DEPARTMENT OF THE NAVY
OFFICE OF THE JUDGE ADVOCATE GENERAL
1322 PATTERSON AVENUE SE, SUITE 3000
WASHINGTON NAVY YARD DC 20374-5066

IN REPLY REFER TO:

JAG/CNLSCINST 5510.30
Code 30
29 Nov 11

JAG/COMNAVLEGSVCCOMINST 5510.30

From: Judge Advocate General
Commander, Naval Legal Service Command

Subj: PERSONNEL SECURITY AND CLASSIFIED INFORMATION PROGRAM

Ref: (a) SECNAV M-5510.30, Department of the Navy Personnel Security Program
(b) SECNAVINST 5510.30B
(c) SECNAV M-5510-36, DON Information Security Program
(d) SECNAVINST 5510.36A
(e) DOD 5200.1-R, DOD Information Security Program, January 1997
(f) DOD 5200.2-R, DOD Personnel Security Program, January 1987
(g) E.O. 13526
(h) E.O. 12968
(i) E.O. 10450
(j) OPNAVINST 5530.14E
(k) DOD 5200.08-R, DOD Physical Security Program, April 2007
(l) E.O. 13488
(m) NSAW ltr Ser N00/126 of 14 Jun 2011
(n) DOD Directive 5220.6 of 2 Jan 1992
(o) Defense Industrial Personnel Security Clearance Review Program

Encl: (1) Responsibilities of Centralized Personnel in Conjunction with Security Programs
(2) Security Department Program Management
(3) Area Security
(4) Security Requirements Peculiar to OJAG and NLSC
(5) Security Awareness and Education Program
(6) Foreign Travel Briefings
(7) Limited Access Authorizations and Access to Individuals Outside of the Command
(8) Continuous Evaluation
(9) Granting Security Clearances, Adjudicative Agencies and Adjudicative Guidelines
(10) Loss or Compromise of Classified Information Spillage

(11) Original Classification Authority Classification Management
(12) Control, Reproduction, Dissemination, Safeguarding and Disposal of Classified Material
(13) Locking Procedures for Securing Storage Containers
(14) Industrial Security Programs
(15) Security Review
(16) Sensitive and Information Technology Positions/Personnel Security Investigations
(17) Personnel Security Clearances and Access
(18) Security Office Customer Service Hours and Phone Numbers
(19) Designation of Security Managers/Officers Template

1. Purpose. This instruction establishes and implements Information, Personnel and Physical Security Programs for the Office of the Judge Advocate General (OJAG) and Commander, Naval Legal Service Command (CNLSC) in accordance with references (a) through (o). The command's internal procedures cover access to classified information or assignment to sensitive duties and identify the process for handling, safeguarding and maintaining classified information. This publication does not replace and must be used in conjunction with references (a) through (o) relating to security programs.

2. Responsibilities.

a. Judge Advocate General (JAG) and Commander, Naval Legal Service (NLSC) are responsible for effective management of the Information, Personnel and Physical Security Programs.

b. The OJAG/NLSC Security Program Director is responsible to the Commander for security program oversight and management, including implementation of and program compliance.

c. Command Security Managers are responsible for notifying the Security Office within 30 days when the level of security requirements change within their area(s) of responsibility.

d. On an annual basis or as directed upon regulatory compliance notification, Security Office personnel will review the policies and procedures of this publication and make required changes as necessary.

4. Applicability.

a. This instruction is applicable to all military and civilian personnel employed by or at OJAG or NLSC Headquarters. All personnel with access to classified information must protect the material in accordance with the guidelines set forth in this instruction and its references.

b. Where contractor personnel are involved, OJAG and NLSC must adhere to the provisions of the Industrial Security Regulation (ISR), and contractor personnel must adhere to the provisions of the Industrial Security Manual (ISM) and any additional security regulations specified by the employing command.

c. This instructional may be used by NLSC field sites only if processes contained herein are applicable to their site. Otherwise, they must establish an Information, Personnel and Physical Security Program Manual that specifically meets the needs and requirements unique to their individual site. All Security Program Manuals must be written in accordance with references (a) through (l).

5. Action.

a. All OJAG and NLSC civilian, military and contractor personnel shall comply with the provisions of this security program and supervisors must ensure employee awareness and procedural compliance.

b. The OJAG/NLSC Security Program Director shall direct and monitor all aspects of the Information, Personnel and Physical Security Programs.

c. The OJAG/NLSC security management basic policy qualifications, duties, responsibilities and requirements, including designation letters, are outlined in Chapter 2 of references (a) and (c). All designation letters must be on file in the NLSC Security Office. Enclosure (19) is a sample copy of the Designation of Security Managers/Officers.

d. Program requirements and protective measures must be implemented to provide an effective security posture.

e. Provisions of this instruction are effective immediately. Specific or unique security problems that are not specifically covered by this instruction shall be referred to

the OJAG/NLSC Security Program Director for resolution. Copies of all activity Information, Personnel and Physical Security Program designations, publications, and servicing agreements shall be forwarded to the NLSC Security Program Director, as promulgated.

6. Violations of this Instruction. Personnel may be subject to disciplinary action, criminal penalties or administrative sanctions if they knowingly, willfully or negligently violate the provisions for protecting and safeguarding classified or sensitive information.

NANETTE DERENZI
Rear Admiral, JAGC, U.S. Navy
Commander, Naval Legal Service Command

JAMES W. HOUCK
Vice Admiral, JAGC, U.S. Navy
Judge Advocate General

Distribution:
Electronic only, via Navy Directives website, http://doni.daps.dla.mil; and the OJAG website, http://www.jag.navy.mil.

RESPONSIBILITIES OF CENTRALIZED PERSONNEL IN CONJUNCTION WITH SECURITY PROGRAMS

1. GENERAL. No person shall be appointed, accepted or retained as a civilian or contractor employee in OJAG/NLSC, granted access to classified information, or assigned to other sensitive duties that are subject to investigation under the provisions of reference (a) unless appointment, acceptance, retention, clearance or assignment is clearly consistent with the interests of national security.

2. HUMAN RESOURCE AND PERSONNEL SECURITY SUPPORT

a. Civilian Personnel. The OJAG/NLSC Security Office provides Information and Personnel Security support to civilian personnel assigned to OJAG or NLSC.

b. Contractor Personnel

1. The designated Contracting Officer Representative (COR) is the liaison for contracts between OJAG/NLSC and companies for contractor personnel and their employment.

2. The COR provides a Statement of Work to OJAG/NLSC Security Office that identifies duties to be performed and the level of clearance required.

3. The OJAG/NLSC Security Manager completes a DoD Contract Security Classification Specification (DD Form 254) for all contractors working on a classified contract.

