



DEPARTMENT OF THE NAVY  
UNITED STATES NAVAL ACADEMY  
121 BLAKE ROAD  
ANNAPOLIS MARYLAND 21402-1300

USNAINST 5510.8A  
4/AsstSecMgr  
JUN 6 2008

USNA INSTRUCTION 5510.8A

From: Superintendent, United States Naval Academy

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM

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

Encl: (1) Personnel Security Clearance and Access  
(2) Accounting, Control, Reproduction, and Destruction of Classified Material  
(3) Physical Security of Classified Material  
(4) Classified Information Nondisclosure Agreement (SF 312 (1-00))  
(5) Visit Request (OPNAV 5521/27 (9-92))  
(6) Classified Material Cover Sheets (SF 703, 704, and 705 (8-85))  
(7) Security Discrepancy Notice (OPNAV 5511/51 (5-80))  
(8) Activity Security Checklist (SF 701 (8-85))  
(9) Security Container Information (SF 700 (8-85))  
(10) Security Container Check Sheet (SF 702 (8-85))

1. Purpose. To provide supplemental regulations to references (a) through (c) concerning the information and personnel security policies and procedures of the United States Naval Academy (USNA).

2. Cancellation. USNA/NSAA Instruction 5510.8

3. Information. References (a) and (b) carry out the Department of the Navy's Information and Personnel Security Program. Reference (c) issues the Navy's Automated Data Processing (ADP) Security Program.

4. Scope. This instruction addresses the Navy Information and Personnel Security Program for military and civilian, appropriated and non-appropriated fund personnel attached to the USNA and tenant commands receiving program support. It provides supplemental guidance to the information contained in references (a) through (c). Nothing in this instruction can countermand the material in those references; it is to be used with those instructions.

5. Responsibilities. Security is the daily responsibility of every person. Each individual will familiarize himself/herself with enclosures (1) through (10). The specific responsibilities related to the management of the Information and Personnel Security Program follows:

a. Security Manager. Serves as principal advisor to the Superintendent for the Information and Personnel Security Program. The Security Manager will coordinate any Preliminary Inquiry or Judge Advocate General Manual (JAGMAN) investigations required to identify circumstances surrounding potentially lost or compromised classified information.

b. Assistant Security Manager. The Assistant Security Manager will:

(1) Ensure access to classified information is limited to those with a need-to-know.

(2) Process required security investigations for USNA and tenant command personnel. Record personnel security investigations, clearances, and access. Maintain access lists of cleared personnel.

JUN 6 2008

(3) Ensure compliance with the requirements of references (a) through (c) for the day-to-day security operation. Coordinate with command and security personnel for the physical protection of classified material and for the protection of classified information contained in Information Systems.

(4) Provide specific guidance to personnel to make sure that receipt, marking, reproduction, transmission, and destruction of classified material comply with references (a) through (c).

(5) Inform the Security Manager of all security violations. Ensure security compromises are reported, recorded, and when necessary, investigated vigorously. Ensure that incidents falling under the investigative jurisdiction of Naval Criminal Investigative Service (NCIS) are immediately reported.

(6) Develop a command security training program. Ensure that annual and biannual training requirements are met in accordance with references (a) and (b). Provide informal training as required for designated Security Representatives on a quarterly basis. Provide security debriefings to command personnel as required for discontinuation of access to classified information.

(7) Designate each civilian position as either critical-sensitive, non-critical sensitive, or non-sensitive per reference (a).

(8) Manage and administer a program for the continuous evaluation of command and tenant personnel who have access to classified information or are employed in a sensitive position.

c. Top Secret Control Officer. The Security Manager is designated as the Top Secret Control Officer (TSCO). The TSCO is responsible for the proper handling, control, distribution, inventory, and destruction of all Top Secret material.

d. Assistant Top Secret Control Officer. The Assistant Security Manager is designated as the Assistant Top Secret Control Officer (ATSCO). The ATSCO assists the TSCO as required, and functions as the TSCO during his/her absence.

e. The Staff Judge Advocate; USNA Commandant's Legal Advisor; NSA Annapolis Legal Officer; Director Human Resources Department; and Commanding Officer, Naval Health Clinic will report:

(1) Any information obtained or developed concerning any individual, including midshipmen, which may bear on that individual's loyalty, reliability, judgment, and trustworthiness. Upon initial receipt of credible derogatory information, a determination to temporarily suspend the individual's access to classified information will be made by the Assistant Security Manager.

