DEPARTMENT OF THE NAVY
U.S. NAVAL SUPPORT ACTIVITY
PSC 817, BOX 1
FPO AE 09622-1000

NAVSUPPACT NAPLES INST 5511.2J
N1A:rr
30 MAY 2003

NAVSUPPACT NAPLES INST 5511.2J

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

Subj: INFORMATION AND PERSONNEL SECURITY REGULATIONS

Ref: (a) SECNAVINST 5510.36
(b) SECNAVINST 5510.30A
(c) SECNAVINST 5239.3
(d) SECNAVINST 5510.27
(e) NAVSUPPACT NAPLES INST 5511.6B
(f) SECNAVINST 5510.13B
(g) OPNAVINST C5510.101
(h) SECNAVINST 5212.5D

Encl: (1) Classified Material Control Organization
(2) Application for Security Information Access
(3) Stowage of Classified Material
(4) Receipt and Routing of Classified Material
(5) Destruction of Classified Material
(6) Classified Information Nondisclosure Agreement (SF 312)
(7) Personnel Security Action Request (OPNAV Form 5510/413)
(8) Security Container Information (SF 700)
(9) Correspondence/Material Control Report (OPNAV Form 5216/10)
(10) Record of Receipt (OPNAV Form 5511/10)
(11) Classified Material Destruction Report (OPNAV Form 5511/12)

1. Purpose. To establish policy and procedures for compliance with and implementation of references (a) through (h) and to ensure that classified material in the custody of U.S. Naval Support Activity (NAVSUPPACT), Naples, Italy, receives proper handling and security protection. This instruction applies to all departments of NAVSUPPACT Naples. Each individual, military or civilian, in or employed by NAVSUPPACT Naples, is responsible for compliance with this instruction. This instruction is a complete revision and should be read in its entirety.

2. Cancellation. NAVSUPPACT NAPLES INST 5511.2H.

3. Background. Security of the naval establishment depends upon the success attained in the safeguarding of classified material. The security of classified material within the naval establishment is a command responsibility. Rules governing security procedures do not guarantee protection against every conceivable situation. The goal sought by this instruction is a satisfactory degree of security with a minimum sacrifice of operating efficiency.

4. Policy. This instruction provides specific command guidance regarding information and personnel security regulations. It is not intended to replace or deviate from policies set forth in:

a. Department of the Navy (DON) Information Security Program Regulation (reference (a));

b. DON Personnel Security Program Regulation (reference (b));

c. DON Information Systems Security Program (reference (c));

d. Disclosure of Classified Military Information to NATO Nations (reference (d));

e. NAVSUPPACT Naples Emergency Destruction Plan (reference (e));

f. Security Education and Training (reference (f));

g. NATO Security Procedures (reference (g));

h. Navy and Marine Corps Records Disposition Manual (reference h)).

5. Responsibilities. It is the responsibility of all hands to know the standard procedures associated with the safeguarding of classified material, as specified in references (a) through (h) and this instruction.

D J Frederick

D. J. FREDERICK

Distribution:
NAVSUPPACT NAPLES INST 5216.4W
Lists: I; II

Copy to:
List: IV (1 and 2 only)

LIST OF COMMONLY USED ABBREVIATIONS/ACRONYMS

ADP	Automated Data Processing
CMS	Communications Security Material System
CMSC	Classified Material Security Clerk
CMCP	Classified Material Control Program
COMSEC	Communications Security
DON	Department of the Navy
DON CAF	Department of the Navy, Central Adjudication Facility
EDP	Emergency Destruction Plan
ENTNAC	Entrance National Agency Check
FGI	Foreign Government Information
ISSM	Information Systems Security Manager
LAA	Limited Access Authorization
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NCIS	Naval Criminal Investigative Service
NOFORN	Not Releasable to Foreign Nationals
OCA	Original Classification Authority
OPM	Office of Personnel Management
PR	Periodic Reinvestigation
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SECMGR	Security Manager
SSBI	Single Scope Background Investigation
TSCO	Top Secret Control Officer

CLASSIFIED MATERIAL CONTROL ORGANIZATION

1. Program Management

a. Security Manager (SECMGR). The SECMGR (Officer/GS-11 or above) will be designated in writing by the Commanding Officer. The SECMGR will assist the Commanding Officer in fulfilling his/her responsibilities for personnel security investigations and the security of classified information/material assigned to the command. The SECMGR will also supervise the overall command Classified Material Control Program (CMCP) to ensure compliance with references (a) and (b).

b. Assistant SECMGR. The Assistant SECMGR (E6/GS-6 or above) will be designated in writing by the Commanding Officer. The Assistant SECMGR will assist the SECMGR in fulfilling his/her responsibilities for personnel security investigations and the security of classified information/material.

c. Top Secret Control Officer (TSCO). The Commanding Officer will designate, in writing, an officer, chief petty officer, or DoD civilian (GS-7 or above) who has final Top Secret clearance as TSCO, under the direction of the SECMGR. The activities of the TSCO will include receipt, custody, accounting, and distribution of Top Secret information within NAVSUPPACT Naples and its transmission outside of the command as per guidelines set forth in reference (a).