4. The Security Program Director will verify the contractor's eligibility. If the JPAS record shows "No Determination Made," a CAC cannot be issued and the person will not be allowed to work on an OJAG or NLSC contract, unless the command can make a favorable determination from the Personnel Security Investigation results. Reference (1) contains guidance for such determinations. The authority to establish criteria for making fitness determinations remains within the discretion of the Commander. The Commander must use the criteria for making fitness determinations equivalent to suitability standards established by the Office of Personnel Management (OPM) and shall take into account OPM guidance when exercising this discretion.

5. If a contractor does not require a CVS/CAC for a NMCI or DON account, their access control will be subject to

RAPIDGate Program Enrollment. Reference (m) contains access control changes, procedures and information on RAPIDGate Program Enrollment for Naval Support Activity Washington (NSAW), effective 1 July 2011. These procedures will directly impact vendors, contractors, sub-contractors and service providers who regularly access NSAW installations. NSAW's priority is to maintain a safe and secure installation while offering a solution for streamlining access. Reference (m) contains specific details on how to gain streamlined access onto the installations.

6. The OJAG/NLSC Security Office initiates the personnel security investigations for contractor personnel assigned to OJAG or NLSC, if and when the appropriate investigation has not been initiated by the contracting company.

c. Military Personnel. Military personnel are assigned to NLSC under military orders and are under the jurisdiction of the military service. The OJAG/NLSC Security Office provides Personnel Security Program support for military personnel assigned to OJAG or NLSC, as required by their military orders.

3. HUMAN RESOURCE AND PERSONNEL SECURITY OFFICE RESPONSIBILITIES

a. The following procedures must be accomplished before a civilian can be officially offered and appointed to a position. This includes new Federal employees and transfer employees from other DoD facilities.

(1) The Fiscal and Resources Services Division (Code 64) will forward candidate's security paperwork to OJAG/NLSC Security Office.

(2) The OJAG/NLSC Security Office will review security paperwork and candidate's JPAS record (if one is on file) for type and date of current Personnel Security Investigation and the eligibility determination that was made by the adjudicating agent, and they will make a suitability determination based on their findings. The OJAG/NLSC Security Office will then determine and identify requirements on new federal employees.

(3) During the review process, as required, OJAG/NLSC Security Office will request a copy of the position description from Code 64, check and review position sensitive designation/security requirements.

e. Upon receipt of the position description, the OJAG/NLSC Security Office will check the duties against the criteria for designating sensitive positions that is identified in Chapter 5 of reference (a).

f. If a Personnel Security Investigation is required, the OJAG/NLSC Security Office will follow the standards identified in Chapter 6 of reference (a) to determine those investigative requirements.

g. The OJAG/NLSC Security Office will initiate and submit required security forms via e-QIP, using those specific guidelines, to the Office of Personnel Management for conduct of the appropriate Personnel Security Investigation.

SECURITY DEPARTMENT PROGRAM MANAGEMENT

1. ORGANIZATION. The OJAG/NLSC Security Office is responsible for planning, organizing, implementing, and executing the Information, Personnel and Physical Security Program operations for OJAG/NLSC.

2. PROGRAM MANAGEMENT RESPONSIBILITY

a. Security Program Director. The Security Program Director (synonymous with Security Manager) will be appointed by name in writing. The Security Program Director manages and oversees the Information, Personnel and Physical Security Programs at OJAG and NLSC.

b. Assistant Security Manager. The Assistant Security Manager will be appointed by name in writing. The Assistant Security Manager oversees the Information, Personnel and Physical Security Programs in the absence of the Security Program Manager.

c. Top Secret Control Officer (TSCO). The Top Secret Control Officer will be appointed by name in writing. The TSCO duties are carried out by the Security Program Director.

3. **PROGRAM COMPLIANCE.** Program Management of the Information, Personnel and Physical Security Programs will be implemented and adhere to the instructions set forth in this instruction and in accordance with references (a) through (k). Program compliance will be strictly enforced throughout the command.

4. PROVISIONS AND RESPONSIBILITIES

a. The following provisions are in place to constantly monitor security programs to assure procedures are up to date and that they meet the security needs of command, as well as the procedures for internal and subordinate security reviews and inspections:

(1) The OJAG/NLSC Security Office uses a Security Inspection Checklists to ensure Information, Personnel, and Physical Security program compliance and required updates are incorporated into procedural process, as required.

(2) OJAG and NLSC follows the guidelines in references (a) - (i) concerning the development of local security requirements for classification management, accountability,

control, safeguarding/ storage, reproduction, declassification and destruction of classified information, as well as the internal controls set forth in this manual.

AREA SECURITY

1. GENERAL

a. Different areas of OJAG/NLSC require different degrees of security protection. Areas requiring protection of sensitive, critical, classified material, mission essential resources, high value storage areas, and other areas where positive control is essential are designated as restricted areas.

b. Restricted areas are off limits and only authorized personnel are allowed access. Unauthorized personnel found within restricted areas will be detained and the purpose of their presence will be established before they are released.

c. Restricted areas are designated, established, and controlled in accordance with reference (j).

d. A restricted area is established to provide the following:

(1) Effective application of necessary security measures and exclusion of unauthorized personnel.

(2) Intensified controls over those areas requiring special inspection.

(3) Conditions for protection/safeguarding of classified information, mission essential material/information, sensitive or critical assets or articles having a high likelihood of theft with minimum impact on operations.

2. RESTRICTED AREAS REQUIRING PROTECTION

a. The OJAG/NLSC restricted areas have been established and designated as follows:

(1) Security Office

(2) Security Office Strong Room

(3) OJAG/NLSC Mailroom

4. RESTRICTED AREA SIGNS. Restricted Area signs are posted on all rooms listed above, except the OJAG/NLSC Mail Room has an "Authorized Personnel Only" sign posted. OJAG/NLSC shall

strictly enforce applicable security controls for all restricted areas.

5. POSTING RESTRICTED AREA SIGNS

a. All restricted areas shall be posted simply as restricted areas so as not to single out or draw attention to the importance or criticality of an area.

b. The OJAG/NLSC Headquarters restricted area signs are red background with white lettering and read as follows:

WARNING
RESTRICTED AREA - KEEP OUT
AUTHORIZED PERSONNEL ONLY
AUTHORIZED ENTRY INTO THIS RESTRICTED AREA
CONSTITUTES CONSENT TO SEARCH
OF PERSONNEL AND THE PROPERTY
UNDER THEIR CONTROL
INTERNAL SECURITY ACT OF 1950
SECTION 21: 50 U.S.C. 797

6. PROHIBITED ITEMS IN RESTRICTED AREAS

a. The following items ARE NOT ALLOWED beyond the entrance door of those rooms marked with an asterisk above.

