



DEPARTMENT OF THE NAVY
FLEET AVIATION SPECIALIZED OPERATIONAL
TRAINING GROUP PACIFIC FLEET

P.O. BOX 357068
NAS NORTH ISLAND
SAN DIEGO, CALIFORNIA 92135-7068

FASOTRAGRUPACINST 55 S
N01F:

MAR 30 2001

FASOTRAGRUPACINST 5510.1S

Subj: COMMAND SECURITY PROGRAM FOR CLASSIFIED MATERIAL

Ref: a) SECNAVINST 5510.36
b) SECNAVINST 5510.30A
c) OPNAVINST 5239.1B
d) FASOTRAGRUPACINST 5239.1B

Encl: 1) Assignment of Individual Responsibilities and Duties
2) Security Container Information (SF700)
3) Activity Security Checklist (SF701)
4) Security Container Check Sheet (SF702)
5) Clearance Request/Authorization/Cancellation (FASO 5521/8)
(6) Clearance Eligibility Incident Report
7) Security Briefing Sheet (FASO 5511/3)
(8) Emergency Plan

1. Purpose. To publish procedures and instructions for the safekeeping, storage, dissemination, accountability and handling of classified material and set procedures for the granting of security clearances and access to classified material per policies in references (a), (b), (c) and (d).

2. Cancellation. FASOTRAGRUPACINST 5510.1R, FASOTRAGRUPACINST 5510.4, FASOTRAGRUPACINST 5510.2G, and FASOTRAGRUPACINST 5510.3G. This is a major revision and changes are not indicated. This instruction should be read in its entirety.

3. Applicability. This instruction is applicable to all military and civilian personnel assigned to FASOTRAGRUPAC.

4. Responsibilities. All personnel in the Department of the Navy (DON) are responsible for ensuring that classified material is protected and that only authorized personnel are granted

MAR 30 2001

access to classified material. Individual responsibilities and duties are outlined in enclosure (1).

Program Management

a. An officer qualified by reference (a) shall be designated in writing as the Command Security Manager (CSM). The CSM shall act as the advisor and direct representative of the Commanding Officer to assist in fulfilling the responsibilities for the security for classified material.

b. A qualified person in the aircrew training division (E-5/GS-6 or above) shall be designated in writing as the Command Classified Material Custodian (CCMC).

c. The CSM will inspect each FASOTRAGRUPAC department at least annually using exhibit 2c of reference (b) to ensure that procedures for the security of classified matter follow reference (a) and this instruction.

d. The CO shall assign, in writing, an officer or qualified civilian as Department Security Manager (DSM). A copy of the assignment shall be forwarded to the CSM and CCMC. Changes will be reported as they occur.

e. The CSM and Department Head (DH) will assign, in writing, a qualified person as Department Classified Material Custodian (DCMC). Duties of the DSM and DCMC may be assigned to the same person. An alternate DCMC will perform the duties listed in enclosure (1) in the absence of the regular custodian. Copies of the assignments shall be forwarded per paragraph 5d.

f. Detachment Officers in Charge shall appoint a Security Manager and locally administer their security program per this directive.

6 Receipt of Classified Material

a. All incoming Secret material will be delivered, seal unbroken, to the CCMC where it will be logged and custody cards prepared. After routing has been determined, addressees will be notified that the material is available for assumption of custody.

b. Secret material will be released only authorized DCMC or alternate custodians.

MAR 30 2001

c. Incoming Confidential and Secret messages will be released by Naval Computer and Telecommunications Detachment (NCTD) North Island to appropriately-cleared designated messengers who will ensure that they are properly protected as specified and delivered to the DCMC. Strict accountability of Secret messages will be maintained .

(1) All incoming Secret messages will be screened by the communication clerk or appropriate qualified individual, i.e. Security Manager or DH, to determine required routing.

(2) If the message requires routing, it must be logged by date-time group (DTG), originator, key words if desired and disposition (i.e., held by, destroyed).

d PERSONAL FOR Messages

(1) Messages will be delivered in an envelope or on disk to the CO. If the message is PRIORITY or above, the CO (only) will open the envelope and read the message. If action is required, the CO will either take action or contact the person to whom the message is addressed. In any case, the message will be delivered to the individual to whom the message is addressed on the first working day after receipt.

(2) Contents are considered sensitive. Access to the information contained in these messages will be strictly controlled and the message will be stored in an appropriate container at all times except when actually in use. Copies shall be limited to the minimum required and shall be made following the procedures in NWP-4.

7. Transmission. Transmission and packaging of classified material shall be performed per reference (a). Classified material will be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and address. The outer cover will be sealed and addressed with no indication of the classification of the contents. Classification markings must not be readable through the outer cover.