d. Classified Material Security Clerk (CMSC). The Commanding Officer, through the SECMGR, may designate departmental CMSCs. These clerks will assist the SECMGR and Assistant SECMGR in the normal day-to-day administration of the command classified material control per this instruction, reference (a), and all other pertinent directives for the safeguarding of classified matter and good security practices. Per reference (e), CMSCs are also designated as the Departmental Primary or Alternate Emergency Destruction Plan (EDP) Representatives. As such, neither the primary nor the secondary CMSC will be assigned duties as a First Responder to the disaster preparedness CBR team. Additionally, if either one is assigned temporary duty to the Auxiliary Security Force, a new departmental CMSC must be identified to cover for the temporary additional duty period.

e. Automated Data Processing (ADP) Security Officer/ Information Systems Security Manager (ISSM). The Commanding Officer will designate, in writing, an ADP Security Officer/ISSM who will be responsible for the protection of classified information being processed in any of the command's automated information systems. The ADP Security Officer/ISSM will be thoroughly familiar with references (a) through (c) and will prepare a command ADP Security Plan.

2. Security Education Program. The purpose of a security education program is to ensure all personnel understand the need to protect and safeguard classified information. The goal, as stated in reference (a), is "to develop fundamental habits of security to the point that proper discretion is automatically exercised in the discharge of duties and security of classified information becomes a natural element of every task." Reference (f) outlines specific education and training requirements to ensure a uniform interpretation and application of security standards. Security education is applicable to all personnel entrusted with the protection of classified material, regardless of position, rank, or grade. The SECMGR will ensure all command personnel having access to classified material/information are provided with quarterly training using guidelines set forth in reference (f). The following matrix outlines minimum briefing/ training requirements:

BRIEFING	NEWLY REPORTING PERSONNEL	PERSONNEL WITH CONFIDENTIAL	PERSONNEL SECRET AND ABOVE	PERSONNEL WITHOUT CLEARANCES
Indoctrination	X			
Orientation		X	X	O
On-the-Job		X	X	
Annual Refresher		X	X	O
Counterintelligence		O	X	O
Special Briefing		X	X	O
Debriefings		X	X	
Legend: X = REQUIRED		O = OPTIONAL		

3. Classified Material Access/Brief. All personnel who require access to classified information are required by reference (a) to receive a Security Orientation Briefing prior to receiving access to classified material. The Security Orientation Briefing will be conducted by the departmental CMSC and will, as a minimum, cover the following topics:

- Command security structure;

- Special security precautions;

- Proper handling/transport of classified material;

- Classified information control procedures;

- Reporting information that could impact security clearance eligibility;

- Reporting suspected security violations;

- Processing classified information on command information (computer) systems.

a. After the brief, the CMSC will have the member read and sign the Classified Information Nondisclosure Agreement (SF 312) (enclosure (6)). The departmental CMSC will retain a copy of SF 312, place a copy in the member's service record, and deliver the original to the SECMGR. For civilian personnel a copy will be provided to the Human Resource Office for filing in the personnel record, and the original will be delivered to the SECMGR.

b. Supervisors must ensure that subordinates know the security requirements impacting the performance of their duties. On-the-job training must be conducted to ensure that specific security procedures unique to the duties are learned.

c. Reference (a) requires that all personnel with access to classified information receive an annual refresher briefing. Supervisors will ensure personnel attend one of the periodic briefings scheduled by the SECMGR at least once a year.

d. A counterespionage briefing by the Naval Criminal Investigative Service (NCIS) must be given once every two years to those personnel who have access to material classified Secret or higher. The SECMGR will ensure that this training is presented on a recurring basis.

e. Foreign travel briefings will be requested as necessary from the SECMGR, per reference (a), and performed by the Physical Security/Force Protection Officer. Debriefings will be

performed after the travel. It is the traveler's responsibility to ensure this requirement is met before traveling to any country listed in Chapter 6 of reference (a).

4. Personnel Security Clearances. Policy and guidelines issued in reference (b) concerning Single Scope Background Investigations (SSBIs) and National Agency Checks (NACs) required for clearances will be strictly adhered to for both military and civilian personnel. A vital element of a command CMCP is ensuring that personnel having access to classified information possess the proper security clearance. Each NAVSUPPACT Naples department will determine which individuals under its control are to be entrusted with access to classified material. Each decision to grant access is based strictly on the "need to know" and the existence of documentation testifying to an individual's trustworthiness.

a. All personnel security clearances will be granted by the Department of the Navy, Central Adjudication Facility (DON CAF). Clearances will be requested in accordance with reference (a) from DON CAF on OPNAV Form 5510/413 (enclosure (7)). DON CAF will make a security clearance determination and forward the results to NAVSUPPACT Naples via message or letter.

b. The Commanding Officer will have full authority to grant, withdraw, lower, or suspend security access. DON CAF will have the sole authority to grant, deny, revoke, or suspend security clearances.

c. Whenever an individual assigned to NAVSUPPACT Naples is employed in a position requiring a security clearance/access, that individual's department head will immediately initiate an Application for Security Information Access (enclosure (2)) and forward it to the SECMGR. For civilian personnel, forward to SECMGR via the HRO. Certification by the department head that the individual has a "need to know" for the level of access requested is mandatory. The HRO Director or designated representative will ensure the position descriptions of civilian employees are appropriately annotated and a copy of the cover sheet, Optional Form 8, is attached to the original of Form 5520/1.