(2) Examples of incidents that must be reported include incidents, infractions, offenses, charges, citations, arrests, suspicion, or allegations of illegal use or abuse of drugs or alcohol, theft or dishonesty, lack of reliability, irresponsibility, immaturity, instability or recklessness, the use of force, violence or weapons or actions that indicate disregard for the law due to multiplicity of minor infractions. Report any indications of moral turpitude, sexual promiscuity, aberrant, deviate, or bizarre conduct or behavior, transvestism, transsexualism, indecent exposure, rape, contributing to the delinquency of a minor, child molestation, spouse-swapping, window peeping, and similar situations from whatever source.

(3) Unlisted full-time employment or education; full-time education or employment that cannot be verified by any reference or record source or that contains indications of falsified education, or military service where the individual was involved in serious offenses or incidents that would reflect adversely on the honesty, reliability, trustworthiness, or stability of the individual.

(4) Foreign travel, visits, correspondence, relatives, or contact with persons from or living in communist-dominated countries or areas designated as terrorist-oriented-only by individuals who have access to classified information.

(5) Mental, nervous, emotional, psychological, psychiatric, or character disorders/behavior or treatment reported or alleged from any source for individuals who have access to classified information.

JUN 6 2008

(6) Excessive indebtedness, bad checks, financial difficulties or irresponsibility, unexplained affluence, bankruptcy, or evidence of living beyond the individual's means by individuals who have access to classified information.

(7) Reports should be forwarded to the Assistant Security Manager, Building 257, Room 307, by messenger or fax to x32969. Information may be consolidated over a period of no more than 30 days. Attachments can be affixed to a covering memo, but minimally the reports should contain the following information:

(a) Full name.

(b) Social Security Number, alpha number, if applicable.

(c) A narrative statement, incident report, honor/conduct violations specific charges including Uniform Code of Military Justice (UCMJ) articles or Federal/State statutes (if known).

(d) Resulting punitive or administrative action taken.

(e) Point of contact with a phone number for additional information if required.

(8) Negative reports are required.

f. Division Directors/Department Heads will:

(1) Promote security awareness within this organization by making sure that all personnel read and understand enclosures (1) and (2).

(2) Appoint an individual, in writing, to serve as the Division or Department Security Representative for their organization, and provide the Assistant Security Manager with a copy of this appointment. The representative must be familiar with security procedures and regulations. Each department is required to appoint a Security Representative even though they do not use classified material. The Representative will liaison with the Assistant Security Manager.

(3) Ensure the Security Representative conducts a formal turnover with the new designee prior to their detachment date.

(4) Report to the Assistant Security Manager any adverse information obtained or developed on an individual that may bear on his/her ability to maintain a security clearance, sensitive position, or position of trust.

g. Division/Department Security Representatives will:

(1) Ensure military personnel in their department check in and check out with the Assistant Security Manager.

(2) Brief newly reporting civilian and military personnel (including part-time and temporary) on USNA security procedures. This briefing should be within one week of their arrival.

(3) Attend quarterly informal security briefings held by the Assistant Security Manager. Provide makeup training for personnel who miss mandatory training as scheduled. Ensure personnel attend annual and biennial mandatory security briefings as required. Provide attendance rosters to the Assistant Security Manager's Office.

(4) Serve as custodian responsible for the proper use, marking, control, accountability, and destruction of classified material. Ensure that safe combinations are changed when required.

(5) Report security violations to the Security Manager or the Assistant Security Manager.

JUN 6 2008

h. All individuals are responsible for:

(1) Reading, understanding, and complying with policies and procedures established in this instruction and its enclosures.

(2) Attending the mandatory annual security refresher training session and the biennial counterintelligence briefing when scheduled.

