hospital San Diego Human Resource Office will ensure that investigative requirements of reference (a) are followed either immediately after appointment or prior to appointment, as directed. Results of investigations and clearance authority, when received, will be passed on to the SM. Security access may then be granted based on these results.

(3) The CMCO will cause the OPNAV 5520/20 to be completed and will ensure the employee is given a security briefing and that documenting papers are completed.

6. Security Education

a. The Security Manager and Classified Material Control Officer shall receive formal training in the management of the IPSP. Documented completion of NAVEDTRA 10987-D Security Manager Correspondence Course or equivalent classroom training satisfies this training requirement.

b. All personnel who are to have access to classified material shall be thoroughly familiar with this instruction, formally briefed by the SM or CMCO, and shall have signed an SF-312, Classified Information Non-disclosure Agreement.

c. The Command Security Education Program shall consist of the following minimum requirements:

(1) Orientation (all command members)

(a) Identification and responsibilities of the Security Team.

(b) Responsibilities of each command member in the program.

27 FEB 1996

incident. (c) Responsibilities if involved in a security
nationals. (d) Foreign travel and contacts with certain foreign

(2) Refresher Briefings (Personnel with clearances)

(a) Annually;
(b) Tailored to command mission;
(c) NCIS, Video Tapes, FLTSUPGRU are available for
assistance.

(3) Debriefings (Personnel with clearances)

(a) Termination of active duty, employment;
(b) Conclusion of Limited Access Authorization;
(c) Clearance revoked or administratively withdrawn;
(d) Inadvertent access to information ineligible to
receive.

(2) Command Security Education File. Documentation of all
security education including: POW notes, posters, briefing
attendance rosters and course completion documentation.

7. Classified Material Management.

a. Incoming Message Traffic

(1) Procedure during working hours:

(a) Personnel Administration Department will download
message traffic via the gateguard once daily.

(b) The CMCO will receive and review all traffic, log
and assign control numbers to each piece of classified material
to be retained.

(c) The CMCO will turn materials over to the Security
Manager for review and appropriate routing.

(d) After routing the material will be returned to
the CMCO for safekeeping.

27 FFB 1996

(2) Procedure for after working hours: If priority, immediate or flash classified message traffic information is received the OOD will do the following:

(a) Ensure an appropriate command journal entry is made.

(b) Contact one of the personnel authorized to download messages via gateguard (list in the watchstanders' guide).

(c) Ensure that no person, not authorized to receive classified material, accepts custody of such material. Urgency is not adequate justification for accepting classified material without clearance or authorized access.

(d) Ensure that the message is transported, safeguarded, and stored in accordance with this instruction, until relieved by the SM, CMCO, or their designee.

b. Incoming Classified Mail. Correspondence addressed to the command shall be handled by administrative personnel with a Confidential or higher, clearance and access. When classified correspondence is received, the inner envelope should be clearly stamped to indicate the overall classification of materials it contains. This container will be hand delivered to the CMCO who will then follow the same handling procedures established for message traffic.

c. Outgoing Classified Messages

(1) By reference (a), classified material must be transported and stored internally with cover-sheets.

d. Outgoing Secret Correspondence

(1) Follow packaging, labeling and mailing procedures in reference (a).

(2) Each piece of correspondence will be logged in the classified material log. Include a return receipt in the inner envelope with each piece of outgoing material classified Secret. The returned signed original receipt will be attached to the file copy of outgoing classified materials. Failure to sign and return a receipt to sender may result in a report of possible compromise.

e. Outgoing Confidential Correspondence

(1) Follow packaging, labeling and mailing procedures in reference (a).

f. Classified Material Log. A Classified Materials Log containing the data required by reference (a) shall be maintained by the CMCO.

g. Storage of Classified Material. When not in use, all classified material will be stored in a file-safe steel container meeting the requirements of reference (a). The safe will be maintained in the Headquarters, Administrative Office.

h. Routing. Upon receipt, the SM or CMCO will attach OPNAV 5216/10 Correspondence Material Control Form, to the classified material and then hand carry to each person designated for access to the attached material. After routing the classified material will be returned to the CMCO for safekeeping.

i. Inventory. A sight inventory is required for material classified "Secret".