d. Upon receipt of enclosure (2) from the requesting official, the departmental CMSC will review individual records for appropriate source documents or other evidence of a successfully completed investigation. The CMSC will also review any available medical or financial records for any questionable information that would require further study/review prior to requesting security access. In the case of civilian personnel, the HRO will assist the CMSC in obtaining the information requested in enclosure (2) prior to forwarding the request to the SECMGR.

e. Upon ascertaining that the military member/civilian employee is eligible for clearance/access requested, if DON CAF adjudication message cannot be found in member's service/ personnel record, the departmental CMSC will complete OPNAV Form 5510/413 (enclosure (7)) and forward to the SECMGR along with enclosure (2) for review and signature. SECMGR will then send enclosure (7) via fax or message to DON CAF for clearance adjudication. Upon receipt of clearance adjudication from DON CAF, the SECMGR will record the final clearance authorization on the Command Security Access List at a level no higher than the level specified by DON CAF. A copy of the DON CAF message must be maintained in each member's local service/personnel record. For military members, a copy will be forwarded to Commander, Navy Personnel Command (PERS-313C1), and for civilian personnel, HRO will forward a copy to the Office of Civilian Personnel Management (OCPM).

f. In the event a source document is not available on which to base a clearance, the CMSC (for military personnel) or HRO (civilian personnel) will notify the SECMGR to initiate the necessary investigation based on access level required. An interim Secret clearance may be granted for up to 180 days based upon a favorable review of DD Form 398-2 or SF-86 and submission of a NAC or NACI request, as appropriate. An interim Top Secret clearance may be granted for up to 180 days based upon a favorable ENTNAC, NAC, or NACI, provided a SSBI is requested and other conditions for interim clearance have been met.

g. When transferring from NAVSUPPACT Naples or retiring/ separating from naval service, both military and civilian personnel will report to the NAVSUPPACT Naples SECMGR/Assistant SECMGR for a security debrief.

5. Continuous Evaluation of Eligibility. Personnel security responsibilities do not stop once a favorable personnel security determination is made. Evaluation of each person's eligibility for access to classified information or service in a sensitive military/civilian position is continuous.

a. Information that could place an individual's loyalty, reliability, and trustworthiness in question, has to be evaluated from a security perspective. Department heads, division officers, and supervisors must be familiar with the adjudication policy in appendixes F and G of reference (b) and be alerted that behavior indicating unexplained affluence, financial instability, or criminal conduct is potentially significant to an individual's security status. They must act at once to notify the SECMGR in the event any derogatory or questionable behavior should arise, at any time, which might impact an individual's ability to retain access to classified material. Department heads and supervisors are also advised to consult with their HRO labor relations specialist should the situation involve a civilian employee.

b. The Commanding Officer will adjudicate the information using the guidelines in reference (b), appendixes F and G, based upon consideration and assessment of all available information, both favorable and unfavorable, with particular emphasis being placed on the nature, seriousness, date, and frequency of and motivation for the individual's conduct; the extent to which conduct was negligent, willful, voluntary, or undertaken with knowledge of the circumstances or consequences involved; and to the extent it can be estimated, the probability that conduct will or will not continue in the future. In all adjudications, the protection of national security will be the paramount determination. If warranted, the Commanding Officer will suspend access and advise DON CAF.

c. Supervisors will comment on eligibility of personnel for continued access to classified information and discharge of security responsibilities in conjunction with regularly scheduled performance appraisals of military and civilian personnel whose duties entail access to classified information.

6. Periodic Reinvestigation (PR). A PR is a reinvestigation initiated by the member through the SECMGR and conducted by the Defense Security Service and/or OPM to update a previous valid investigation to evaluate continued access eligibility. The following PR schedule applies:

a. SSBI PR. Conducted as directed by DON CAF and every five years for individuals in NATO billets (when TS COSMIC clearance is required), SCI, Nuclear Weapon Personnel Reliability Program critical positions, Single Integrated Operational Plan - Extremely Sensitive Information, civilians in critical-sensitive and special-sensitive positions, LAA, White House and some Special Access Programs (SAP).

b. SECRET PR (SPR). Conducted on personnel with Secret clearance or access at 10 year intervals (SAPs with Secret access and Explosive Ordnance Disposal duties require five-year intervals).

7. Compromise and Other Security Violations. There are two types of security violations: (1) those that result in a confirmed compromise or possible compromise of classified information and (2) those that do not result in such a confirmed or possible compromise but in which a security regulation has been violated.

a. Compromise is the disclosure of classified information to a person who does not have authorized access, a valid clearance, or a need-to-know. Compromise obviously presents the greater threat to national security, but other security violations must also be treated seriously because they demonstrate that a weakness exists in the command's CMCP. For this reason, security violations of either type must be reported and vigorously investigated and the problems causing the violation corrected rather than covered up.

b. Any individual who becomes aware of the loss, possible compromise, or compromise of classified information or material will immediately notify the SECMGR or Commanding Officer, who will notify NCIS when a preliminary inquiry is initiated. Timely referral is imperative to ensure preservation of evidence. The overriding priority is to regain custody of the information, if possible, and give it proper protection.