(1) Personal Electronic Devices

(a) Cell Phones

(b) Blackberries

(c) Cameras

(2) USB Flash or Thumb Drives

(3) Personal Data Assistants

b. Additionally, all forms of removable media devices (CD/DVD, flash drives, etc.) on SIPRNET are forbidden. Printed/hard copy documents and email communication are the only authorized forms of SIPRNET transmissions, and that material must be hand-carried and recorded in the Security Office Record Book.

c. In accordance with NETWARCOM Communications Tasking Order 10-25 Protecting Classified Information on DoD SIPRNET, the removable media is prohibited from use on all SIPRNET servers, systems unless specifically authorized and justified as an operational necessity by organizational leadership. The command will assign a Removable Media Representative (RMR) and all exceptions to the policy must be approved by the RMR.

SECURITY REQUIREMENTS PECULIAR TO OJAG AND NLSC

1. VISITOR CONTROL

a. Visitor Control requirements are accomplished with the following actions:

(1) Prepare Visit Request Notifications

(2) Submit Visit Requests

(3) Receive Visit Requests

(4) Receive Visitors After Approval of Visit Request

b. Personnel must adhere above processes to enforce visitor control within OJAG or NLSC spaces.

2. SECURITY REVIEWS AND INSPECTIONS

a. The OJAG/NSLC Security Office is responsible for in house inspections of the Personnel and Classified Information Security Programs. The Security Office staff is responsible for the following:

(1) OJAG/NLSC Security Programs Director will conduct inspections, assists visits and reviews to examine the subordinate commands' overall security posture.

(2) Conducting in-house inspections of the Personnel, Information and Physical Security Programs, utilizing the Article 6 Inspection checklist.

(3) Conducting annual inventories of both COMSEC material and Top Secret materials (if applicable).

3. BUILDING SECURITY, INTRUSION DETECTION AND BADGING SYSTEM

a. OJAG and NLSC Headquarters is protected by an "Access IT! Universal" access control security system that provides a more secured working environment for all personnel. It is a computer based system with a stand-alone file server protected by Uninterrupted Power Supply and back-up batteries, and it is located in the NAVFAC Security Office.

b. The security system is designed with a badging system to control personnel and visitor access into the building and workspaces, and has an intrusion detection and surveillance camera system to serve as an aid in protecting assets and equipment from potential theft. Building access is established and granted based on the civilian, military and contractor requirements for access. The badge is government property and the badge holder will surrender it upon request of OJAG/NLSC Security Office, or upon termination, retirement, voluntary separation or departure from OJAG/NLSC.

c. All exterior doors to OJAG and NLSC spaces are secured by an Electronic Access Card (EAC). However, the Patterson Street and adjacent Court Yard doors are not secured Monday - Friday from 0600 - 1800 (with the exception of holidays) to allow ease of movement for personnel, visitors and vendors.

d. All security system alarms are monitored, reviewed and acknowledged by OJAG/NLSC Security Office staff during work hours. Certain intrusion detection alarms are monitored and responded to by the Naval District Washington Police Force during and after work hours, including weekends and holidays.

e. The security system contract representative is notified within 2 hours of the Security Office making a determination that system problems cannot be resolved by NAVFAC staff.

SECURITY AWARENESS AND EDUCATION PROGRAM

1. OJAG/NLSC SECURITY OFFICE RESPONSIBILITIES. Monitor the Security Education Program for all OJAG and NLSC personnel. Provide briefings in security procedures and responsibilities listed in section 8-3 below in accordance with Chapter 4 of reference (a).

2. MANDATORY SECURITY BRIEFINGS

a. Indoctrination/Orientation. The OJAG and NLSC Initial Security Indoctrination briefing is provided when new personnel check-in with the Security Office.

b. Refresher briefings

c. Special briefings:

(1) Foreign Travel Briefings

(2) New Requirement Briefing

(3) Program Briefings

(4) NATO Security Briefing

(5) Command Debriefing

(6) Security Termination Statement (Exhibit 4 A of reference (a))

(7) Training for Security Personnel

(8) Security Awareness

3. REQUIREMENTS FOR ACCESS TO CLASSIFIED INFORMATION

a. Prior to granting access to classified information, all personnel must:

b. Be cleared for appropriate level of access;

c. Be briefed on the requirements of handling and safeguarding classified information:

(1) Personnel must read and sign a Standard Form (SF) 312 Classified Information Nondisclosure Agreement, witnessed by a

security official. Refusal to sign the agreement will be grounds for denial of access to classified information. The SF 312 form is contained in Exhibit 4 A of reference (a).

(2) An oral attestation is required and administered when the access level is Top Secret or higher.

4. WHEN ACCESS IS NO LONGER REQUIRED

a. Upon termination/separation of employment, administrative withdrawal of security clearance, or contemplated absence from duty or employment for 60 days of more, those personnel granted a security clearance shall:

b. Be given a security debriefing:

(1) Read and sign Security Debriefing Acknowledgement, SF 312.

(2) Read and sign Security Termination Statement, when applicable.

(3) Return all classified material to the Security Office.

5. COUNTERINTELLIGENCE BRIEFINGS

a. Briefings are conducted when required.

b. These briefings will be conducted by the Naval Criminal Investigative Service (NCIS).

6. TRAINING FOR SECURITY MANAGERS. OJAG Division Directors and NLSC Commanding Officers shall ensure that newly designated Security Managers receive adequate training within 6 months of initial appointment.

7. SPECIALIZED TRAINING

a. Derivative Classification.

(1) Personnel must report their documents as derivative classification when incorporating, paraphrasing, restating, or generating, in new form, information that is already classified. They must mark the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of

information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification. Persons who apply derivative classification markings shall observe and respect original classification decisions and carry forward to any newly created documents any assigned authorized markings.

(2) The OJAG/NLSC Security Office may provide advice, assistance and training to those personnel working with derivative classification. Reference (c), Chapter 4, paragraph 4-9 covers derivative classifiers and classification.

b. Original Classification Authority (OCA). Director of Security Programs is responsible for providing annual OCA training to JAG and CNLSC. For further guidance, see Chapter 4 of reference (c).

c. Classification Couriers. OJAG and NLSC will follow the specialized training procedures listed in reference (c), Chapter 9, paragraph 9-11.5.

d. Declassification Authorities. This function is performed by OJAG/CNLSC, SECNAV or the DoN (OCA). OJAG/NLSC Security Managers, Security Specialists or any other personnel whose duties significantly involve management and oversight of classified information ARE NOT authorized as Declassification Authorities. Reference (c), Chapter 4, paragraph 4-19 covers guidance for declassification authorities.