(3) Safeguarding classified information by using classified information and controlled unclassified information (CUI) under conditions adequate to prevent unauthorized persons from gaining access to it; using the enclosed forms; locking classified information in appropriate security containers, whenever it is not in use or under direct supervision of authorized persons; and reporting any suspected compromise or loss of classified material to their Division/Department Head, Security Representative, or by notifying the Assistant Security Manager immediately.

(4) Reporting any adverse information bearing on any individual's loyalty, reliability, judgment, and trustworthiness to their Division/Department Head, Security Representative, or the Assistant Security Manager.

6. Action. All personnel assigned responsibility under the Information and Personnel Security Program will take required actions.

7. Forms. Enclosures (4), (5), (7), (8), and (10) may be obtained at [www.navysecurity.navy.mil](http://www.navysecurity.navy.mil). Click on forms at the top of the web site. Enclosures (6) and (9) can be obtained from the Assistant Security Manager.

/S/  
J. L. FOWLER

Distribution:  
All Non Mids (electronically)

## PERSONNEL SECURITY CLEARANCE AND ACCESS

1. Access to Classified Material. No one has a right to have access to classified information solely because of rank, position, or investigative basis. Access will be granted on a need-to-know basis as determined by an analysis of the functions of each billet/position. Do not assume military and civilian personnel hold adequate security clearances. Do not disclose classified information until you verify a need-to-know and the clearance level of an individual.

a. Access to classified material/information is granted by the Security Manager based upon a mission requirement and the designated position sensitivity of an individual's position description. Individuals processed for a clearance must sign a Classified Information Nondisclosure Agreement (SF 312), enclosure (4). The appropriate information is forwarded to the Department of Navy Central Adjudication Facility which has authority under reference (a) to adjudicate a security clearance.

b. The Assistant Security Manager will grant access to individuals with a mission requirement for NATO access after briefing them on NATO security procedures.

### 2. Security Education Responsibilities

a. Assistant Security Manager:

- (1) Conduct security refresher briefings as required by reference (a).
- (2) Keep records of security briefing attendance.

b. Division/Department Security Representatives:

- (1) Brief newly reporting personnel within one week from their arrival on security procedures.
- (2) Ensure all personnel who have access to classified material receive the required security briefings. Forward attendance rosters to the Assistant Security Manager.
- (3) Ensure all personnel who have access to classified information attend a counterespionage briefing at least once every two years.
- (4) Ensure all personnel who require access to NATO information are briefed by the Security Manager on NATO security procedures before access is granted.
- (5) Ensure temporarily assigned personnel, whether military or civilian, are briefed on proper Division/Department security procedures.

3. Visits and Meetings. Basic policy regarding visits and meetings is found in Chapter 7 of reference (b). Classified meetings will be arranged by the Assistant Security Manager's Office.

a. For Security purposes, the term "visitor" applies to:

(1) Any person who is not attached to or employed by the USNA, NSA Annapolis, or tenant activities.

(2) A person on temporary additional duty.

b. Outgoing Classified Visits. A Visit Request, Visitor Clearance Data (OPNAV 5521/27), enclosure (5), will be filled out by Division/Department clerical support when USNA/NSA Annapolis personnel plan classified visits to other activities or organizations. The Visit Request form will be forwarded, hand carried, or faxed to the Assistant Security Manager, Stop 18h, for security certification at least five days in advance of the proposed visit. In lieu of enclosure (5), a visit request may be entered into the Joint Personnel Adjudication System (JPAS) data base. For JPAS visit requests the visitor's name and social

JUN 6 2008

security number, the visit start and end dates, and the destination JPAS Security Management Office (SMO) code and point of contact name and phone number must be provided to the USNA Security Manager's office.

c. Incoming Classified Visits. The Assistant Security Manager is the central point for receiving and recording incoming classified visit requests from outside activities. If the office to be visited receives a classified visit request directly, a copy of the request must be forwarded to the Assistant Security Manager's Office. Incoming visit requests from other organizations are maintained on file in the Security Manager's Office for the duration of the visit, not to exceed one year.

d. Granting Access to Visitors. Custodians must adhere to the following before granting access to classified information to a visitor:

- (1) Verify visitor identification and visitor's need-to-know.
- (2) Check with the Assistant Security Manager's Office for clearance verification.