8. Custody, Storage and Accounting

a. All incoming mail will be handled in a manner that provides maximum protection in the event that it contains classified material. Screening points shall be established to ensure classified material is properly controlled and that

MAR 30 2001

access to the material is limited to cleared personnel with need-to-know.

b. The responsibility for security of classified material rests upon each person attached to this command regardless of how such information was obtained.

c. Individuals needing to hand-carry classified material within the command or from one command to another will comply with provisions specified in chapter 9 of reference (a). Transport via commercial aircraft should be used only when other methods will not meet operational objectives or contract requirements. Personnel authorized to carry classified material while in a travel status or aboard commercial aircraft must hold a courier authorization card, DD Form 2501, in addition to any other required documentation. Travelers will be cognizant of the requirements of chapter 9 of reference (a).

d. Classified material security containers found unlocked in the absence of assigned personnel shall be reported to the assigned custodian and Command Officer of the Deck (OOD) and guarded until the OOD arrives. Action shall be taken as prescribed in reference (a). The CSM will be advised as soon as possible of all known circumstances.

e. Classified documents removed from storage will be kept under constant surveillance and placed face down or covered when not in use. Document cover sheets, Standard Forms 704 and 705, may be used for covering Secret and Confidential documents, respectively. These cover sheets replace all existing cover sheets.

f. Any individual who becomes aware of classified material found adrift will notify their DH, who shall take possession of and store such material as required by the level of classification. If such storage is not possible, the material will be guarded until released to a responsible custodian. In all instances, an investigation will be conducted by the CSM who will make a full report to the CO and initiate action as required by reference (a).

g. Enclosure (2) will be maintained for each container, vault or secured room used for storage of classified material. Complete parts 1 and 2a per instructions on the form, ensuring the name and signature of the person making the change are entered in block 9. Attach part 1 to the inside of the security container. Place part 2A inside and file part 2 with the CSM.

MAR 30 2001

h. Combinations to all security containers will be changed whenever a person having knowledge of the combination is transferred, separated or no longer has the need-to-know, unless other sufficient controls exist to prevent access to the lock; or when the possibility exists that the combination has been compromised. Combinations will also be changed when first placed in use or taken out of service per reference (a).

i. Combinations will be considered to have the same classification as the highest classification of material stowed in the container. Combinations will be released only to those persons properly cleared and having a custodial responsibility. Certain combinations require two-person control.

j. Except by specific authority of the CO, classified material for which the command is responsible shall not be removed from the station. In the event removal is authorized, a complete list will be prepared by the individual removing the material and the list filed with the CSM.

9 Dissemination of Classified Material

a. To determine the limits of dissemination, full consideration will be given to the degree of classification and the need-to-know of individuals to whom specific information is to be disclosed. No person is entitled to have knowledge or possession of classified material solely by virtue of rank.

b. When classified material is discussed or disclosed by any means, the classification of the material concerned shall be brought to the attention of the recipient to prevent the information from being innocently passed along.

c. Standing distribution requirements for Secret and Confidential information and material such as distribution lists will be reviewed annually during the first week in October to verify the "need to know" of the recipients.

d. Department Heads may authorize reproduction of other classified material, in the minimum number of copies, observing any stated prohibitions. Such copies shall be classified, accounted for and safeguarded in the same manner as the original. Extracts shall be assigned a classification based on content and not necessarily that of the basic document.

MAR 30 2001

e. To the extent possible, manned classified reproduction facilities will be established where only designated personnel can reproduce classified materials. After normal duty hours, key controls will be instituted for reproduction facilities or equipment. Only dry copiers utilizing non-sensitive reproduction paper may be used for reproducing copies. Warning notices shall be posted on all reproduction equipment. If reproduction of classified material is authorized the notice will read: "THIS MACHINE MAY BE USED FOR REPRODUCTION OF MATERIAL UP TO SECRET. REPRODUCTION MUST BE APPROVED BY COMMAND SECURITY MANAGER." If reproduction of classified material is not authorized, the notice will read: "THIS MACHINE IS LIMITED TO REPRODUCTION OF UNCLASSIFIED MATERIAL."

f. Typewriter ribbons used in typing classified material shall be protected in the same manner as required for the highest level of classification for which they have been used. They must also be destroyed as classified waste. Exceptions are: After the upper and lower sections have been cycled through the machine five times in the course of regular typing, all fabric ribbons may be treated as unclassified regardless of their classified use thereafter. Any typewriter ribbon that remains substantially stationary in the typewriter until it has received at least five consecutive impressions may be treated as unclassified.

g. Only those individuals authorized in writing by the CO will be given access to classified material. Such authorization will be granted per reference (a).