FOREIGN TRAVEL BRIEFINGS

1. REQUIRED FOREIGN TRAVEL BRIEFINGS AND TRAINING

a. The OJAG/NLSC Security Office has posted the Foreign Travel Briefings and pertinent information on the Security Office NKO Portal. Prior to travel (30 days in advance), personnel who travel outside the U.S. on official or personal business will be required to access the OJAG/NLSC Portal and read the briefing material. Additionally, they must check the DOD Electronic Foreign Clearance Guide and state government web site for the country they are visiting. This is necessary in order to check country specific conditions and the threat level for safety aspect, etc. This information is beneficial to the individual, as well as National Security. It alerts personnel of possible exploitation and hazards that may be encountered while traveling to or through foreign countries or attending or hosting meetings of foreign visitors. Personnel must check the Personnel Entry Requirements for Official Travel and complete the clearance requirements for the country they are visiting.

b. Individuals who travel frequently, attend or host meetings of foreign visitors, need not be briefed for each occasion. However, they shall be provided a thorough briefing at least once every 6 months and a general reminder of security responsibilities before each such activity.

c. Prior to foreign travel, personnel must notify the Security Office, and provide an email listing their personal and travel information. They must check that they have completed Training/Force Protection Requirements as follows:

(1) Antiterrorism Force Protection (AT/FP) Level 1 Training (within 12 months of travel).

(2) Survival, Evasion, Resistance, and Escape (SERE) Code of Conduct Level B Training (within 24 months of travel) (if required by country).

(3) Isolated Personnel Report (ISOPREP) (Form DD 1833) (one time requirement) (if required by country).

(4) AT Plan (Form) (New plan for each trip if required by country).

d. In addition to the above, an individual should register on line with the U.S. Department of State through the Smart

Traveler Enrollment Program (STEP). This is a free service provided by the U.S. Government to U.S. citizens who are traveling to, or living in, a foreign country. STEP allows an individual to enter information about their upcoming trip abroad so that the Department of State can better assist them in an emergency. STEP also allows Americans residing abroad to get routine information from the nearest U.S. embassy or consulate.

LIMITED ACCESS AUTHORIZATIONS
AND
ACCESS TO INDIVIDUALS OUTSIDE OJAG AND NLSC

1. **AUTHORIZATIONS** Limited Access Authorizations for non U.S. citizens. Access will be handled in accordance with paragraph Chapter 9, section 9-15 of reference (a) and Appendix A, page A-10 of reference (a).

2. **ACCESS APPROVAL.** Access to Classified Information to Individuals outside OJAG and NLSC. Before granting classified material access to any person outside OJAG and NLSC, the action shall be cleared with the OJAG/NLSC Security Program Director in accordance with procedures contained in Chapter 9, reference (a).

3. **ACCESS FOR CIVILIAN DEFENSE COUNSEL AND OTHER PERSONNEL INVOLVED IN LEGAL PROCEEDINGS.** The Director of Security Programs will coordinate all requests for civilian defense counsel and witness access.

CONTINUOUS EVALUATION

1. GENERAL. Eligibility for access to classified information and/or material, or assignment to other sensitive duties shall be based on a determination and continued evaluation of the person's loyalty, reliability and trustworthiness. This overall, common sense determination will be based on all available information.

2. RESPONSIBILITIES FOR REPORTING DEROGATORY INFORMATION

a. Personnel Security responsibilities do not stop once a security clearance is granted. When an employee has access to classified information, supervisors are encouraged to address employee security concerns, unfavorable information, or questionable behavior immediately to the OJAG/NLSC Security Office. Any information which could place an individual's loyalty, reliability, judgment or trustworthiness in question has to be evaluated from a security standard.

b. OJAG/NLSC will follow the policy/procedures in Chapter 10 of reference (a) for reporting employee security concerns/issues. The OJAG/NLSC Security Office will report the information to DONCAF for evaluation and a personnel security determination.

c. Security is everyone's responsibility; therefore, all employees should notify the Security Office of any derogatory information as it arises or any suspicious behavior from anyone, including co-workers and managers.

d. Exhibit 10A of reference (a) is a Continuous Evaluation Check Sheet that contains a list of security issues that must be reported to the Department of Navy Consolidated Adjudications Facility (DONCAF).

3. CRIMINAL CONDUCT AND ARRESTS AFTER CLEARANCE IS GRANTED

a. OPM sends out notifications to the OJAG/NLSC Security Office regarding an employee's arrest and/or unlawful act/criminal offense. Upon receipt of the OPM notification, OJAG/NLSC Security Office will forward it to DONCAF for a personnel security determination.

b. Criminal conduct or unlawful acts may affect the employee's security clearance eligibility. That determination will be made by the DONCAF.

GRANTING SECURITY CLEARANCES, ADJUDICATIVE AGENCIES AND ADJUDICATIVE GUIDELINES

1. SECURITY CLEARANCES

a. Access to classified information is granted by OJAG/NLSC Security Office at the minimum level of access that is required to perform official duties, only after the Personnel Security Investigation (PSI) has been favorable adjudicated (at or above the same level of clearance) by the applicable adjudication agency listed in 15-2 below.

b. Upon submission of a PSI to OPM, the OJAG/NLSC Security Office may grant temporary access/interim clearances to civilian personnel pending completion and favorable adjudication of their investigation. However, temporary access/interim clearances will be granted only in "no issue" cases.

c. The Defense Industrial Security Clearance Office (DISCO) grants interim clearances to contractor personnel.

2. ADJUDUCATIVE AGENCIES

a. Upon completion of a PSI by OPM, DONCAF adjudicates the investigation and other relevant information to determine eligibility for security clearance or assignment to sensitive duties for both OJAG/NLSC civilian and military personnel. DONCAF also is the authority for denying or revoking OJAG/NLSC civilian and military clearances.

b. Once DONCAF determines the eligibility for security clearances or assignment to sensitive duties, they record their determinations in JPAS and a notification is populated to the appropriate SMO/agency.

c. DISCO is the authority for granting or denying contractor security clearances.

d. DONCAF is the authority for making suitability determinations for contractors for no access requirements.

e. The local civilian personnel office makes suitability determinations for civilians occupying non-sensitive positions.

3. ADJUDICATIVE GUIDELINES AND DOD DIRECTIVES

a. There are 13 Adjudicative Guidelines that apply to all personnel security adjudications and other determinations made under Department of Defense (DOD) directives. The DOD directives and Adjudicative Guidelines are as follows:

(1) DOD Directives:

(a) Department of Defense Directive (DODD) 5220.6, January 2, 1992

(b) Defense Industrial Personnel Security Clearance Review Program

(c) DOD Personnel Security Program, DOD 5200.2-R, January 1, 1987

(2) The 13 Adjudicative Guidelines are addressed in reference (a), Appendix G.

b. Although there are mitigating factors for the 13 Adjudicative Guidelines, all employees should provide truthful and candid answers when completing their security forms and they should cooperate with security official throughout the security clearance process. Failure to do so normally will result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility.

LOSS OR COMPROMISE OF CLASSIFIED INFORMATION AND ELECTRONIC SPILLAGE

1. GENERAL

a. OJAG and NLSC personnel will follow the basic policy, procedures and reporting requirements identified in reference (c), Chapter 12 for loss or compromise of classified material and spillage.

b. Public media compromises of classified information will be handled in accordance with reference (c), Chapter 12, Section 12-18.

c. Incidents involving improper transmissions of classified information will be handled in accordance with reference (c), Chapter 12, Section 12-19.