(1) Secret material will be inventoried upon change of command, change of custodian, or at least annually.

(2) Change of custodian inventories will be conducted by both the incumbent and the receiving officer. A custodian who cannot account for classified material prior to detachment or relief will not be detached or relieved until an investigation is conducted.

k. Destruction of Classified Material. Material no longer required, superseded, or out of date, shall be destroyed in accordance with reference (a).

(1) EMERGENCY Destruction. In the event of a natural disaster, civil conflict or imminent hostile acts by aggressor groups or nations, which could result in possible compromise of classified information, immediate action shall be initiated to destroy all classified material. The following procedures shall be followed:

(a) If directed by the CO, the Security Manager will destroy all classified material by shredding.

27 FEB 1996

(b) In the event the shredder is not operational, the classified material may be destroyed by burning in metal waste paper baskets or other suitable metal containers when necessary.

(c) Secret materials will be destroyed first followed by "Confidential" and "For Official Use Only."

(d) Destruction will be implemented in a manner which will minimize the risk of loss of life or injury to personnel.

(e) Accurate information concerning the extent of emergency destruction of classified material is second in importance only to the destruction of the material itself.

(f) After destruction, report the facts surrounding the destruction to the Chief of Naval Operations (OP09P) with a copy to BUMED, Washington, DC, and COMNAVBASE, San Diego. Reports shall contain the following:

1 Identification of the items that may not have been destroyed.

2 Information concerning classified material which may be presumed to have been destroyed.

3 Identification of materials destroyed and method of destruction.

1. Compromises and Security Violations

(1) The disclosure of classified information to unauthorized persons constitutes a compromise. When this occurs or is suspected of occurring, the SM shall be informed immediately.

(2) If the safe containing classified materials is found unlocked in the absence of authorized personnel, immediately contact the SM and CDO. The container shall be guarded until the SM arrives. The SM will inspect the classified materials involved, lock the container, and make a security violation report to the CO.

(3) If classified material is found outside the proper container, unattended, or in the possession of a person not authorized the level of access for which the material is classified, immediately take possession of the material,

NAVDENCENS DIEGO INST 5510.2C
27 FEB 1996

safeguard it and ensure that it is delivered to the CMCO, SM or other competent authority. Report any possible compromise to the Security Manager.

(4) The SM will conduct a preliminary inquiry to establish one of the following:

(a) A compromise did not occur (terminate inquiry). If this is determined, the initial inquiry will be sufficient to resolve the incident and is considered adequate to support any possible disciplinary action which may result from a security violation.

(b) A compromise did occur. If this is determined, the incident will be reported to the CO and a determination of the severity of the compromise will be made in accordance with reference (a).

(5) Reports of compromise shall be forwarded to COMNAVBASE for review.

(6) Reporting to the Naval Criminal Investigative Service (NCIS) is required in cases of:

(a) Sabotage, espionage or deliberate compromise of classified information.

(b) Contacts with citizens of communist controlled countries.

(c) Suicide or attempted suicide of personnel who have had access to classified information.

(d) Prolonged unauthorized absence of an individual who has had access to classified information.

m. Automatic Data Processing of Classified Material

(1) No classified material shall be input, produced, stored, or otherwise processed on any Naval Dental Center, San Diego computer equipment unless designated.

n. Miscellaneous

(1) Classified information will be discussed only in the immediate presence of authorized persons and where unauthorized persons cannot overhear the discussions. Particular care will be taken when visitors or workmen are present.