10. Security in the Classroom

a. A security brief shall be conducted prior to beginning a course that contains classified information or material. At the beginning of each classified session, the instructor will indicate orally and in writing on a chalkboard/whiteboard the classification of the session.

b. Only bound notebooks will be used for classified notes. All pages must be numbered and marked with the correct classification as directed by reference (a). The outside of the notebook will be properly marked showing the highest classification contained in the notes. Downgrading instructions shall be placed on the outside front cover and on sections as appropriate. Notebooks will be issued at the beginning of each class period by the instructor, or by a class member assigned by the instructor. At the end of each class period, the student

MAR 3 0 2001

notebooks will be collected and properly stowed by the instructor.

c. Upon completion of a classified course of instruction, student notebooks will be retained for a minimum of 60 days, but not more than 180 days, and then destroyed per reference (a). Upon request by the student's parent command classified notebooks may be transferred by mail or hand-delivery prior to destruction following procedures outlined in reference (a).

11. Unauthorized Disclosure of Classified Material

a. Indiscrete personal letters and conversations, including careless talk in offices, public places and by telephone, constitute serious threats to security. Information disclosed to unauthorized persons may be repeated innocently and in ignorance of its importance until it becomes common knowledge. Foreign intelligence agents are scientifically trained to collect and correlate numerous bits of seemingly harmless information from conversation and rumors that circulate in the vicinity of Naval activities. Therefore, automatic censorship of official and unofficial conversation and letters is a fundamental duty of all personnel of this command.

b. The content of all conversation conducted via nonsecure administrative telephone systems are to be restricted to unclassified subject matters. No attempt to "talk around" classified subjects will be made. When answering telephones, the response will include the statement "...this is not a secure line."

c. There are certain classified subjects the very existence of which is classified. Such subjects shall not be mentioned unless conditions provide protection equal to the requirements for the classification assigned. The objective of these precautions is to prevent disclosure that the Navy Department is interested in or involved with such subjects. Subjects in this category are often assigned code words. Policies concerning procedures and use of code words may be found in chapter 6 of reference (a).

d. Situations may arise in which persons not authorized to have knowledge of certain classified information or equipment do, in the course of their duties, take notice of preparations or activities that are classified. In such cases, it is the duty of the custodian of the classified material to inform the unauthorized individuals that the material is classified and

MAR 30 2001

that their deductions or observations are not to be discussed. These persons are to be warned, but not supplied with additional information to supplement that already acquired.

e. Holders of classified material may release such information only after making certain that the person requesting the material is appropriately cleared and has a need-to-know. In case of doubt, consult the CSM.

f. Loss of classified information can be controlled by strict adherence to the doctrine of "security at the source." Official channels exist for the release of legitimate information to the public. Off-the-record interviews are prohibited. Such interviews are quite different from furnishing legitimate unclassified background information without an official statement.

g. Civilian and Naval personnel, including those released from Naval Service, shall not discuss, write or otherwise disclose classified information without official authorization. The unauthorized disclosure of such information makes the individual subject to legal action under provisions of the Espionage Act, Title 18, U.S. Code.

12. Security Checks

a. To ensure that the classified materia held by the department is properly protected at the close of each workday DHs will require that the DCMC make an inspection that will ensure that:

(1) All classified materia stored in the manner prescribed

(2) Burn bags are properly stored and/or destroyed

(3) Classified shorthand notes, carbon paper, rough drafts and similar papers have been properly stored and/or destroyed. As a matter of routine, such items shall be shredded.

b. Enclosure will be used to record the security checks

c. Enclosure (4) will be used to record opening, closing and end-of-day checks of each security container, vault and secure room.

MAR 30 2001

13. Retention of Classified Documents. Classified documents and materials that are not permanently valuable records of the government will not be retained more than five years from the date of origin, unless retention is authorized per the record disposition schedules of SECNAVINST 5215.5C. Department Heads will ensure an annual cleanout day is held during the first week of June. A portion of the work performed in each office will be devoted to the disposal or destruction of unneeded classified material.

14. Destruction of Classified Material

a. Destruction of classified documents shall be accomplished per reference (a) utilizing the mechanical paper shredders located at the document destruction facility, NASNI building 380, or the certified shredders located in the FASOTRAGRUPAC N32 vault.

b. The destruction of Secret material requires two persons cleared to the appropriate level to be involved in the entire destruction process, including transportation of burn bags. When burn bags are used, they will be sealed, serially numbered and a record kept of all subsequent handling to preclude unauthorized removal or removal of the contents prior to actual destruction. Burn bags containing Confidential material do not require serialization or records of handling.

c. All classified messages will be disposed of by shredding.

15. Automated Information System (AIS) Security References (c) and (d) promulgate the AIS security program formerly Automated Data Processing (ADP)).

Entry and Exit Inspection Program

a. Department Heads will conduct random inspections at a sufficient frequency during normal duty hours to deter and detect unauthorized introduction or removal of classified material. The method and frequency of inspections will be determined by the CO but should focus on areas where classified work is performed and on those persons employed within or visiting such areas. When practicable, inspections will be conducted after normal duty hours at all entry and exit points.