e. Visits by Foreign Nationals. Visits by foreign nationals, which will involve substantive technical discussions or the disclosure of classified information, must first be approved by the Director, Special Events Office. The Assistant Security Manager will notify and coordinate with the Director, Special Events; Director, International Programs Office and Public Affairs Office for visits from foreign nationals.

f. Foreign National Faculty and Staff. The USNA employs Foreign National Faculty and Staff who do not have citizenship with the United States of America. These colleagues are issued Common Access Cards (CAC) distinguished by a vertical red stripe down the center. The red stripe identifies the holder as a Non-U.S. citizen, and therefore is not eligible for access to classified national security information, nor Controlled Unclassified Information (CUI). All civilian identification cards shall be displayed above the bearer's waist, either by a clip device or neck chain. This policy is generally known and policed by all members of the command.

JUN 6 2008

**ACCOUNTING, CONTROL, REPRODUCTION, AND DESTRUCTION OF CLASSIFIED MATERIAL**

1. Classified Material Cover Sheet. All personnel will affix the proper Classified Material Cover Sheets (SF 703, 704, and 705); enclosure (6), to all classified material when it is originated or upon discovering material is without such protection.

2. Security Markings. All classified material must be properly marked and formatted. Division/Department Security Representatives should be consulted regarding questions related to classification markings.

3. Mailing of Classified Material

a. Yard Mail. DO NOT send classified material through the yard mail. If you receive classified material through the yard mail, report it immediately to your Division/Department Security Representative or the Assistant Security Manager. The Division/Department Security Representative will forward a Security Discrepancy Notice (OPNAV 5511/51), enclosure (7), to the Assistant Security Manager.

b. U.S. Mail. Classified material will be delivered to the Assistant Security Manager's office for issuance of a classified control number and mailing.

4. Use of Classified Material in the Local Area

a. All classified material will be placed into a system of accountability by the Assistant Security Manager. Bring any hand-carried classified information to the Assistant Security Manager for processing into the Classified Material Accounting System.

(1) All official registered mail will be received by the Assistant Security Manager. If classified material is erroneously forwarded directly to an individual, it is their responsibility to immediately hand-carry the material to the Assistant Security Manager for processing into the Classified Material Accounting System.

(2) An annual inventory of all classified holdings will be completed by the responsible custodian or Security Representative and forwarded to the Security Manager annually on 15 February. The Assistant Security Manager may conduct unannounced inspections of classified holdings in departments, as required, to ensure proper procedures are being followed.

b. All Secret and Confidential material that is to be transmitted from USNA to another facility or agency will be prepared by the Assistant Security Manager. This includes the use of U.S. Mail.

5. Escort or Hand Carrying Documentation. Individuals hand carrying classified information will carry a Letter of Authorization to Hand Carry Classified Material issued by the Assistant Security Manager. The authorization statement may be included in official travel orders, except for travel aboard commercial aircraft, in which case an authorization letter is also required. Individuals who frequently hand carry classified information may be issued the optional Courier Authorization Card, DD Form 2501. The Courier Authorization Card will allow an escort to pass security inspection points at Department of Defense (DOD) facilities without the material being opened and inspected. Classified material being hand carried for use outside the USNA will remain in the custody of the action officer at all times. Classified material will not be hand carried in folder or similar container. The material will not be studied or displayed on public conveyances (i.e., DOD buses, metro, shuttle, etc.), or left unattended in private or government vehicles, hotel, or conference rooms. A lockable briefcase may serve as the outer wrapper.

b. When hand carrying classified material for transfer to another command, the requirements of reference (a) for wrapping, addressing, and receipt must be followed.

c. Classified material will not be transmitted by facsimile equipment or similar devices using unsecured telephone lines. Classified discussions must be conducted on Secure Telephone Units. If you must

JUN 6 2008

discuss classified information, contact the Assistant Security Manager's Office for the location of the nearest secure telephone.

6. Top Secret Accountability. All Top Secret material must be taken to the TSCO who will inventory and maintain the document. The TSCO will retain physical custody of all Top Secret material. The Top Secret document can be released to the custody of an individual with Top Secret access and a verified "need-to-know." It will be returned to the TSCO that working day. The individual must sign for the document and is responsible for its return to the TSCO. There will be two-person integrity for the control of Top Secret Communications Security material.