27 FEB 1996

(2) Preliminary drafts, carbon sheets, working papers and similar items containing classified information will be dated and marked to reflect the highest classification of material contained in the notes. Each paragraph will be marked in parenthesis, with the highest classification of information it contains. Working papers will be stored in file-safe when not being used. Normally, working papers will not be maintained in excess of 90 days and will be destroyed when no longer required. A destruction report is not required for destruction of working papers.

(3) Correctable film typewriter ribbons used in preparation of classified material will be labeled, handled, and stored at the highest level of classification for which they have been used. They will be destroyed as classified waste.

(4) Voice recordings will not be utilized during briefs or presentations which contain classified materials.

(5) Telecopier, and Facsimile (FAX) will not be used to transmit classified materials.



R. C. MELENDEZ

Dist:

List I, Case 1, 2

NAVDENCENS DIEGO INST 5510.2C
27 FEB 1996

PERSONNEL SECURITY CHECK IN

1. Screen all service records for OPNAV Form 5520/20 (Attachment A). These forms will be retained in the division officer's records until service member checks out of the command. Personnel checking into the command without information in Part II, Record of Investigation, under column type, agency and date will have their form original 5520/20 forwarded via regular mail to Headquarters Administration Office. If Part II of the form is completed it will be filed in the division officer's records. Personnel checking into the command with a "Confidential" clearance or above will forward the same to Headquarters Administration Office. All original forms will be updated and returned to their respective clinics.

PERSONNEL SECURITY CHECKOUT

1. Personnel departing the Navy will fill out a OPNAV Form 5511/14 Security Termination Statement (Attachment B). The Senior Enlisted Leader/Leading Petty Officer will ensure the service member has received an oral debrief, circle which ever applies in paragraph six and have service member provide Social Security Number, signature and date. The SEL/LPO will then sign the witness block as indicated, and provide service member with the original for entry into the service record, a copy will be retained by the clinic for two years.

OFFICE SPACES AND SAFE COMBINATIONS

1. All office spaces with safes shall maintain a Standard Form 701, Activity Security Checklist (attachment C), only items that apply need be checked. The Word "Security" can be crossed out and the blank boxes can be filled in to read "check the safe." This only applies to an officer where a safe is located. The last person to leave the office at the end of each will ensure the checklist is complete. These forms only need to be retained for thirty days, unless an incident has occurred.

2. All safes will have a Standard Form 702 "Security Container" Check Sheet (Attachment D) attached conspicuously, and will be filled in whenever the safe has been opened. If an office is being checked on a daily bases but the safe not opened everyday the guard will check the blocks being signed by the person who is checking the office.

3. All combination changes will be hand delivered to the Security manger via a Standard Form 700, Security Container Information (Attachment E) envelop. Before you hand deliver form 700, ensure the following:

Enclosure (1)

NAVDENCENS DIEGO INST 5510.2C

27 FEB 1996

a. The top sheet is properly filled out with the correct information.

b. Card 2A (Attachment F) has been filled out and insert in the envelop, Sheet 2A.

c. Sheet 2 is sealed, initialed, dated and sealed with tape.
4. Safes will be numbered. The number will consist of the building number followed by a dash and then the number. Example: 3230-01. This number will also be entered on Sheet 1 of Standard Form 700. Only the number 01 will appear on the safe itself.

NAVDENCENSIEGOINST 1650.2F
14 FEB 1996

COMMANDING OFFICER'S AWARD FOR EXCEPTIONAL SERVICE
INFORMATION SHEET

Full Name: _____ RANK: _____

Length of time in service: _____

Length of time in Command: _____

Branch/Department: _____

Education:

_____	_____	_____
(year)	(degree)	(institution)
_____	_____	_____
_____	_____	_____
_____	_____	_____

Post-Graduate Training:

_____	_____	_____
(year)	(position)	(institution)
_____	_____	_____
_____	_____	_____
_____	_____	_____

Responsibilities:

Attach a proposed Navy Achievement Medal citation.

Enclosure (2)