MAR 30 2001

b. Inspections of personal belongings will be limited to examination of briefcases, shoulder or handbags, luggage, athletic bags, packages or similar containers. Wallets, change purses, clothing, cosmetic cases or other objects of an unusually personal nature shall not be examined. Personnel who have a legitimate need to remove classified material for official purpose will be provided with written authorization utilizing the Standard Department of Defense (DOD) Courier Authorization Card (DOD Form 2501).

Personnel Security

a. Of equal importance with proper security of classified material is the issuance of personnel security clearances and access to classified material.

b. The Department of the Navy Central Adjudication Facility (DON CAF) is the sole authority for the granting, revocation and denial of both military and civilian final personnel security clearances. Interim clearance may be granted by the CO per reference (b).

c. Upon reporting on board, the DH/CSM shall make a determination as to whether or not an individual, either military or civilian, will require access to classified material. If access is required, enclosure (5) will be prepared in triplicate and two copies forwarded to the CSM. The CSM will screen military service records or civilian official personnel folders to determine if the person meets minimum qualifications for the level of clearance requested. If the clearance or investigation is not appropriate, the CSM will upgrade/downgrade or prepare the necessary investigation forms to meet command requirements. Non-U.S. citizens (immigrant aliens and foreign nationals, including non-immigrant aliens) are not eligible for a security clearance, which is clearly consistent with the interests of national security.

d. Final preparation of investigation forms will be accomplished by the CSM. The CSM is responsible for the accuracy of the information and to be aware of any potential security problems.

e. Procedures for civilian clearances. The Human Resources Office (HRO), as part of the hiring process, is responsible for verifying U.S. citizenship of all newly hired civilian employees. A National Agency Check with Written Inquiries (NACI) is required by the Office of Personnel Management (OPM)

MAR 30 2001

for civilian employees for Federal Government suitability determinations. Reference (a) provides guidance for the preparation and submission of standard investigative request forms to the U.S. Investigative Service (USIS) for personnel security investigations.

Security Clearance Reques

(1) When a civilian employee requires a security clearance the CSM will initiate a Clearance Request/ Authorization/Cancellation Form (CNRSW 5521/8), enclosure (5), and forward original to the Regional Security Management (RSM) office.

(2) The RSM will request the employee's official personnel file (OPF) from HRO to ensure that the file contains a record of a favorably completed investigation.

(3) An interim Secret or Confidential security clearance can be granted if there is a favorable review of investigative request questionnaire, the submission of an appropriate investigative request to USIS and a favorable review of local records.

4) Final security clearance will be granted by DON CAF when all investigative requirements have been met.

(5) The RSM will complete the Regional Security Management Authorization section of enclosure (5) and return to the CSM.

g. When DON CAF sends results of an adjudicative matter (i.e. results of a final clearance), the CSM will ensure the results are forwarded to HRO for inclusion in the employee's OPF.

h. If DON CAF intends to deny or revoke a clearance a Letter of Intent (LOI) will be sent to the command. The CO will withdraw any interim security clearances issued and associated access will be suspended. Procedures for unfavorable determinations and appeals are addressed in reference (b) paragraphs 7-7 and 7-8.

i. Military security clearance requests will be conducted per reference (b), chapters 6, 7, and 8.

MAR 30 2001

18. Eligibility for Clearance and Access. Evaluation of each person's eligibility for access to classified information or Service sensitive position, whether or not that person holds a security clearance, must be a continuous evaluation. Any individual who is aware of circumstances that indicate a Service member or civilian employee may no longer be eligible for access to classified information shall immediately notify the CSM via their department head and DSM.

a. Procedures for continuous evaluation of personnel

(1) The CSM has the responsibility to coordinate the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

(2) Reference (b) requires the CO to notify DON CAF via OPNAV 5510/413 of any significant incidents that may raise questions about an individual's eligibility, whether or not that person holds a security clearance. Such incidents include but are not limited to: events that may lead to non-judicial punishment, assignment to Level II program, indebtedness letters, civil infractions, desertions, incarceration as a result of a conviction on a criminal offense, award of a punitive discharge by a Court Martial, award of other than honorable discharge and arrest of any type, including driving under the influence (DUI). Incidents shall be reported as they occur, without waiting for final resolution. Follow-up reports will be submitted as required and upon final disposition.

(3) Enclosure (6) will be submitted to the CSM and department head. Enclosure (6) must be treated as "administrative sensitive" information and as such be enclosed in two opaque, sealed envelopes and addressed "FOR THE SECURITY MANAGER ONLY."

(4) Medical, Family Services and Counseling and Assistance Center personnel must be familiar with the continuous evaluation program as set forth in reference (a) and make use of enclosure (6) in a timely fashion. The first sign of any disqualifying behavior must be reported in addition to follow-up information as it develops.

(5) When derogatory or questionable information is received, the command will make a determination of the seriousness of the information and whether access will be temporarily suspended pending final adjudication by DON CAF

MAR 3 0 2001

b. The CSM has overall administrative responsibility or continuous evaluation of personnel access.