7. Secret Accountability. Secret material must be carefully controlled. Division or Department Security Representatives are the only authorized personnel who may sign for material contained in the Assistant Security Manager's Classified Material Repository. He/She will maintain logs, indicating disclosure and destruction records of Secret material. When Secret messages are in circulation, they must be handled as individual Secret documents with a Secret Classified Material Cover Sheet attached (see enclosure (6)). This includes Secret messages and media used to originate messages. The messages must be signed for, destroyed by shredding or burning and the destruction record signed.

8. Confidential Accountability. Although procedures for the protection of Confidential material are less stringent than those for Secret material, all Confidential material removed from the Classified Material Repository will be signed for by the Division/Department Security Representative. Confidential material will have the Confidential Classified Material Cover Sheet affixed and will be safeguarded in a manner that will ensure that it is not disclosed to unauthorized users.

9. NATO and NATO Classified Information. NATO classified documents will not be intermingled with U.S. documents in storage containers. They may be filed in the same drawer of a security container with U. S. documents if they are segregated and clearly identified as NATO files. Additional information regarding the protection of NATO material may be obtained by contacting the USNA Security Manager's office. NATO and NATO classified material may not be reproduced without the permission of the Assistant Security Manager.

10. Accountability of Classified Automated Data Processing Material. ADP material or media containing classified information will be labeled, controlled, and safeguarded in a manner equivalent to the classification of the information. Specific procedures for the protection of classified information contained in information systems are contained in reference (c).

11. Destruction. All classified material will be destroyed when no longer required. The TSCO is responsible for destroying or accounting for return to originator all Top Secret material.

a. Methods of Destruction. Shredding and burning are the only authorized methods of destruction. Classified material awaiting destruction must be protected in transit and destroyed by authorized personnel cleared to the level of the material. One person must destroy and one person must witness the destruction.

b. Documentation

(1) Use of the Classified Material Destruction Report (OPNAV 5511/12) is no longer required but may be used. Record destruction of classified material and any special category information (if required) by any means, as long as the record includes identification of material destroyed, number of copies, and date of destruction. Destruction documentation will be retained for two years.

(2) The fact that an originator may state in a document that it may be destroyed without report does not change the requirement to record destruction; it only means you do not have to notify the originator that the document was destroyed.

JUN 6 2008

(3) Classified working papers must now be accounted for, marked, and controlled as a finished document at 180 days from date of origin, vice 90 days.

(4) Destruction reports are not required for Confidential material.

(5) All message traffic, classified or unclassified, that is printed must be destroyed either by shredding or burning. Do not place message traffic in trash receptacles.

12. Reproduction of Classified Material. Reproduction of classified material must be mission essential and approved by the Assistant Security Manager.

13. Information Technology (IT) Policy and Controls

a. The Naval Academy Data Network (NADN) is a non-SIPRNET, non-NIPRNET teaching and learning network supporting midshipmen, faculty and staff in the educational and research mission of the USNA. Midshipmen, faculty, and staff are not authorized to access any classified materials via NADN. The entire user workforce can access:

(1) Email. Users have an email address from the .edu domain (loginID@usna.edu). Email gives users the ability to send email from USNA servers in our .edu domain and receive email from internal and external users. In addition, Foreign Nationals have an email alias that includes their first and last name and defines their nationality (Firstname.Lastname.cc@usna.edu). The cc abbreviation equates to the standard FIPS country code. Email display names and signature blocks also contain the country of origin.

(2) Intranet. The intranet provides access to information restricted to midshipmen, faculty, and staff. The general public cannot access this information.

