Commanding Officer
and
Executive Officer

Information and Personnel Security Reference Handbook

Assistant for Information and Personnel Security
(N09N2)
Office of the Chief of Naval Operations

Governing Documents

- ✓ **EO 12958, as Amended Classified National Security Information**
- ✓ **EO 12968 Access to Classified Information**
- ✓ **EO 10450 Security Requirements for Government Employees**
- ✓ **EO 12829 National Industrial Security Program**
- ✓ **DoD 5200.1-R Information Security Program Regulation**
- ✓ **DoD Instructions 5200.2R**
- ✓ **SECNAVINST 5510.36A Information Security Program Instruction**
- ✓ **SECNAVINST 5510.30B Personnel Security**
- ✓ **OPNAVINST 5530.14C Physical Security**

Emergency Plan & Supplement

- ✓ Commands shall develop an **Emergency Plan** for the protection of classified information in case of natural disaster or civil disturbance. The minimum plan requirements are indicated in SECNAV M-5510.36, Exhibit 2B.
- ✓ Commands outside the U.S. and its territories and units that are deployable shall also develop an **Emergency Destruction Supplement**. Conduct emergency destruction drills as necessary to ensure that personnel are familiar with the plan and associated equipment. Any instances or emergency destruction of classified information shall be reported to the CNO (N09N2).

Security Policy

- ✓ No individual will have access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made regarding his/her loyalty, reliability and trustworthiness. A personnel security investigation (PSI) is conducted to gather information pertinent to these determinations.

- ✓ Commanding Officers are responsible for compliance with and implementation of the Department of the Navy Information and Personnel Security Program within their command. The effectiveness of the command's security program depends on the importance the commanding officer gives it.

Loss/Compromise Of Classified Information

A compromise is the unauthorized disclosure of classified information to a person(s) who does not have a valid clearance, authorized access, or need-to-know.

- ✓ Immediately notify the local NCIS office and initiate a Preliminary Inquiry (PI) when a loss or compromise of classified information under command cognizance occurs.

- ✓ Appoint, in writing, a command official (other than the Security Manager or anyone involved with the incident) to conduct a PI.

- ✓ SECNAV M 5510.36, para 12-3 through 12-7, and Exhibit 12A and B, contain specific guidance for initiating and conducting a PI.

- ✓ Appoint, in writing, an individual to conduct a JAGMAN investigation, if, after completing the PI, compromise cannot be ruled out, or if corrective or disciplinary action is required.

Commanding Officer's Responsibilities

- ✓ Safeguard classified material
- ✓ Approve an emergency plan for protection and destruction of classified information
- ✓ Designate key sensitive positions in writing
- ✓ Issue written security plan
- ✓ Inspect subordinate commands
- ✓ Establish an industrial security program, if applicable
- ✓ Ensure a robust security education & training program
- ✓ Evaluate personnel with significant security responsibilities (include critical security element in fitness reports & Personnel Advancement Requirements)

Loss/Compromise f Classified Information

- ✓ SECNAV M-5510.36, para 12-9 through 12-14, and Exhibit 12C and D, contain specific JAGMAN guidance.
- ✓ Public media compromise is the unofficial release of classified information to the public. Public media compromises shall be immediately reported to CNO (N09N2).
- ✓ Security discrepancies involving classified information improperly handled, addressed, packaged, transmitted, or transported require a determination as to whether the information was *subjected* to compromise. If classified information has been *subjected* to compromise, follow the guidance in SECNAV M-5510.36, para 12-9.

Command Security Manager

- ✓ MUST be assigned and designated in writing
- ✓ MUST be an U.S. Citizen
- ✓ MUST be a commissioned officer or a civilian employee, GS-11 or above
- ✓ MUST have been the subject of a favorably adjudicated SSBI completed within the previous 5 years
- ✓ MUST have direct access to the Commanding Officer
- ✓ MUST be identified by name on command organizational charts, telephone listings, rosters or other media
- ✓ Remain cognizant of all command information, personnel, and industrial security functions
- ✓ Ensure that the security program is coordinated and inclusive of all requirements in the ISP and the PSP regulations.

Industrial Security Program

- ✓ Establish an industrial security program if the command engages in classified procurements or if cleared DoD contractors operate within areas under direct control of the command.
- ✓ Ensure a DD form 254 is incorporated into each classified contract.
- ✓ Comply with the requirements of DoD Directive 5200.1, to include development of a Program Protection Plan, if responsible for the acquisition of classified defense systems.