Security Orientation, Education and Training

a. DSMS will become familiar with the requirements of chapter 4 of reference (b) and ensure that all military and civilian personnel who have been granted access to classified material are regularly given instruction and training in safeguarding classified material. The following procedures apply:

(1) An orientation briefing, utilizing enclosure (7), shall be given to all personnel (military and civilian) as soon as possible after reporting to ensure that they are aware of the basic requirements for protection of classified information and the command's security procedures.

(2) A refresher briefing will be given annually to all personnel who have access to classified information. This briefing can be on general security practices or a special briefing emphasizing specific security areas as they apply to the command; i.e., visitor control, classification management communications security, etc. The CSM can assist DSMS as necessary.

(3) All personnel who have access to information classified Secret or above shall receive a Naval Investigative Service (NIS) counterespionage briefing at least once every two years. The NCIS Resident Agent (NISRA), Naval Station San Diego, telephone DSN 524-1514, provides the brief annually and upon request. This brief may be incorporated into, but shall not replace, the annual refresher brief required in subparagraph (2) above.

b. DSMS shall maintain appropriate records on completion briefings.

c. Division Training Petty Officers will ensure that all military personnel, whether or not granted access to classified material, are given continuing instruction in all phases of command security.

20. Compromises and Violations Of Security. Situations may occur in which classified material was subjected to compromise. These incidents are serious and may point toward problems in the

MAR 30 2001

command security program. Any person who is aware of the compromise of classified material, or of the apparent violation of security regulations, has the obligation to report that incident to proper authority as soon as possible. Failure to report a violation, actual or apparent, is as serious as the incident itself. Violations should be reported to the CSM via the department head.

a. Upon receipt of a report that a violation of security has occurred, a preliminary inquiry will be conducted per chapter 12 of reference (b), utilizing the format and information required in exhibits 12a and 12b of reference (b)

b. The preliminary inquiry shall be conducted and reported per articles 12-3 through 12-7 of reference (a).

21. Emergency Plan (EP). An emergency plan is included as enclosure (8). It is prepared per exhibit 2B-1 of reference

22. Debriefings. Department heads shall ensure that security debriefings are given to their personnel, including execution of Security Termination Statement (OPNAV Form 5511/14), under the following situations:

a. Prior to termination of active military service or civilian employment, or temporary separation for 60 days (including sabbaticals or leave without pay).

b. When the person's security clearance is revoked or cause.

c. When the person's security clearance is administratively withdrawn.

23. Forms and Reports

a FASOTRAGRUPAC Forms

(1) Clearance Request/Authorization/Cancellation Form (CNBSD-FASO-5521/g) and Security Briefing Sheet Form (CNBSD-FASO-15)-551/3) are included in this instruction as enclosure (5) and (7), respectively, and may be copied for use.

(2) Annual Inventory of Secret Material Form (CNBSD-FASO (11)-5511/10) is available upon request from the Administrative Officer (N1).

MAR 30 2001

(3) Certificate of Personnel Security Investigation, Clearance and Access (OPNAV 5520/20); Security Container Information (SF 700); Activity Security Checklist (SF 701); Security Container Check Sheet (SF 702); Classified Document Cover Sheets, Secret (SF 707) and Confidential (SF 708); Classified label (SF 709); Unclassified label (SF 710); and Classified Material Destruction Report (OPNAV 5511/14) may be obtained through the supply system.

b. Reports. The semiannual inventory of Secret material will be submitted to the Command Classified Material Custodian on 30 June and 31 December of each year.



F. M. GALLIE

Distribution:
FASOTRAGRUPACINST 5216.23A
Lists A and B

MAR 30 2001

ASSIGNMENT OF INDIVIDUAL
RESPONSIBILITIES AND DUTIES

1 Command Security Manager (CSM)

The Commanding Officer (CO) shall designate in writing a CSM, per chapter 2-2 of reference (b), who shall:

(1) Exercise overall supervision of the Information and Personnel Security program in compliance with references (a) and (b).

(2) Serve as the CO's advisor and direct representative in matters pertaining to the security of classified information and personnel security.

(3) Develop and promulgate written policies and procedures for the security of information and personnel security and ensure they comply with current directives.

(4) Review the command Emergency Plan to ensure compliance with current directives and their applicability to this command and the material held.

Supervise the security education program.

(6) Ensure that threats to security, compromise and other security violations are reported and, when necessary, investigated vigorously.

(7) Coordinate with the NCISRA on those incidents falling under NCIS jurisdiction

(8) Coordinate with the Public Affairs Officer to ensure that proposed press releases that might contain classified information are reviewed prior to release per reference (b).

(9) Supervise the classified material control program and ensure compliance with accounting and control requirements for classified material, including receipt, distribution, inventory and disposition.

(10) Approve requests to reproduce Secret and Confidential material.

(11) Coordinate physical security measures for the protection of classified material.