(3) Internet. Midshipmen, faculty, and staff can access the internet and can view any publicly available pages which may include some .mil sites.

b. Faculty members have access to USNA teaching and learning applications. These systems contain sensitive privacy information relating to midshipmen, including alpha numbers, grades, and other academic, professional development, and physical education related information. More sensitive Protected Personal Information (PPI), such as social security numbers, parents names and addresses, home phone numbers, etc. is further restricted to faculty and staff with specific job related requirements. The Academic Dean's Registrar grants faculty access to academic related information based upon the faculty member's teaching assignments. The Commandant's Midshipman Personnel Officer controls access to midshipman performance development and personal information. These accesses are reviewed and modified before and after each semester.

c. Special hardware configurations are required to give the .edu domain the appearance of a .mil domain. The specific physical location of the hardware device is known to and monitored by IT security personnel. Accounts with this special configuration are approved by the Naval Academy's Information Technology Services Information Assurance Manager. An increasing number of .mil domain sites require users to authenticate using their Common Access Card (CAC). This authentication is in addition to identifying the physical location of the device requesting access to the .mil site. The network devices in all faculty offices have a .edu address and allow access only to publicly available .mil sites and any other internet site which allows .edu access. This ensures unauthorized personnel cannot access controlled .mil domains.

JUN 6 2008

## PHYSICAL SECURITY OF CLASSIFIED MATERIAL

1. Unauthorized Personnel. All Naval Academy personnel must be alert to the entry of unauthorized or uncleared personnel into areas where classified information is held. Challenge strangers, escort them from the area, and report the incident to your Division/Department Security Representative.

2. Activity Security Checklist. A security inspection of working spaces will be conducted by the building Duty Officer at the end of each working day. This inspection will include:

a. Thoroughly examining each working space to ensure all classified and valuable government and personal property has been secured.

b. Verifying proper closure of all safes and vaults in each working space.

c. Initialing an Activity Security Checklist (SF 701), enclosure (8), as verification that a security inspection has been conducted and that all spaces have been properly secured. The security checklist will be maintained for a minimum of five working *days*.

d. Division/Department Security Representatives should conduct random inspections of their areas to verify checklists.

3. Limiting Areas for Use and Storage of Classified Material. Classified material will be *used* and stored to ensure access is granted only to those with the proper clearance and need to know.

a. Division/Department Security Representatives will ensure the spaces designated for *use* and storage of Top Secret and Secret material are continually manned when *safes* are open or classified material is being used.

b. Division/Department Security Representatives and NSA Installation Program Directors will report the movement of safes containing classified material to the Assistant Security Manager.

4. Safe Combinations. Changes to safe combinations will be event driven. Combinations will be changed:

a. When placed in *use*.

b. When the combination has been subjected to compromise.

c. When the combination is taken out of service.

d. When an individual knowing the combination no longer needs access to it.

Combinations will be recorded on copy 2 of the Security Container Information Form (SF 700), enclosure (9), and placed in the Combination Change Envelope. After completion of the Security Container Information Form, copy 1 must be affixed to the inside of the safe drawer containing the lock. The envelope is then hand carried to the Assistant Security Manager's Office.

5. Safes. All safes must have a USNA number and must display the Security Container Check Sheet (SF 702), enclosure (10). The Security Container Check Sheet must be posted for *easy access*. A divisional double-check procedure, using a second person for the "checked-by" column on the Security Container Check Sheet, must be employed when securing any safe. If you are the last person in the area and cannot locate another individual to double check your safe, call the Duty Officer and *ask* for his/her assistance in securing the container. If a safe is reopened, such as for stowage of a last-minute paper, all of the foregoing must be repeated.

6. Security Inspections. Division Directors/Department Heads and NSA Installation Program Directors will instruct building duty officers of their responsibility for conducting daily inspections of spaces for possible security violations and to assess physical security conditions.

JUN 6 2008

a. Unsecured Safes. If a container with classified material is found unattended/opened, the discoverer is to leave items intact and under guard and call the responsible custodian to the *scene* immediately (even outside normal working hours). If there is any possibility of compromise, the custodian of the safe must conduct an immediate inventory of all classified material in the container.

b. If a loss is discovered notify the Assistant Security Manager.

7. Loss, Compromise, and Other Security Violations. Individuals who become aware of a loss, compromise, or possible compromise of classified information must notify the Assistant Security Manager immediately. All security violations are serious and must be promptly reported and investigated and the causes of the violation immediately corrected. There are two types of security violations: one results in compromise of classified information; the other, security regulations are violated but no compromise occurs. Compromise is the disclosure of classified information to unauthorized persons. Compromise presents the greater threat to national security, but other security violations are serious because they demonstrate vulnerable areas in our security program.

a. When a probable loss is reported, the Assistant Security Manager will conduct a preliminary inquiry within three working days and notify the cognizant NCIS Office who will accept or decline investigative jurisdiction. The preliminary inquiry must:

(1) Determine the circumstances surrounding the incident.