Security Manager Duties

- ✓ Advise CO on information and personnel security
- ✓ Develop command security procedures
- ✓ Safeguarding - Control measures
- ✓ Military operations - Emergencies
- ✓ Manage security education program
- ✓ Establishes procedures that deal with threats, compromises, and violations
- ✓ Coordinate with other security personnel
  - ➢ Physical Security Officer
  - ➢ Special Security Officer
  - ➢ Public Affairs Officer
  - ➢ Information Assurance Manager
- ✓ Coordinate with local/regional HR Office
- ✓ Coordinate with Command Contract Office Representative (COR)
- ✓ Maintenance of Security Classification Guides (SCG)
- ✓ Develop procedures for classified visits
- ✓ Coordinate with Navy IPO
- ✓ Interpret regulations for disclosure to Foreign Governments
- ✓ Establish Industrial Security Program, if applicable

Storage & Destruction

- ✓ Ensure all classified information is stored in a manner that will deter or detect access by unauthorized persons.
- ✓ Establish procedures, to include screening points, to ensure that all incoming mail, including bulky shipments, are secured until a determination is made as to whether or not they contain classified information.
- ✓ Establish administrative procedures for the control and accountability of keys and locks whenever high security key-operated padlocks are used.
- ✓ Establish procedures to ensure all classified information intended for destruction is destroyed by authorized means and appropriately cleared personnel.

Security Manager
Duties

- ✓ Manage the Joint Clearance and Access Verification System (JCAVS)
- ✓ Track Personnel Security Investigations (PSI)
- ✓ Serve as the CO's advisor and direct representative in matters pertaining to the security of classified information and personnel security
- ✓ Develop written command information and personnel security procedures including an emergency plan which integrates emergency destruction bills, where required
- ✓ Formulate and coordinate the command's security education program
- ✓ Ensure threats to security and other security violations are reported, recorded and when necessary, investigated vigorously
- ✓ Administer the command's program for classification, declassification and downgrading of classified information
- ✓ Ensure that command personnel who perform security duties are kept abreast of changes in policy and procedures and are provided assistance in problem solving

Dissemination

- ✓ Establish procedures for the dissemination of classified and controlled unclassified information originated or received by the command.

- ✓ Ensure that technical documents are assigned an appropriate distribution statement. Specific guidance is provided in SECNAV M-5510.36, para 8-7 and Exhibit 8A.

- ✓ Establish a program to ensure that all proposed public releases undergo prepublication security and policy review. SECNAV M-5510.36, Exhibit 8B, identifies specific categories of information requiring review by higher authority.

Security Manager Duties

- ✓ Coordinate the preparation and maintenance of security classification guides under command's cognizance
- ✓ Maintain liaison with the command Public Affairs Officer to ensure that proposed press releases and non-official work or speeches which could contain classified information are referred for security review
- ✓ Ensure compliance with accounting and control requirements for classified material including receipt, distribution, inventory, reproduction and disposition
- ✓ Coordinate with the physical security officer, information assurance manager, special security officer and other command officials regarding information and personnel security policies and procedures and other matters of common concern
- ✓ Develop security measures and procedures regarding visitors who require access to classified information
- ✓ Ensure that all electrical or electronic processing equipment meets control of compromising emanations (TEMPEST) requirement

Transmission & Transportation

- ✓ Ensure that only appropriately cleared personnel or carriers transmit, transport, escort, or hand-carry classified information.
- ✓ Establish procedures for shipping bulky classified information as freight.
- ✓ Authorize official travelers to escort or hand-carry classified information only when the conditions in SECNAV M-5510.36, para 9-11(4) are met.

Security Manager Duties

- ✓ Ensure protection of classified information during visits to the command when the visitor is not authorized access to classified information
- ✓ Implement and interpret, regulations governing the disclosure of classified information to foreign governments
- ✓ Ensure compliance with the Industrial Security Program for classified contracts with DoD contractors
- ✓ Ensure that access to appropriately cleared personnel have a need-to-know
- ✓ Manage the command's Joint Personnel Adjudication System/Joint Clearance and Access Verification System (JPAS/JCAVS)
- ✓ Ensure that all personnel who handle classified information or assigned to sensitive duties are appropriately cleared and that the requests for PSI are properly prepared, submitted and monitored
- ✓ Coordinate the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties

Safeguarding

- ✓ Afford information a level of control commensurate with the assigned security classification level.
- ✓ Ensure that all Top Secret information originated or received by the command is continuously accounted for, individually serialized, and entered into a Top Secret log.
- ✓ Establish administrative procedures for the control of Secret and/or Confidential information.
- ✓ Ensure that classified discussions at meetings and other types of gatherings are held only when disclosure of the information serves a specific U.S. Government purpose.
- ✓ Designate specific equipment for classified reproduction, limit this reproduction, facilitate oversight and control of reproduction, and ensure expeditious processing of classified information.
- ✓ Ensure classified information is processed on an accredited IT system only in secure facilities, and under conditions, which prevent unauthorized persons from gaining access.