U.S. NAVAL SUPPORT ACTIVITY, NAPLES, ITALY

APPLICATION FOR SECURITY INFORMATION ACCESS NAVEUR NAVSUPPACT NAPLES 5510/2 (New 5-02)

NAME (LAST, FIRST, MIDDLE)	*SSN*	*GRADE/RANK*	*COMMAND/UIC/DEPARTMENT*

DATE AND PLACE OF BIRTH	*LEVEL OF ACCESS REQUIRED*	*U. S. CITIZEN*
		YES / NO (circle one)

TYPE OF INVESTIGATION	*DATE INVESTIGATION COMPLETED OR MAILED*	*AGENCY COMPLETED BY*	*PERIODIC REINVESTIGATION COMPLETED ON*

ABOVE INVESTIGATION DATA DERIVED FROM: _____ (Example: EDVR/SVCRCD/ETC.)

DOCUMENTS VERIFIED FOR DEROGATORY INFORMATION (Initial as applicable):

SERVICE/PERSONNEL RECORD _____
MEDICAL RECORD _____
FINANCIAL RECORDS _____
BASE SECURITY _____
SJA (Command Legal) _____
OTHER (Provide source) _____

REQUEST FOR CLEARANCE AND ACCESS: I hereby certify that the above listed individual has a "Need-to-Know" and requires access to classified material in the performance of his/her duties. SF-312 has been completed and the original is provided as an attachment to this form.

Name and Rank/Rate of Department Head _____ Signature of Department Head _____ Date _____

(If civilian, route through Human Resources Office)

From: Human Resources Office, NAVSUPPACT Naples
To: Security Manager, NAVSUPPACT Naples

1. Member's position description outlines requirement for access to classified information. YES / NO (circle one)
2. The above listed security investigation data on member is **correct / not correct**. (circle one)
3. Comments (if any): _____

Print name of HRO Representative _____ Signature _____ Date _____

From: Security Manager, U.S. Naval Support Activity, Naples, Italy
To: Department Head, _____ (List Department)

1. The above listed member **has / has not** (circle one) been granted _____ access.
2. Comments (If applicable, discuss issue as to why access was not granted): _____
3. OPNAV Form 5510/413 was mailed on _____ to DON CAF for adjudication. Member is granted interim access until final adjudication is received from DON CAF. Interim access expires on _____.

Signature of Security Manager or Assistant Security Manager _____ Date _____

Copy to: NSA ADMIN SECURITY ACCESS FILES
PERSONNEL RECORDS, HRO (CIVILIANS ONLY)

ENCLOSURE (2)

STOWAGE OF CLASSIFIED MATERIAL

1. General. All classified material will be afforded physical security per Chapter 10 of reference (a) or reference (g) for NATO material. As a general guideline, all classified matter held by NAVSUPPACT Naples and not in actual use by appropriately cleared personnel or under their direct personal observation will be stowed in General Services Administration (GSA)-approved safes equipped with combination locks meeting Federal Specification FF-L-2740 (Mas-Hamiliton XO-7). The combination to a security container will be changed when any person having knowledge of it transfers from the command or no longer requires access, when there is reason to believe the combination has been compromised, or in any case every 12 months (every six months for NATO material). Any paper showing the combination to a safe will bear the same classification as the most highly classified material inside the safe. In selecting combination numbers, multiples of five, simple ascending or descending arithmetical series, and personal data, such as birth dates, must be avoided. The same combination will not be used for more than one container in any one space. Money, jewelry, narcotics, weapons, etc., will not be stowed in containers used for stowage of classified material. DO NOT place number/symbol on exterior of container to indicate priority in the event of emergency destruction (never show level of classification stored).

2. Records of Safe Combinations. Combinations to safes containing classified material will be placed in a sealed Security Container Information envelope, SF 700, (enclosure (8)) and filed as outlined below. The envelope must bear the same classification as the most highly classified material within the safe. It should be emphasized that these provisions, as well as all others in this instruction, apply only to safes used for the stowage of classified material.

a. Classified material safes assigned to departments and individuals of NAVSUPPACT Naples (except those containing Top Secret material). Enclosure (8) containing the combinations to these safes will be placed in the custody of the SECMGR. Envelopes should indicate plainly the number of the safe, its location, persons having access, and the classification of material contained therein.

b. Safes containing Top Secret material. Enclosure (8) containing combinations to safes storing Top Secret material will be stored in the Joint Operation Control Center (JOCC), CTF-67, located in Building 401 (C4I), Capodichino. The CMSC will notify the SECMGR and the TSCO prior to delivery of enclosure (8) to the JOCC CTF-67.

RECEIPT AND ROUTING OF CLASSIFIED MATERIAL

1. Instruction for Receipt, Internal Dissemination, and Transmission of Secret and Below Material

a. General. Department heads and special assistants are responsible for ensuring that their personnel have clearance/ access commensurate with the duties assigned and the "need to know" to perform those duties.

(1) No foreign national, regardless of clearance, is allowed access to material bearing a "NOFORN" caveat.