(2) Identify the responsible individual(s).

(3) Identify *all* witnesses to the violation after consultation with NCIS personnel. The local Staff Judge Advocate will interview the witnesses to determine the extent of the violation.

(4) If possible, identify the individual(s) responsible.

(5) Make an attempt to discover the weaknesses in security procedures that allowed the loss, compromise, or possible compromise to occur.

(6) Establish the following:

(a) That a loss or unauthorized disclosure of classified information did not occur.

(b) That a loss of control of classified material occurred but there are no indications of actual loss, compromise, or possible compromise of classified material.

(c) That compromise may have occurred but under conditions presenting a minimal threat to national security based on initial impact statement confirmed, or that the probability of damage to the national security cannot be discounted (compromise of *Top Secret* or *Secret* cannot be determined to be minimal impact).

(d) It is determined that a compromise is confirmed and the harm to national security cannot be discounted.

(e) That punitive disciplinary action will occur as a result of the incident.

b. If harm to national security is determined, significant security weaknesses are revealed, and punitive disciplinary action is contemplated, the NCIS office originally notified will be informed and a JAGMAN investigation will be initiated.

c. Disciplinary action taken against individuals found culpable for security violations will suit the offense and be applied regardless of rank, rate, or grade.

JUN 6 2008

d. The Superintendent or Commanding Officer NSA Annapolis, as appropriate, shall review all completed inquiries and investigations to ensure the reports are complete and that appropriate action has been taken.

**CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT**

JUN 6 2008

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.)*

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 <i>(See Notice below)</i>
-----------	------	---

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

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

**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 <i>(Type or print)</i>	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.

**VISIT REQUEST**

PRIVACY ACT STATEMENT ON PAGE 2.

USNAINST 5510.8A

JUN 6 2008

VISITOR CLEARANCE DATA

OPNAV 5521/27 (Rev. 1-75) S/N 0107-LF-055-2235

**CHECK ONE**

REPLY REQUIRED

REPLY ONLY IF NEGATIVE

(SEE CURRENT EDITION OF OPNAVINST.5510.1 FOR DETAILED INSTRUCTIONS)

FROM (COMPLETE ADDRESS OF REQUESTING ACTIVITY)		DATE OF REQUEST
TO (NAME AND ADDRESS OF VISITING ACTIVITY)		SPECIFIC PERSONNEL OR SECTION OF COMMAND TO BE VISITED
_____ FOLD ON THIS LINE _____		
DURATION OF VISIT (ARRIVE)	(DEPART)	DEGREE OF ACCESS REQUIRED
PURPOSE OF VISIT/REMARKS (IF THE VISIT IS TO A CONTRACTOR FACILITY, INCLUDE CONTRACT NUMBER IF APPROPRIATE)		

NAME, RANK, TITLE OR POSITION, SOCIAL SECURITY NO.	DATE AND PLACE OF BIRTH	NATIONALITY (CHECK ONE)	LEVEL OF SECURITY CLEARANCE
		<input type="checkbox"/> U.S. CITIZEN	
		<input type="checkbox"/> IMMIGRANT ALIEN	
		<input type="checkbox"/> U.S. CITIZEN	
		<input type="checkbox"/> IMMIGRANT ALIEN	
		<input type="checkbox"/> U.S. CITIZEN	
		<input type="checkbox"/> IMMIGRANT ALIEN	
		<input type="checkbox"/> U.S. CITIZEN	
		<input type="checkbox"/> IMMIGRANT ALIEN	
		<input type="checkbox"/> U.S. CITIZEN	
		<input type="checkbox"/> IMMIGRANT ALIEN	

NAME, RANK AND TITLE OF OFFICIAL AUTHORIZING VISIT AND CLEARANCE	SIGNATURE
--	-----------

COPY TO \_\_\_\_\_

JUN 6 2008

**PRIVACY ACT STATEMENT**

AUTHORITY: E.O. 11652

PRINCIPAL PURPOSE: Information is obtained to identify personnel visiting activities when such visits are expected to involve access to classified information.