Enclosure

MAR 30 2001

(12) Ensure security is maintained during classified visits to and by the command.

(13) Ensure classified material is protected during unclassified visits to the command.

(14) Review recommendations/requests for release of classified information to foreign governments.

(15) Ensure compliance within Industrial Security program for classified contracts with DOD contractors.

(16) Ensure that all personnel handling information assigned to sensitive duties are properly cleared and granted access.

(17) Ensure that personnel security investigation requests are initiated when required, that the forms are properly prepared and submitted and that the investigations are properly monitored.

(18) Ensure that personnel security investigation results are disclosed only to personnel having a need-to-know

(19) Ensure that personnel authorized access to classified information are continuously evaluated concerning eligibility for continued access.

(20) Ensure that personnel security investigations, clearances and access are properly recorded.

(21) Coordinate reviews of the command's internal security programs, when necessary.

b. The Command Security Manager (CSM) may delegate the duties listed above to ensure proper performance of those duties. This delegation shall not relieve the CSM of the responsibility to ensure that personnel perform their duties per this instruction and directives from higher authority. When this directive conflicts with directives from higher authority those directives shall take precedence.

2. Department Security Managers. Designated by department heads, it shall be their responsibility to:

MAR 30 2001

a. Assure that the number of personnel authorized access to classified material is held to an absolute minimum.

b. Initiate requests for investigation and clearance of department personnel and ensure that:

(1) The immediate supervisor recommends individuals as being loyal, trustworthy, of excellent character and possessing the discretion and good judgment necessary for access to classified material.

(2) Any known or suspected derogatory information regarding the subject is forwarded with the request for investigation or clearance to CSM.

c. Assure that all persons who have access to classified material are appropriately cleared and instructed per applicable provisions of references (a) and (b).

d. Immediately notify the Security Officer of any derogatory information received concerning persons known to be under investigation for a security clearance or who have been authorized access to classified material.

e. Assure that an index of clearance requests and authorizations of all personnel within the department is maintained. Access to this index shall be limited to those persons having a need-to-know and shall be handled as "For Official Use Only."

f. Assure that information is provided, as required, to divisions and other activities regarding clearance status of personnel assigned.

g. Assure that the department copy of Form CNSB-FASO-15-5521/8 (Rev 4-94) is prepared and forwarded to the Security Officer to cancel access to classified material when personnel are separated, transferred, or no longer require access. The cancellation request will indicate the reason for the action, including date and ultimate duty station in case of transfers. Notify the CSM whenever an individual has a name change.

h. Semi-annually, forward a list of personnel holding security clearances to the CSM.

3. Command Classified Material Custodian. Designated by the CSM, responsibilities include:

Enclosure

MAR 30 2001

a. Receipt, accounting, distribution, control and destruction of all Secret and Confidential material received. Custodian shall perform the duties listed below:

(1) Receive all incoming registered and certified mail plus that marked "FIRST CLASS" and "POSTMASTER: DO NOT FORWARD-RETURN TO SENDER" and conduct the initial screening to ensure that all classified material is accounted for.

(2) Log in all Secret and Confidential material upon receipt. Entries to include: date received, registered/certified number, originator of the material, classification, subject, number of copies received and distribution codes/custody card prepared.

(3) Review incoming classified material for compliance with current directives concerning proper preparation and transmission; i.e., was the material wrapped in two opaque, sealed envelopes, was a receipt card enclosed with secret material, and CLASSIFIED BY and DECLASSIFIED ON information correct. When errors are noted, notify the originator of the material immediately using the Security Discrepancy Notice (OPNAV Form 5511/51).

(4) Screen outgoing classified material for compliance with chapter 9 of reference (b), specifically:

(a) Is the material properly marked with the highest classification of material within?

(b) Are all paragraphs and subparagraphs marked with their classification level?

(c) Is the classification authority and declassification date indicated in the proper place (normally in the lower left corner of the first page)?

(d) Is the letter of transmittal properly marked as to the level of classification of material covered and the level of classification of the transmittal itself?

e) Is the material properly addressed

f) Is the material properly signed out?

MAR 30 2001

b. Function as the Administrative Department's Security Manager.

NOTE: This list is not all-inclusive. Other items may be required to be checked, depending on the classification/warning notice(s) on the material.

4. Department Classified Material Custodian. Designated by Department Heads, it shall be their responsibility to:

a. Receive and sign custody receipt cards for all Secret material routed to their department.

b. Ensure proper storage and accountability for all classified material per reference (b).

c. Ensure that a continuous chain of receipts is maintained for Secret material.

d. Maintain current inventory lists of all Secret material retained within the department. Secret material shall be covered by a receipt between commands and other authorized addressees.

e. Conduct an annual sight inventory of all Secret material held and report results to the Command Classified Material Custodian on 30 June and 31 December.

f. Upon being relieved, conduct an inventory in the presence of their relief and report in person to the Command Classified Material Custodian to be officially relieved. The newly designated custodian will then sign the custody receipt cards for all Secret material inventories charged to the department.