(2) All classified material (i.e., typing ribbons, diskettes, etc.) must be attended to at all times by an appropriately cleared person and properly stored and/or disposed of per reference (a).

b. Receipt. All classified material addressed to this command will be received initially by the SECMGR or his/her representative who will execute the registered mail receipts, custody receipts, and other documents necessary to acknowledge receipt of the material by NAVSUPPACT Naples.

c. Classified material will not be routed through guard mail. It must be hand-carried/delivered by personnel cleared for access to the highest classified level being carried and person must have a valid courier card. Classified material must be double wrapped with the inner wrapping marked with the classification of the material and the outer wrapping bearing no indication of the classification of the material. A locked briefcase may serve as the outer wrapper, **except** aboard commercial aircraft. Within departmental use and routing, a classified information cover sheet (SF703 for Top Secret, SF704 for Secret and SF705 for Confidential) must be used when hand-carrying.

d. Internal Dissemination and Filing of Classified Material

(1) Operation Plans and Orders, Instructions, Tactical Warfare Publications, and Other Documents. Upon initial receipt, all such documents will be routed on a need-to-know basis to departments having cognizance over the material contained therein. OPNAV Form 5216/10 (enclosure (9)) will be used. Classified material will be personally hand-carried back

to the SECMGR, initialed and filed. Any individual choosing to retain a Secret document after initial routing may do so by signing a custody receipt from the SECMGR. Otherwise, the document will be returned to the SECMGR for storage. Confidential material need not be signed for. The Administration Department CMSC will indicate control on the copy of the route slip held by the SECMGR. All classified material will be hand-carried by personnel cleared to the classification level of the material they are transporting.

(2) Changes to Operation Plans and Orders, Instruction, Tactical Warfare Publication, and Other Documents Classified Secret. Changes to publications will be routed only to the individual in whose custody the basic document is held. The individual receiving the change will sign for it on the route slip at the time the document is received from the Classified Files Center. After incorporating the change, the residue will be hand-carried to the Classified Files Center for destruction.

(3) Letters and Other Correspondence

(a) Letters and other correspondence will be routed initially for information or action on a need-to-know basis to departments having cognizance.

(b) The SECMGR will maintain a duplicate copy of all route slips while the document is in routing so that a control record of the document is maintained. When the original route slip is returned, the duplicate will be destroyed.

(c) If any department or individual chooses to retain the correspondence for information or for use in preparing a reply, they will so indicate on the route slip, sign the original slip to indicate custody of the document, and return the route slip to the SECMGR.

(d) Upon completion of routing, the SECMGR will retain all needed incoming classified correspondence and the route slip which accompanied it or, if the correspondence was retained by an individual, only the route slip. A serial file containing copies of all classified outgoing correspondence will be maintained separately.

(4) Messages

(a) Confidential Messages. The security advantages gained by centrally controlling individual copies of Confidential messages would not be commensurate with the administrative effort expended due to the large volume of such messages received and because these messages will be distributed to various departments without requiring receipt signatures. These copies may be used, filed, or destroyed by individual departments with no further report to the SECMGR. However, individual departments must ensure that all confidential messages are stowed, handled, and destroyed in strict accordance with reference (a). While centralized control is impractical, security over this information must be maintained.

(b) Secret Messages. Secret messages will be routed to individual officers and departments by the SECMGR. If they do not choose to retain the message, they will immediately return it to the SECMGR for filing or destruction.

e. Transmission of Classified Material Outside the Command. All Secret material transmitted by NAVSUPPACT Naples to other commands or activities will be recorded on OPNAV Form 5511/10, Record of Receipt, (enclosure (10)). If Confidential matter is transmitted by registered mail, the registered mail receipt will suffice as evidence of transfer. For Secret material, enclosure (10) and registered mail receipts will be filed in numerical control number and date order, respectively.

f. Reproduction of Classified Material. Reproduction of classified material will be strictly controlled. Detailed control procedures are listed in Chapter 7 of reference (a). Secret material will not be reproduced without the permission of the SECMGR. Top Secret material can only be reproduced by the Top Secret Control Officer and only after permission has been obtained by the originator of the document.

g. Level of Classification. Classification can be accomplished either by Original Classification Authority (OCA) or derivative classification.

(1) Original classification authority rests with the Secretary of the Navy and a limited number of officials he has designated as listed in chapter 4, exhibit 4A of reference (a).

Neither NAVSUPPACT Naples nor any of its members is an original classification authority.

(2) Derivative classification is accomplished by anyone who incorporates, paraphrases, relates, or generates new form information which is already classified. Information extracted from a classified source will retain the classification markings exactly as shown on the source material.

(3) Unnecessary or higher than necessary classification will be avoided. However, when there is reasonable doubt about the level at which to classify information, the material will be safeguarded at the higher level until the proper level is determined through a classification guide or the OCA. Department heads and special assistants are responsible for ensuring appropriate classification, per reference (a), is assigned to all classified documents and messages originated by their departments.

h. Marking. Classified material/correspondence will be physically marked, per reference (a), to identify the classification level and the degree of protection required to safeguard it. Classified hardware, software, recordings, photographs, etc., will also be physically annotated or identified by other means as prescribed in references (a), (c), and (g). SECNAVINST 5216.5D, DON Correspondence Manual, provides additional guidance on the use of classification markings.