ROUTINE USE: Information provided in the form, when compared with information known to or normally in the possession of an individual, is used in determining whether or not an individual is who he purports to be when visiting an activity. The information may be disclosed to all those charged at the activity with making the foregoing determination.

DISCLOSURE: (Mandatory or voluntary; consequences, etc.): Completion of OPNAV 5521/27, including the disclosure of your Social Security Number, is voluntary. Failure on your part, however, to answer all questions, or any misrepresentation (by omission or concealment, or by misleading, false, or partial answers), may serve as a basis for denial of the request to visit, or for access to information classified in the national interest pursuant to E.O. 11652.

JUN 6 2008

# TOP SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT WILL BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

# TOP SECRET



703-101  
NSN 7540-01-213-7901

STANDARD FORM 703 (8-85)  
Prescribed by GSA/ISOO  
32 CFR 2003

JUN 8 2008

# SECRET

**THIS IS A COVER SHEET**

**FOR CLASSIFIED INFORMATION**

**ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.**

**HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.**

**(This cover sheet is unclassified.)**

# SECRET

704-101  
NSN 7540-01-213-7902

**STANDARD FORM 704 (8-85)**  
Prescribed by GSA/ISOO  
32 CFR 2003

# CONFIDENTIAL

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

# CONFIDENTIAL

705-101  
NSN 7540-01-213-7903

STANDARD FORM 705 (8-85)  
Prescribed by GSA/ISOO  
32 CFR 2003

## SECURITY DISCREPANCY NOTICE

JUN 6 2008

FROM		DATE	
REF a. _____ <i>(Insert ref. (a))</i>		b. OPNAVINST 5510.1 SERIES	
ENCL			
TO: [ ]		(Note - This form may be mailed in a window envelope.)	
<p>1. Reference (a) has been found to be inconsistent with or in contravention of reference (b) for the reason(s) checked below.</p> <p>2. If applicable, corrective action should be taken and where this involves changing classification, all holders of reference (a) should be notified accordingly.</p>			
<b>IMPROPER TRANSMITTAL/PACKAGING</b>			
SENT VIA NON-REGISTERED/ NON-CERTIFIED MAIL		CLASSIFICATION NOT MARKED ON INNER CONTAINER	RECEIVED IN POOR CONDITION; COMPROMISE IMPROBABLE
SENT IN SINGLE CONTAINER		NO RETURN RECEIPT	ADDRESSED IMPROPERLY
MARKINGS ON OUTER CONTAINER DIVULGE CLASSIF. OF CONTENTS		INADEQUATE WRAPPING, NOT SECURELY WRAPPED OR PROTECTED	OTHER <i>(Specify)</i>
<b>CLASSIFICATION</b>			
BASIC CLASSIFICATION QUESTIONABLE		DOCUMENT SUBJECT MARKING	CHART, MAP OR DRAWING MARKING
OVERALL MARKINGS		DOCUMENT TRANSMITTAL MARKING	PHOTO, FILM OR RECORDING MARKING
PARAGRAPH/COMPONENT MARKINGS		MESSAGE MARKING	OTHER <i>(Specify)</i>
<b>DOWNGRADING/DECLASSIFICATION</b>			
CLASSIFICATION AUTHORITY NOT IDENTIFIED OR UNAUTHORIZED		DOWN GRADING DATA INCORRECT	DECLASSIFICATION (OR REVIEW) DATA OMITTED OR INCORRECT
OTHER <i>(Specify)</i>			
<i>Fold here ↑ with face of form in view</i>			
COMMENTS <i>(Continue on reverse, if necessary)</i>			
COPY TO: N-009D (WITH ADDRESSEE DELETED)			
SIGNATURE		TITLE	

JUN 6 2008

SAMPLE



JUN 6 2008

<b>SECURITY CONTAINER INFORMATION</b> 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. 10. Immediately notify one of the following persons, if this container is found open and unattended.		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 HOME PHONE
EMPLOYEE NAME HOME ADDRESS		HOME PHONE

**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

**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