2. UNLOCKED SECURITY CONTAINERS

a. **After Duty Hours**: If a security container is found open or unlocked and it cannot be secured, the command Duty Officer immediately calls a member of the Security Office staff. The container shall be guarded until the Security Office staff member arrives at the location of the unlocked security container. If the Duty Officer and Security Office staff members finds evidence that classified information has been compromised, the responsible custodian will be required to return to the office to make a report and conduct an inventory of the material. The command Duty Officer shall immediately prepare a separate report of findings and it shall be delivered to the Security Manager the following workday. If the Duty Officer and the Security Office staff does not find evidence of compromise, he/she shall lock and seal the container with tape and make a Security Violation Report to be forwarded to the Security Manager the following workday.

b. **During Duty Hours**: Should any container used to store classified information be found unlocked in the absence of responsible custodian, the OJAG/NLSC Security Manager shall be notified immediately. The individual reporting the incident shall guard the container until the arrival of the Security Manager and responsible custodian. If upon inspection of the container, the possibility of compromise is considered to exist, an immediate inventory of classified material stored therein will be conducted. Otherwise, the safe shall be secured and action taken as indicated above

3. RESPONSIBILITIES

a. Violations or regulations pertaining to the safeguarding of classified information not resulting in compromise shall be acted upon by the JAG or CNLSC.

b. The Commander will determine the type of corrective or disciplinary action.

c. Examples on this category include unsecured containers, improper transmission, and unauthorized reproduction wherein there is no compromise of material.

4. REPORTING VIOLATION TO NLSC SECURITY MANAGER

a. A sanitized memorandum report of all security violations shall be forwarded to the OJAG/NLSC Security Manager.

b. The report will include:

(1) Date of violation;

(2) Type of violation;

(3) Corrective action taken; and

(4) Disciplinary action taken.

ORIGINAL CLASSIFICATION AUTHORITY/CLASSIFICATION MANAGEMENT

1. STATEMENT

a. The JAG and CNLSC have been delegated as the Original Classification Authority.

2. GENERAL

b. The formulation and maintenance of an effective, realistic, and responsive security classification management program, as an integral part of the DOD Information Security Program, is essential in the interest and protection of national security and is handled by OPNAV in accordance with Chapter 4 of reference (c).

c. OJAG and NLSC's responsibility is to handle and safeguard/protect classified material and information against unauthorized disclosure in the interests of national security.

3. THREE LEVELS OF CLASSIFIED MATERIAL

a. National Security Information requiring protection against unauthorized disclosure is classified in one of three categories as follows:

(1) Top Secret

(2) Secret

(3) Confidential

CONTROL, REPRODUCTION, DISSEMINATION, SAFEGUARDING AND DISPOSAL OF CLASSIFIED MATERIAL

1. CONTROL OF CLASSIFIED MATERIAL

a. Procedures and requirements for the control of classified documents are as follows and shall be strictly observed:

(1) Top Secret Material.

(a) All OJAG and NLSC personnel requiring access to and/or handling Top Secret material must:

(1) Be properly cleared and granted Top Secret access;

(2) Sign a SF 312;

(3) Do a Personal Attestation Upon the Granting of a Security Clearance and/or Access; and

(4) Be listed on the local access roster and authorized to handle Top Secret material within OJAG or NLSC and have a requisite "need to know."

(b) Top Secret material shall not be removed from NLSC without the express written approval of the OJAG/NLSC TSCO.

(c) Top Secret material shall not be processed through Secondary Control Points. Individual users must obtain material from the OJAG/NLSC Security Office.

(d) Top Secret material shall not be prepared or transmitted on word processing or AIS equipment unless previously approved by the OJAG/NLSC TSCO.

(e) All Top Secret material is accountable and shall be handled in accordance with control procedures in Chapter 7, Section 7-3 of reference (c). OJAG and NLSC shall maintain a continuous chain of signature receipts for all Top Secret material received or routed.

(2) Top Secret Control Officer (TSCO) duties are addressed in Chapter 2 and Chapter 7, Section 7-3 of reference (c).

(3) Secret and Confidential Material.

(a) All NLSC personnel requiring access to and/or handle Secret or Confidential material must:

(1) Be properly cleared and granted Secret or Confidential access, as required by level of classification on classified document;

(2) Sign a SF 312;

(3) Be listed on the local access roster and authorized to handle Secret or Confidential material within NLSC;

(4) Have the requisite need-to-know.

(b) Secret and Confidential documents, shall, if required, be maintained by appropriate codes, and be return to the NLSC Security Office for transfer or destruction. EXCEPTION: Classified bulk documents beyond the storage capability of the code may be stored in the Security Office vault but must be reviewed at least every 6 months by the appropriate code.

(c) Temporary removal of Secret and Confidential material may be authorized by Division Directors or higher authority when it is to be taken to a local conference meeting being held at a government facility and returned to NLSC on the same day. Under no circumstances shall classified material be taken to a private residence or held overnight in commercial hotel/motel accommodations. A complete listing of documents being removed from NLSC under this authority shall be recorded in the Classified Material Logbook.

2. INCOMING MAIL, BULK SHIPMENTS, DELIVERED MATERIAL

a. Incoming Accountable/Special Services Mail procedures are in place to ensure that all incoming mail, including registered mail, bulk shipments, and delivered material are adequately protected until a determination is made as to whether it contains classified material.

b. Screening points shall be established in command mail handling facilities to ensure that incoming material is properly

controlled and that access to classified material is limited to cleared personnel.

3. TRANSMISSION AND TRANSPORTATION OF CLASSIFIED MATERIAL

a. All classified documents shall be prepared for transmission as directed by the Security Manager and in accordance with reference (c), Chapter 9.

b. All individuals authorized to carry or escort classified material while in a travel status shall be fully briefed by the Security Office of the provisions of Chapter 9, reference (c), prior to departure from their duty station.

c. Individuals hand carrying classified material outside the command must have a Courier Authorization (DD Form 2501) or Courier Authorization Letter in their possession. They also must receive a courier briefing and sign an acknowledgement that they have been briefed as to their security responsibilities while performing the duties of a courier.

d. A Record of Receipt (OPNAV 5511/10) must be completed and signed for by an activity receiving classified material. The OPNAV 5511/10 must be returned to the Security Office.

4. REPRODUCTION OF CLASSIFIED INFORMATION

a. TOP SECRET

(1) Requests for reproduction of Top Secret material shall be directed to the TSCO for action.

(2) Those portions of documents and materials which contain Top Secret information shall not be reproduced without the consent of the originating activity or higher authority.

(3) Top Secret information shall only be prepared, printed, and reproduced in the designated Navy areas, DOD facilities or as specifically approved by the Director, Defense Automated Printing Service.

b. SECRET AND CONFIDENTIAL. Secret and Confidential documents may be reproduced with the approval of the OJAG/NLSC Security Manager.

c. In all cases, reproduced documents shall be controlled and accounted for in accordance with Chapter 7, Section 7-15 of reference (c).

d. Reproduction of classified material shall be restricted to equipment located in the NLSC designated secured area.