2. Instruction for Receipt, Internal Dissemination, and Transmission of Top Secret Material. Per reference (a), the TSCO will use two-person integrity when handling and processing all Top Secret or special category material.

DESTRUCTION OF CLASSIFIED MATERIAL

1. Basic Policy. Destruction of unneeded classified information is essential to an effective Command Security Program. The benefits of reducing classified holdings are:

- Allows for better protection
- Reduces storage needed
- Reduces administrative workload
- Better prepared for emergency

Reference (e) provides specific command guidelines on the emergency destruction of classified material. Reference (h) includes information to determine what constitutes record information on the retention/transfer of record information to the Federal Records Center. For destruction of special types of classified information (SCI, CMS, NATO), refer to the applicable guidance for the programs or contact the SECMGR.

2. Destruction Procedures. Use only authorized means and personnel cleared to the level of information being destroyed. Burn bags may be used if classified information cannot be immediately destroyed and to help ensure adequate storage prior to destruction. Only striped burn bags are authorized and they must be marked and stored in containers according to classification level until actually destroyed. If burn bags need to be transported by vehicle for destruction, only an enclosed vehicle will be used, and prior authorization must be obtained from the SECMGR/ASST SECMGR.

3. Destruction Records

a. Confidential information requires no record of destruction except for NATO and Foreign Government Information (FGI).

b. Secret information requires record of destruction. OPNAV Form 5511/12, Classified Material Destruction Report, or any other record (computerized or log book) that fully identifies the material, shows the number of copies destroyed, indicates the name of the person conducting destruction procedures and shows the date of destruction. Retain Secret destruction records for one year.

c. Top Secret information destruction requires the same procedures listed under Secret information destruction. **Additionally, OPNAV Form 5511/12 (enclosure (11)) or any other record used, must be signed by two cleared witnesses.** Although a record of destruction is not required for Top Secret waste products, such as working papers and notes, proper destruction procedures as outlined in reference (a) must be adhered to. If in doubt as to what constitutes waste products, contact the SECMGR for guidance and clarification. Retain Top Secret destruction records for five years.

4. Destruction Methods. Use a method that prevents later recognition of reconstruction, such as:

a. Burning, the traditional method, has both advantages and drawbacks. Although large quantities may be destroyed at once, it requires constant monitoring and rotating of bottom material to ensure total disintegration.

b. Shredding machines. Ordinarily suffices as complete destruction; residue handled as unclassified waste (there are exceptions for COMSEC, SCI, and some Information Systems (IS) media (e.g, CD-ROMs). Use only crosscut shredders-shreds 3/64 inches wide by 1/2 inch long.

c. Pulverizers and disintegrators - must have 3/32 inches or smaller security screen. May be used for information such as photographs, typewriter ribbons, or glass slides.

Reference (a) lists additional authorized methods, such as mutilation and chemical decomposition. For guidance on the destruction of nonpaper classified information, such as IS Media (hard drives, floppy disks, CD-ROM, etc.), contact the ADP Security Manager/ISSM.

NOTE: Every NAVSUPPACT Naples department holding classified material should make every effort possible to purchase a GSA-approved shredder. To avoid transport or delay in the event of emergency destruction, shredder should be placed in close proximity to the safe/area containing classified information.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.2, 1.3, and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, * the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.

STANDARD FORM 312 (Rev. 1-00)
Prescribed by NARA/ISOO
32 CFR 2003, E.O. 12958

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military): Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See Notice below)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		**THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.**	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or print)*		NAME AND ADDRESS *(Type or print)*	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (Rev. 1-00)

PERSONNEL SECURITY ACTION REQUEST

PART I - SUBJECT INFORMATION

(Items 1 Thru 8 must be completed for all requests)

1. Name (Last, First, Middle)	2. SSN	3. Grade/Rank	4. Designator/MOS/RATING

5. Status	6. Former Maiden Name/Aliases	7. Date of Birth (YYYYMMDD)	8. Place of Birth

(Items 9 thru 11 required when requesting SCI eligibility determination)

9. Date and Place of Current Marriage (YYYYMMDD)	10. Date and Place of Divorce (YYYYMMDD)

11. Citizenship of: a. Parents: _____ b. Brothers: _____ c. Sisters: _____

d. Spouse/Cohabitant: _____ e. Children: _____

PART II - LOCAL SECURITY REQUIREMENTS

12. U.S. Citizenship verified: ☐ YES ☐ NO

13. Local Records Check Accomplished: ☐ Favorable ☐ Unfavorable (ATTACH ANY UNFAVORABLE COMMENTS).

14. Subject has continuous service with no break greater than 24 months verified: ☐ YES ☐ NO

PART III - NOTIFICATION OF COMMAND ACTION

15. ☐ Final ☐ Interim ☐ Top Secret ☐ Secret ☐ Confidential clearance granted IAW OPNAVINST 5510.1H requirements.

16. Personnel Security Investigation mailed to DIS on (YYYYMMDD): _____

17. Subject's clearance and access were administratively lowered without prejudice to: ☐ No Clearance ☐ Confidential ☐ Secret.