MAR 30 2001

SF 700 (8-85)
Prescribed by
GSA/ISOO
32 CFR 2003

2A USER IN ENVELOPE

WARNING
COPY OF PARTS OF THIS CONTAINER
SHOULD NOT BE RELEASED
UNLESS AUTHORIZED BY THE
APPROPRIATE AGENCY

COMBINATION

one to the (flap) (1-11)
one to the (flap) (1-11)
one to the (flap) (1-11)
one to the (flap) (1-11)

DETACH

WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

WARNING

SECURITY CONTAINER INFORMATION INSTRUCTIONS		1. AREA OR POST (if required)	2. BUILDING (if required)	3. ROOM NO.
1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).		4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.		6. MFG. & TYPE CONTAINER	7. MFG. & TYPE LOCK	8. DATE COMBINATION CHANGED
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.		9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		
4. DETACH PART 2A AND INSERT IN ENVELOPE		10. Immediately notify one of the following persons, if this container is found open and unattended		
5. SEE PRIVACY ACT STATEMENT ON REVERSE.		EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

1. ATTACH TO INSIDE OF CONTAINER 700-101 NSN 7540-01-214-5372 STANDARD FORM 700 (8-85) Prescribed by GSA/ISOO 32 CFR 2003

CLEARANCE-REQUEST/AUTHORIZATION/CANCELLATION

FASOTRAGRUPACINST 5510.1S

FASOTRAGRUPAC 5521.8 (10) (APR 84)

MAR 30 2001

NAME: (Last, First, Middle)		FILE, SERVICE OR PAY NUMBER:	RANK, RATE, OR TITLE:
DATE OF BIRTH:	PLACE OF BIRTH:		
FROM:	TO: COMMANDING OFFICER (CODE 15)	DATE:	

As the records of this department disclose no disqualifying information, it is requested that subject be investigated and authorized access to classified matter as indicated:

TOP SECRET
 SECRET
 CONFIDENTIAL
 OTHER

SIGNATURE: (Department)

AUTHORIZATION TO BE FILLED IN BY SECURITY DEPARTMENT

FROM:	TO:	EFFECTIVE DATE:
COMMANDING OFFICER		
SUBJECT HAS BEEN INVESTIGATED AND IS AUTHORIZED ACCESS TO:	<input type="checkbox"/> INTERIM <input type="checkbox"/> FINAL	NDA EXECUTED:
TYPE OF INVESTIGATION:	DATE COMPLETED:	SIGNATURE:
BY DIRECTION		

CANCELLATION

RELEASED FROM ACTIVE DUTY
 DISCHARGED
 TRANSFERED TO:

ADMINISTRATIVELY WITHDRAWN
 RESIGNED
EFFECTIVE DATE

BY TO: _____ SIGNATURE: _____

MAR 30 2001

CLEARANCE ELIGIBILITY INCIDENT REPORT

From: _____
To: Security Manager (N01F)

INCIDENT REPORT ICO _____

a) SECNAVINST 5510.30A

1. Evaluation of each person's eligibility for access to classified material is continuous, per reference (a). Accordingly, this report contains information regarding subject's security clearance eligibility.

Information category

- | | |
|---|---|
| <input type="checkbox"/> Alcohol Abuse | <input type="checkbox"/> Disloyalty to U.S. |
| <input type="checkbox"/> Drug Abuse | <input type="checkbox"/> Foreign Associations |
| <input type="checkbox"/> Financial Problems | <input type="checkbox"/> Security Violations |
| <input type="checkbox"/> Emotional/Mental Problems | <input type="checkbox"/> NJP/Court Martial |
| <input type="checkbox"/> Criminal Acts/Local Civilian Involvement | <input type="checkbox"/> Sexual Misconduct |
| <input type="checkbox"/> Desertion | <input type="checkbox"/> Falsification of Information |
| <input type="checkbox"/> Other | |

Explanation of item(s) checked

Source of information: _____

Action taken: _____

Signature/Rank/Rate/Grade

Enclosure (6)

MAR 30 2001

ASOTRAGRUPAC 0)-55 3(4-94

SECURITY BRIEFING SHEET

1. This briefing is to advise you of your responsibilities for safeguarding classified information to which you may have access during your assignment/employment at this activity. You have a direct responsibility for compliance with various security regulations that dictate the measures used to guard against the possibility of classified information falling into unauthorized hands.