5. DISSEMINATION OF CLASSIFIED INFORMATION

a. Upon receipt into OJAG or NLSC, all Top Secret, Secret and Confidential material must be hand-carried to the NLSC Security Office for in-house control and distribution. The material must contain the appropriate classified cover sheet, SF 703 for Top Secret, SF 704 for Secret and SF 705 for Confidential.

b. Top Secret material may only be routed from one individual/code to another by the TSCO/Assistant (Security Manager/Assistant). Each and every transfer of Top Secret material shall be accomplished through the Security Office.

c. For additional information on markings and dissemination of classified information and controlled unclassified information originated or received, follow the guidance contained in Chapters 6 and 8 of reference (c). Procedures for assigning distribution statements on technical documents are contained in reference (c), Exhibit 8 A.

d. When custody of classified information is transferred from one individual to another, the releasing custodian must complete an Acknowledgement of Classified Material Transfer form listing the description and date of classified material that is being transferred. Both the releasing custodian and the receiving custodian must sign the form. The completed Acknowledgement of Classified Material Transfer form must then be provided to and kept on file in the Security Office.

6. DISPOSAL OF CLASSIFIED INFORMATION

a. Record and non-record documents shall be destroyed as soon as their retention period has expired or the intended purpose has been served, as authorized by the latest version of SECNAVINST 5212.

b. Destruction of classified material in burn bags.

(1) Classified material awaiting burn shall be stored and protected with respect to the level of classified material contained within. Destruction of classified material will be recorded on DD2843 Classified Material Destruction Record.

(2) Burn Bags must be folded over and stapled and will not weigh more than 10 pounds. Each bag must be marked with the following information:

(a) Highest Classification of information contained

(b) Organization/Code

(c) Date

(d) Contact number for office

(e) Location (WNY/PNT)

(3) Washington Navy Yard burn bags collection will be Friday mornings at 0800. The bags are picked up by personnel from the Pentagon Incinerator Facility between Building 33 and Building 111. Burn bags will be accepted every day at the Pentagon's Remote Facility Loading Dock between 0800-0900 and 1100-1200, except for the last Thursday of the month.

(4) On the last Thursday of the month, hard drives are accepted for destruction at the Pentagon. The following procedures shall be followed for destruction of hard drives.

(a) Classified hard drives will not be placed in the same bags as other classified or sensitive material.

(b) Hard drives will be listed in the remarks section of DD Form 2843, "Classified Material Destruction Record."

(c) Hard drives will not be placed in a box/bag and must be stripped of any brackets and/or hardware prior to turn in.

c. Destruction of Top Secret Material

(1) A Record of Destruction is required for Top Secret information using OPNAV 5511/12 Classified Material Destruction Report.

(2) The OJAG/NLSC TSCO or representative, using OPNAV Form 5511/12, shall review material and destruction certificate for correctness, sign and date certificate, and place classified material in a burn bag. Signatures of two witnesses are required in accordance with Chapter 10, Section 10-19 of reference (c) when information is placed in burn bag or destroyed.

(3) Witnessing officials for Top Secret material shall be at least grade level GS-5 or E-5 and hold a Top Secret clearance.

(4) Top Secret material, including notes, rough drafts, carbon paper, and waste sheets, typewriter ribbons, etc. shall be brought to and destroyed only by the TSCO.

d. Destruction of Secret or Confidential Material. For Secret or Confidential material, the appropriate classified custodian for respective code and one witnessing official shall place all material, such as non-record working papers, preliminary drafts, typewriter ribbons, proof sheets, plates, photographs, negatives, reproduction papers, stenographic notes, work sheets, and similar items, in a burn bag when the material has served its purpose.

e. OJAG/NLSC Security Office

(1) The Security Office shall randomly spot check destruction burn bags to ensure they are properly packed and contain no unauthorized material. Items not permitted in destruction burn bags are binders, cardboards, newspapers, magazines, food scraps, trash, tobacco, metal, glass objects, etc. Any bag not properly packed, or containing unauthorized material, shall be returned to the responsible code for repacking.

(2) OJAG/NLSC Security Office shall serially number each burn bag, complete a Classified Material Destruction Record, DD Form 28433. The burn bags will be delivered to the loading platform on Patterson Street (East side of building) and loaded onto the designated destruction vehicle by two appropriately cleared persons, each Friday, excluding holidays. The burn bags are picked up at 8:00 a.m. and then taken to the Central Destruction facility (Pentagon incinerator) by DOD-WHS personnel. The two cleared persons shall witness placement of burn bags in DOD-WHS destruction vehicle and certify by signing Section 6 of the DD Form 28433.

f. Annual Clean Out Day. The annual clean out day for disposition of unneeded classified information at NLSC will be February 1st of each year.

g. Additional Information. For additional information on destruction of classified information and controlled unclassified information, see procedures in Chapter 10, reference (c).

7. CLASSIFICATION MARKINGS

a. Classified documents shall be marked in accordance with reference (c), Chapter 6, and Exhibit 6A.

8. SERIAL NUMBERS

a. All outgoing classified correspondence or letters of transmittal shall be identified by a serial number.

b. OJAG and NLSC personnel shall obtain serial numbers from classified files.

c. The serial number shall be typed below the originator's code and/or file number in the upper right hand corner of the first page of the document.

d. The letter C, S, or T, as appropriate, shall precede serial numbers to denote the overall classification of the document. Example: C123 for Confidential, S123 for Secret, or T123 for Top Secret.

9. SAFEGUARDING CLASSIFIED INFORMATION

a. OJAG and NLSC will follow the procedures listed in this instructional manual, as well as the procedures in Chapter 7 of reference (c) for safeguarding classified information. Chapter 7, Section 7-10 of reference (c) covers procedures for safeguarding classified information during working hours.

b. Classified information or material shall be used only where there are facilities or conditions adequate to prevent unauthorized access or visual sight.

c. Custodians of classified material shall be responsible for safeguarding the material at all times and for locking it in appropriate security containers when not in use. Classified

information must be returned to the Security Office prior to the end of the day for storage, unless custodian has a designated storage container that has been approved by the Security Office.

e. Personnel shall not remove classified material from workspaces without specific approval from their supervisor, Division Director, Department Head and Security Manager.

f. Under no circumstances shall classified material be removed to an individual's residence.

g. Visitors not authorized access to classified information or not having a "need to know" shall be received or interviewed outside of areas in which classified information is displayed or being discussed.

h. Signal or magnetic cards, showing "OPEN" or "SECURED" (or "LOCKED") shall be used to call attention to containers that are open or locked to indicate the condition of container. The cards must be clearly visible.

i. Classified information shall never be discussed or transmitted over unsecured telephone circuits, by graphic transfers or in public places, and personnel should never 'talk around" a classified subject.

j. A Secure Terminal Equipment (STE) encrypted telephone communications system, as well as reproduction and shredding equipment, are available in the command's strong room. All personnel shall comply with security requirements for handling and safeguarding classified information over STE equipment, and reproduction and disposition of material.

k. AIS media used for processing or storing classified information shall be marked with an SF 706 (Top Secret), SF 707 (Secret), SF 708 (Confidential), 709 (Classified), SF 710 (Unclassified), SF 711 (Data Descriptor), as applicable in accordance with Exhibit 6A of reference (c).

l. Safeguarding Classified Material During Emergencies, such as fire or other emergencies will be handled in accordance with the Emergency Action Plan For Protection of Classified Material and Equipment.

m. Reference (a), Appendix F addresses non-U.S. Citizens eligibility for access to classified information.

n. Safeguarding U.S. Classified Information in Foreign Countries is covered in reference (c), Chapter 7, Section 7-14.