18. Suspended subject's access for cause to: ☐ SCI Only ☐ All Classified Information on (YYYYMMDD): _____ (ATTACH DETAILS)

19. Other:

PART IV - DONCAF ACTION REQUESTED

20. Determination Requested: ☐ Confidential ☐ Secret ☐ Top Secret ☐ SCI Eligibility ☐ TIS (YYYYMMDD) _____

(CIVILIAN) ☐ Non-Critical Sensitive ☐ Critical Sensitive ☐ Special Sensitive

21. Other:

PART V - ADMINISTRATIVE

22. Remarks/Enclosures

23. Requesters Complete Mailing Address:	24. UIC/RUC/OPFAC (SUBMITTING): _____ 25. UIC/RUC/OPFAC (RETURN): _____ 26. NSG Asset: ☐ YES ☐ NO

27. Date	28. Name, Grade/Rank, Title and DSN/Commercial Number	29. Signature

INSTRUCTIONS FOR COMPLETING OPNAV 5510/413

1. NAME: Last name in all CAPS, omit commas, hyphens, periods, apostrophes or blanks within the name.

2. SOCIAL SECURITY NO: Use hyphens after the 3rd and 5th digits.

3. GRADE/RANK: Self-explanatory.

4. DESIGNATOR/MOS/RATING: 1630, 1100, 0211, IS1, CTTCS, RM2, etc.

5. STATUS: Use one of the following codes:

B - Active Duty Enlisted	I - NAF Employee	N - Academy Cadet	V - Consultant
C - Active Duty Officer	J - Civilian Educator	Q - Nato	W - Non-DoD Affiliated
D - Reserve Enlisted	K - Contractor	R - Civilian Temporary/Seasonal/Co-op	X - Officer Candidate
E - Reserve Officer	L - General/Flag Officer	S - Delayed Entry Program	Z - Unknown
H - Civilian Employee	M - ROTC - Cadet	T - Retired General/Flag Officer	5 - Warrant Officer - Active
		U - Foreign National Employee	6 - Warrant Officer - Reserve

6. FORMER/MAIDEN NAMES/ALIASES: If no other names enter "None".

7. DATE OF BIRTH: Year, month and day.

8. PLACE OF BIRTH: Enter state if US born; city and country if foreign born. Specify part of country if politically divided (e.g., North or South Korea).

9. DATE AND PLACE OF CURRENT MARRIAGE: Year, month and day, and city and state. **(SCI ONLY)**

10. DATE AND PLACE OF DIVORCE: Year, month and day, and city and state. **(SCI ONLY)**

11. CITIZENSHIP OF PARENTS, BROTHERS, SISTERS, SPOUSE/COHABITANT/CHILDREN. **(SCI ONLY)**

12. U.S. CITIZENSHIP VERIFIED: Check Yes or No.

13. LOCAL RECORDS CHECK ACCOMPLISHED: Check Favorable or Unfavorable. If there is unfavorable information, provide details under item 22 or on an addendum sheet.

14. SUBJECT HAS CONTINUOUS SERVICE WITH NO BREAK GREATER THAN 24 MONTHS VERIFIED: Check Yes or No.

15. INTERIM/FINAL CLEARANCE GRANTED TO TOP SECRET/SECRET/CONFIDENTIAL: Check Interim or Final and check either Top Secret/Secret or Confidential.

16. PERSONNEL SECURITY INVESTIGATION MAILED TO DIS ON: Date package forwarded to DIS; year, month and day.

17. SUBJECT'S CLEARANCE AND ACCESS WERE ADMINISTRATIVELY LOWERED WITHOUT PREJUDICE TO: Check the appropriate answer.

18. SUSPENDED SUBJECT'S ACCESS FOR CAUSE TO: Check either SCI Only or All Classified. Provide year, month and day of suspension and provide detailed information either under item 22 or on an addendum sheet.

19. OTHER: To be used for changes such as name or status or to advise that an individual who has security clearance eligibility without access has been moved to a non-sensitive position.

20. DETERMINATION REQUESTED: Check ALL the determinations that are required. Civilians will usually have at least two requested actions checked (e.g., position sensitivity and clearance) and requests for SCI should also indicate clearance level required (as well as position sensitivity if civilian).

21. OTHER: If other than clearance, identify action required.

22. REMARKS/ENCLOSURES: If space is sufficient, provide details from items 13 and/or 18. Also use this space to provide an unclassified "Statement of Urgency and Justification" for non-routine requests for SCI eligibility or any other narrative necessary to support your request.

23. REQUESTERS COMPLETE MAILING ADDRESS: When results are to be returned to the Submitting Command/Unit, provide the complete mailing address of Submitting Command/Unit, also enter UIC/RUC/OPFAC in item 24. When the Submitting Command/Unit is requesting a clearance for a Gaining Command/Unit, provide the complete mailing address of the Gaining Command/Unit, also enter UIC/RUC/OPFAC in item 25, if known.

24. UIC/RUC/OPFAC (SUBMITTING): UIC of Submitting Command/Unit.

25. UIC/RUC/OPFAC (RETURN): UIC of Command/Unit requiring final eligibility message.

26. NSG ASSET: If the individual is in a Naval Security Group Billet, check Yes.

27. DATE: Self Explanatory.

28. NAME, GRADE/RANK, TITLE, AND DSN/Commercial No: Self Explanatory.

29. SIGNATURE: Self Explanatory.

OPNAV 5510/413 (Rev. JAN 1994)

SECURITY CONTAINER INFORMATION

INSTRUCTIONS

1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP).
2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER.
3. MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER.
4. DETACH PART 2A AND INSERT IN ENVELOPE.
5. SEE PRIVACY ACT STATEMENT ON REVERSE.