2. The following represents some of the important aspects of your security responsibilities:

a. Do Not Discuss Classified Information with Unauthorized Personnel. Before discussing any information, determine and know the classification of such information; discuss it only with those who officially have a need to know and are cleared to receive it. Friends, dependents and uncleared persons are not authorized to receive classified information. Discussion of classified information over the telephone is prohibited. You cannot talk around classified information by trying to be hypothetical. If it is classified, **DO NOT DISCUSS IT ON THE PHONE.** News releases concerning Naval Air Station, North Island or the mission of Naval Air Station, North Island and tenants may contain information requiring official concurrence. Do not make such stories official by commenting on their accuracy. They will be referred to the Public Affairs Officer.

b. Report All Infractions of Security Regulations. Whenever an infraction of classified document security regulations comes to your attention, it is your duty and responsibility to report it to your supervisor.

c. Safeguard Classified Documents and Material Entrusted to Your Care. Whenever classified documents or other material come into your possession, you are responsible for properly safeguarding them against improper handling and loss or unauthorized dissemination. There are physical safeguards provided to properly secure classified matter. If they are not used as directed, loss and compromise may result. Personnel will be held responsible, within their own areas of accountability, for compliance with applicable regulations pertaining to handling, transmission and storage of classified material.

Enclosure

MAR 30 2001

d Be Security Conscious. Most of the security violations that occur are due to carelessness, lack of knowledge or regulations, indifference, lack of security consciousness, and ignorance of the penalties for security violations. A successful security management program is dependent upon how well and how fully each individual discharges their responsibilities. Effective security within this activity can be maintained only if each and every member understands and complies with security requirements and regulations.

3. All personnel of the Department of Defense, military and civilian, are responsible for complying with security regulations. Violations by military personnel may be referred for either judicial or non-judicial action. Violations by civilian personnel may be punishable under the provisions of Office of Personnel Management instructions.

I certify that I have read and thoroughly understand the contents of this document.

_____ Date

I certify that I have thoroughly explained the contents of this document to the person whose signature, which I have witnessed, appears above.

_____ Date

MAR 30 2001

EMERGENCY PLAN

1. Purpose. To provide practical means for accomplishing protection and/or removal of classified material in case of enemy action, natural disaster or civil disturbance.

2. Discussion. Proper security measures prevent unauthorized access to classified information. This plan provides guidance and specifies the removal or emergency protection of such material during natural or operational emergency. Personnel safety is always of paramount concern. All actions are to be taken without unnecessarily endangering the health or safety of personnel.

a. The following courses of action may be taken to protect classified material from unauthorized viewing:

(1) Emergency Protection. Includes actions such as increasing the guard force, securing storage areas normally kept open during normal work hours, placing all classified documents and materials in security containers, locking the containers and securing power and ventilation to the areas. This may be taken to include the evacuation of personnel for safety considerations with the material remaining on site in a secured fashion. All material will be stowed in GSA-approved security containers.

(2) Emergency Removal. Includes removing classified material in a systematic manner and making every effort to prevent viewing of the material by unauthorized persons. Removed materials must be placed under guard in an area where physical security can be maintained.

b. Priorities for emergency removal will be based on potential damage to national security should the material into unauthorized hands. Priorities are as follows.

Priority one: SECRET

(2) Priority two: CONFIDENTIAL

c. Activation of the emergency plan will be at direction of the Commanding Officer or a designated representative.

d. Protection or removal will be accomplished in such a manner, as determined by the department heads, so that priority one material handling will be accomplished first.

MAR 30 2001

e. An inventory of classified material shall be maintained and kept in the front of the top drawer of each security container.

Action

a. Emergency Protection. When notified of a situation requiring emergency protection during working hours the classified material custodian or, if not available, the alternate custodian will immediately ensure that any classified material in use is placed in a security container and that the container is locked. Upon completion, report to the Officer of the Day (OOD) that the required action has been taken. Outside of normal work hours, all offices will be checked by the OOD to ensure that no classified material has been left out.

b. Emergency Removal

(1) The most common scenario involving emergency removal would be a natural disaster such as earthquake, fire or flood. If time and conditions permit, all classified material will be systematically removed by the classified material custodian or, if not available, the alternate custodian. Assistance will be provided by other departments if required. If removal is not possible, the area will be kept under surveillance by the station security force to prevent unauthorized access.

(2) Any attempt at removal must be made without interfering with efforts to control the emergency situation

(3) Classified material will be evacuated to building 335 and secured. If building 335 is not available, material will be taken to the base security department and put under guard. Material will be accounted for by checking against the inventory list. Results of the inventory will be reported to the OOD.

(4) All classified material shall be inventoried as soon as possible after the emergency to determine accountability and to report any compromises. The results of the inventory shall be reported to the CSM.

c. Emergency Plan Drills. The Department Security Manager will conduct drills during June and December. These may be held in conjunction with fire drills. Results will be reported to the CSM with recommendations for improvement.

MAR 3 0 2001

d. Departmental responsibilities. Each DH will ensure that the following requirements are met in their departments:

(1) A number shall be placed on the exterior of each security container indicating priority for destruction

(2) A listing of classified material by type (documents, equipment, etc.), location and priorities for destruction.