10. MEETINGS, CONFERENCES AND SYMPOSIA

a. Classified defense information shall not be disclosed at conferences, symposia, exhibits, clinics, scientific and technical conventions and gatherings unless sponsored by an activity of the Executive Branch of the government.

b. OJAG NLSC personnel sponsoring or participating in a meeting at which classified information is to be revealed shall consult with the Security Manager, prior to the fact, to ensure that requisite requirements of reference (c) are met.

c. The Security Manager of the sponsoring activity shall ensure that the provisions of Chapter 7, section 7-12 of reference (c), are followed in all respects where meetings involve disclosure of classified material to visitors.

d. The attendance of non-government attendees who are not properly cleared members of the Executive Branch of the government or cleared DOD contractor employees sponsored by NLSC, where classified material will be disclosed, shall be authorized by the Chief of Naval Operations (CNO). This approval shall be received by the sponsoring activity before invitations are issued; requests shall be submitted through Security Managers to OPNAV at least 30 days prior to the proposed meeting.

11. STORAGE OF CLASSIFIED MATERIAL

a. Classified information in the custody of NLSC shall be protected by stowage only in authorized security containers or vaults approved by the Security Manager. Security containers procured for government use during recent years bear a plate denoting GSA approval and the class of security provided. Containers that do not bear such identification shall be reported to the Security Manager for a determination as to whether the container meets current protective criteria. Reference (c), Chapter 10 covers procedures for storage of classified material that NLSC shall abide by in the following areas:

(1) Basic Policy

(2) Standards for Storage Equipment

(3) Storage Requirements for Top Secret, Secret, and Confidential Information

(4) Procurement of New Storage Equipment

(5) Removal of Security Containers

(6) Shipboard Containers and Filing Cabinets

(7) Vaults and Secure Rooms

(8) Specialized Security Containers

(9) Decertified Security Containers

(10) Residential Storage

(11) Replacement of Combination Locks

(12) Combinations

(13) Keys and Padlock Control

(14) Securing Security Containers

(15) Repair, Maintenance and Operating Instructions

(16) Electronic Security System

b. Knowledge of or access to the combination of a vault or container for the storage of classified material shall be given only to those appropriately cleared persons who are authorized access to the classified information therein.

c. Electrically actuated locks (e.g., cipher and magnetic strip card locks) do not afford the degree of protection required for classified information and shall not be used as the locking device on security containers.

12. CUSTODIANS OF CLASSIFIED MATERIAL

a. At a minimum, a custodian and an alternate shall be requested by Directorates and approved and designated by the Security Office, in writing, for each container used for stowage of classified information. Under no circumstances shall the names of the custodian and alternate be affixed to the outside

of a container. Custodians must possess valid security clearances and appropriate access for the highest category of information stowed. Custodians shall bear primary responsibility for compliance with all the stowage procedures relating to the container and its contents as set forth in this instruction and reference (c), Chapter 10.

13. SECURITY PROCEDURES FOR OJAG and NLSC

a. Entrance to the OJAG/NLSC Security Office will be restricted to official business.

b. Only properly cleared personnel with SIPRNET accounts are allowed unescorted access into the command's SIPR secure room. These individuals must:

(1) Sign and date the log sheet and enter the times of entry and departure for each visit.

c. Classified information will not be discussed over non-secure circuits. If a secured call needs to be made, contact the NLSC Security Office.

d. End of Day Security Checks. Supervisors shall designate personnel to conduct a security check at the end of each working day to ensure that all classified material and security containers (safe or vault) are properly secured, using the SF 701 Activity Security Checklist and SF 702 Security Container Check Sheet in accordance with reference (c) Chapter 7-11. The SF 702 will be initialed, dated and time entered on the open/close record.

e. Visitors will be kept to a minimum and shall not be allowed in areas designated for work with classified material unless properly cleared.

f. The retention of classified documents and material is authorized only if needed to mission accomplishment. All classified control point or codes holding classified documents and materials shall conduct a quarterly review on all classified holdings to ensure retention is justified. All classified material no longer needed shall be destroyed. Besides this requirement, the retention of classified documents and material more than 5 years from the date of origin is prohibited unless authorized by the latest version of SECNAVINST 5215.

g. All unoccupied rooms, including conference and training rooms shall be secured and access monitored to ensure only authorized personnel use these spaces. The designated point of contact for these areas is the responsible person for ensuring compliance.

h. All personnel will carry on their person their building badge and CAC identification throughout all building areas. Unfamiliar persons found in areas will be challenged to ensure authorized presence.

i. The Security Office will conduct unannounced security inspections of classified containers to ensure that all documents assigned to those containers are accounted for that that no unauthorized reproduction is being made of classified documents.

j. The Security Office and/or a designated OJAG or NLSC representative will conduct unannounced security inspections during working hours to ensure classified material are being properly protected.

LOCKING PROCEDURES FOR SECURING STORAGE CONTAINERS

1. PROCEDURAL PROCESS

a. The use of proper locking procedures in securing stowage containers is essential and the following procedures apply:

(1) Safes. Firmly shut door(s), close (handle(s)) and rotate the combination dial at least four complete turns in one direction. Check and recheck.

(2) Safe-File Cabinets. Various models of safe-file cabinets manufactured by several different firms are presently being used, and the mechanical arrangements for securing these cabinets differ between brands and models. The following procedure will properly secure all models of safe-file cabinets.

(a) Close all drawers other than combination drawer. Push each drawer in firmly as far as possible.

(b) Close combination drawer. Push in firmly as far as possible.

(c) If lock has a manipulation proof knob in dial center, turn knob in a Counter clockwise direction to free dial for locking.

(d) Rotate dial in one direction at least four complete revolutions.

(e) Test each drawer individually by depressing latch release and pulling on handle.

c. Chapter 10 of reference (c) contains guidelines on changing combinations to security containers and vaults.

2. ACCOUNTABILITY OF SECURITY CONTAINERS

a. All security containers are controlled by the Security Manager and shall not be moved, altered, or repaired without specific approval.

b. Requests for additional or replacement security containers shall be submitted to the Security Manager for appropriate action.

c. Strict accountability for GSA-approved security containers shall be maintained by the Security Manager.