1. AREA OR POST (If required)	2. BUILDING (If required)	3. ROOM NO.
4. ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5. CONTAINER NO.
6. MFG. & TYPE CONTAINER	7. MFG & TYPE LOCK	8. DATE COMBINATION CHANGED
9. NAME AND SIGNATURE OF PERSON MAKING CHANGE		

10. Immediately notify one of the following persons, if this container is found open and unattended.

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

WARNING

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

DETACH HERE

CONTAINER NUMBER

COMBINATION

_____ turns to the (Right) (Left) stop at _____

_____ turns to the (Right) (Left) stop at _____

_____ turns to the (Right) (Left) stop at _____

_____ turns to the (Right) (Left) stop at _____

WARNING

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.

UNCLASSIFIED UPON CHANGE OF COMBINATION.

2A INSERT IN ENVELOPE

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

☆U.S. GOVERNMENT PRINTING OFFICE: 1986 — 485-058

CORRESPONDENCE/MATERIAL CONTROL (4 PT)
OPNAV 5216/10 (6-78) SN: 0107-LF-052-1650

CONTROL NUMBER	CLASSIFICATION OF THIS SHEET, ONLY	**CLASSIFICATION OF ATTACHED MATERIAL**

FROM	SERIAL	DATE	FILE SYMBOL (SSIC)	CROSS REFERENCE
VIA	DATE RECEIVED		REPLY DUE BY	
TO	NUMBER OF COPIES RECEIVED		ENCLOSURES RECEIVED	
SUBJECT				

WARNING: ENTRY OF CLASSIFIED SUBJECT OR TITLE WILL REQUIRE CLASSIFICATION OF THIS FORM AND ALL COPIES

CONTROL CENTER PRIMARY ROUTING					INTRA-ACTIVITY SECONDARY ROUTING				
TO	AC*	DATE OUT	INITIAL RECEIPT	RETURN DATE	TO	AC*	DATE OUT	INITIAL RECEIPT	RETURN DATE

*ACTION CODES

A - Action
C - Comment
I - Information
P - Prepare reply
R - Retain copy

INSTRUCTIONS:

1. Extra copies will be destroyed after 30 days unless interested offices give contrary instructions to CONTROL CENTER.
2. Office retaining material, detach and return this control record to the CONTROL CENTER.
3. When detached, this form is unclassified unless a classification has been assigned in the spaces provided, as required by existing security instructions.
5. Offices having primary interest check one:
   - ☐ Retain indefinitely. (Reference value)
   - ☐ Retain _____ months. (Info material having only temporary reference value)
   - ☐ Destroy after routing. (No further reference or information value)

CODE | SIGNATURE

REMARKS

THIS FORM IS UNCLASSIFIED WHEN DETACHED FROM THE DESCRIBED MATERIAL, UNLESS OTHERWISE INDICATED.	CONTROL NUMBER
CLASSIFICATION OF ATTACHED MATERIAL	CLASSIFICATION OF THIS SHEET, ONLY

Enclosure (9)

NOTE: OPNAV 5216/10 SUPERSEDES OPNAV FORMS 5511/23, 5511/23A, 5511/23B, 5511/23C, WHICH MAY BE USED UNTIL EXHAUSTED.

OPNAV 5511/10 (REV. 6-79)
S/N 0107-LF-055-1151

RECORD OF RECEIPT

(REFERENCE SECNAVINST 5216.5)

THIS RECEIPT MUST BE SIGNED AND RETURNED.

ORIGINATOR'S CODE	FILE OR SERIAL NUMBER	DATE OF MATERIAL	UNCLASSIFIED DESCRIPTION	COPY NO.	NO. OF ENCLS. TO MAT'L RCD	REGISTERED NUMBER

ADDRESSEE (ACTIVITY RECEIVING MATERIAL)

SIGNATURE (AUTHORIZED RECIPIENT)	DATE

CLASSIFIED MATERIAL DESTRUCTION REPORT TO:	CLASSIFICATION *(Indicate when title or other identification is classified)*
FROM *(Name and address of activity)*	

The classified material described below has been destroyed in accordance with regulations established by the Department of the Navy Information Security Program Regulation, OPNAV INSTRUCTION 5510.1E.

The purpose of this form is to provide activities with a record of destruction of classified material. Also, copies may be utilized for reports to activities originating material, where such reports are necessary.

DESCRIPTION OF MATERIAL

SERIAL/LOG	ORIGINATOR	DATE	COPY NO.	LOG/ ROUTE SHEET	ENCLOSURES (IDENT. & NO.)	TOTAL NO. PAGES

OFFICER OR INDIVIDUAL AUTHORIZING DESTRUCTION *(Signature, Rank/Rate/Grade)*	DATE OF DESTRUCTION
WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)*	WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)*

OPNAV 5511/12 (Rev. AUG 1975)

CLEAR