3. COMBINATIONS

a. All custodians having approved safes will:

(1) Record each combination on an SF 700 Security Container Form;

(2) Complete Part 1 and 2A (on end of flap);

(3) Read the Privacy Act Statement on the reverse side of the form;

(4) Detach Part 1 and attach to inside of container;

(5) Mark Parts 2 and 2A with the highest classification stored in this container;

(6) Detach Part 2A and insert in envelope;

(7) Hand carry the envelope containing Part 2A to the Security Office for storage and safekeeping.

b. Combinations will be changed immediately upon departure of personnel having access to safe vault.

INDUSTRIAL SECURITY PROGRAM

1. GENERAL

a. Chapter 11 of reference (c) covers the industrial security program for contractor personnel with regard to classified information.

c. Contractor personnel shall also comply with NLSC security regulations contained in this manual when handling and safeguarding classified information.

2. RESPONSIBILITIES

a. The Contracting Officer shall designate, in writing, a Contracting Officer Representative in accordance with reference (c), Chapter 2-6.

b. The COR's responsibilities are defined in Chapter 11-5 of reference (c).

SECURITY REVIEW

1. POLICY

a. All material prepared for publication or otherwise disseminated, unless classified or containing limiting statement, is normally available to the public. Accordingly, originators in OJAG and NLSC shall ensure that all material being released is unclassified and contains no proprietary or other information of trade secrets of private concerns communicated to the NLSC in confidence, nor critical technologies.

b. Review of information prepared within the NLSC prior to publication shall not be made in isolation. Information shall first be routed through appropriate offices, reviewed for technical accuracy and protection of proprietary information, antiterrorism considerations and, finally to assure that no classified information is inadvertently revealed. Nothing contained in this chapter is to be construed as circumventing the Freedom of Information Act or matters covered by the Privacy Act.

SENSITIVE AND INFORMATION TECHNOLOGY POSITIONS/ PERSONNEL SECURITY INVESTIGATIONS

1. POLICY AND PROCESS

a. OJAG and NLSC will follow the procedures in Chapter 5 of reference (a) to fulfill the requirements for the following topics:

(1) Position Designation

(2) Criteria for Designating Positions

(3) Non Sensitive and Sensitive IT Positions

(4) Suitability and Security Investigation and Adjudication

(5) Security Adjudication Criteria

(6) Citizenship Requirements

(7) Dual Citizenship

(8) Investigation Equivalency Table

(9) Waiver Procedures and Processes

PERSONNEL SECURITY CLEARANCES AND ACCESS

1. GENERAL

a. A personnel security clearance, when granted, is an administrative determination that an individual is eligible for access to classified information at a specified level.

b. Access to classified information is also an administrative determination based on the principle of "need to know" and will be handled in accordance with reference (a), Chapter 9.

c. To properly monitor the Information, Personnel and Physical Security Programs, all NLSC Security Managers shall be considered to have a "need to know" for access to all levels of classified information in the possession of their activity, commensurate with their level of security clearance.

2. RECORDING PERSONNEL SECURITY INVESTIGATIONS AND ACCESS ELIGIBILITY

a. DONCAF records adjudication determinations in JPAS and NLSC receives notification. DISCO records this information in JPAS for all contractors.

b. Citizenship is recorded in JPAS via the Defense Civilian Personnel Data System for civilians, Personnel Support Detachment for military members, and the sponsoring contracting company for contractors. Citizenship requirements are addressed in Appendix F of reference (a).

3. TEMPORARY AND ONE TIME ACCESS

a. Temporary access to classified information will be handled in accordance with reference (a), Chapter 9-4.

b. One time access to classified information will be handled in accordance with reference (a), Chapter 9-5.

4. EMERGENCY APPOINTMENTS

a. Any emergency appointments will be handled in accordance with Chapter 6-6, paragraph 7 of reference (a).

b. Emergency appointments should not be an expected practice but kept to an absolute minimum and handled on a limited and exceptional basis.

5. PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS

a. Investigative requirements for OJAG and NLSC civilian, military and contractor personnel in sensitive positions, including IT positions, will be determined and handled in accordance with Chapter 6 of reference (a).

b. Sensitive and Information Technology Positions, and position designation, citizenship, suitability, and waivers requirements are addressed in Chapter 5 and Exhibit 5-B of reference (a).

c. OJAG/NLSC Security Office will:

(1) Determine and request appropriate security forms;

(2) Provide specific guidance and requirements for preparing and processing investigative paperwork;

(3) Review security forms for completeness and accuracy;

(4) Fingerprint personnel, as required;

(5) Initiate appropriate investigations to the Office of Personnel Management via e-QIP, as required;

(6) Input/record pertinent personnel security information in JPAS;

(7) Monitor the Period Reinvestigation Program;

(8) Prepare waiver letters/requests, when required; and

(9) Determine and grant interim clearances, when required.

SECURITY OFFICE CUSTOMER SERVICE HOURS
AND
PHONE NUMBERS

1. SECURITY OFFICE HOURS OF OPERATION

a. Staff permitting, the OJAG/NLSC Security Office hours of operation are 0700 - 1600, Monday through Friday.

2. SECURITY OFFICE PHONE NUMBERS

a. Customer Service Support Counter: 202-685-5482

b. Assistant Security Manager: 202-685-5482

c. Security Manager: 202-685-5470

d. Fax Number: 202-685-5467

DESIGNATION OF SECURITY MANAGERS/OFFICERS
(COMMAND LETTERHEAD)

From: Commanding Officer
To: (Name, Title, Grade)

Subj: DESIGNATION AS SECURITY MANAGER

Ref: (a) SECNAV M-5510.30, Department of the Navy Personnel Security Program
(b) SECNAVINST 5510.30B
(c) SECNAV M-5510-36, DON Information Security Program
(d) SECNAVINST 5510.36A

1. In accordance with references (a) through (f), you are hereby designated as Security Manager for Naval Facilities Engineering Command. In this capacity, you shall serve as my advisor and direct representative in cases pertaining to the Information, Personnel and Physical Security Programs.

2. You are directed to familiarize yourself with pertinent duties in references (a) through (f) and take appropriate action to ensure that the security provisions are effectively administrated to preclude unauthorized access to the facility and unauthorized disclosure or compromise of classified material or violation of security requirements. Further, you shall provide direction and guidance to subordinate Security Managers and monitor their effectiveness in complying with the command Information, Personnel and Physical Security Programs.

3. All previous appointments to this position are hereby rescinded.

_____
(Typed name and signature of Commander)

Copy to:
CNO (N09N2) (for NLSC Headquarters only)
NLSC Security Program Manager

(NOTE: If an alternate Security Manager is designated, an identical letter of designation, appropriately modified, shall be issued and signed by the Commander.)