Personnel Security Clearance Eligibility

A formal determination that an individual meets personnel security requirements and is eligible for access to classified information other than that protected in a special access program, and/or access to sensitive National Security Information

Three Levels

- ✓ **Top Secret** - Eligibility for access to Top Secret, Secret, and Confidential classified information
- ✓ **Secret** - Eligibility for access to Secret and Confidential classified information
- ✓ **Confidential** - Eligibility for access to Confidential classified information

DON CAF is the sole DON security clearance granting authority (Designated by SECNAV)

Security Classification Guides (SCG)

- ✓ Serve both legal and management functions by recording DON original classification decisions, and are the primary reference source for derivative classifiers.
- ✓ SCGs are forwarded to the CNO (N09N2), RANKIN Program Manager, after approval by an OCA
- ✓ The RANKIN Program is a computerized database that provides for the standardization, centralized management and issuance of all DON SCGs

Marking

- ✓ Intended to alert holders classified information is contained in a document, and serve to warn holders of special access, control or safeguarding requirements.
- ✓ All classified information, regardless of media, shall be clearly marked per SECNAV M-5510.36, Chapter 6
- ✓ Supplemental marking guidance is available at www.navysecurity.navy.mil.
- ✓ Proper marking is the specific responsibility of the original or derivative classifier.

Investigative Requirements

Secret or Confidential access or non-critical sensitive duty assignment
Are supported by the following investigation types
NACLC (Military – New Accession)
ANACI (Civilian – New Hire)
Periodic Reinvestigations NACLC SSBI-PR Phased PR

Top Secret Access or Critical Sensitive Duty Assignment
SSBI
SSBI-PR
Phased PR

Classification Management

- ✓ **Original Classification:** An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.
- ✓ **Original Classification Authority (OCA):** An official authorized in writing, either by the President, an agency head, or the Senior Security Official for the DON, to make an original classification decision.
  - ➢ Current DON OCAs are posted at www.navysecurity.navy.mil
- ✓ **Derivative Classification:** The incorporating, paraphrasing, restating, or generating, in new form, information that is already classified and ensuring that it continues to be classified by marking or similar means when included in newly created materials. Derivative classification decisions are the responsibility of the originator.

Investigative Requirements

Military

- ✓ Enlisted Navy, Commissioned Officers, Midshipmen and ROTC Candidates – **NACLC**

Civilian

- ✓ Nonsensitive – **NACI**
- ✓ Noncritical Sensitive - **ANACI**
- ✓ Critical Sensitive – **SSBI** (Completed & Adjudicated)
- ✓ Special Sensitive - **SSBI**
- ✓ Pre-appointment Requirement – New Hires Previous
- ✓ PSI (Except ENTNAC, NAC) or Emergency Appointment
  - ➢ PSI Submitted
  - ➢ Justify in Writing
  - ➢ File (Investigation) Locally
- ✓ DON Contractor Personnel
- ✓ Contractor FSO submits PSI to DSS

New PSI required if break in service is greater than 24 months

JPAS

The Department of Defense (DoD) system that connects security personnel and the DoD Agency Central Adjudication Facilities

- ✓ Provides virtual consolidation of the DoD CAFs
- ✓ For use by personnel security program mangers, Special Security Officer, and DoD contractor security officers
- ✓ Mandated for use by all DOD
  - ➢ All DON organizations (to include contractors)
  - ➢ Central Adjudication Facilities (CAFs)
- ✓ **Promotes standardization within DOD**

Continuous Evaluation

- ✓ When questionable or unfavorable information becomes available concerning an individual who has been granted access to classified information or assigned to sensitive duties, commands will report that information to the DONCAF.
- ✓ Commands should report all information without attempting to apply or consider any mitigating factors that may exist.
- ✓ The information must be forwarded to the DON CAF via the Joint Personnel Adjudication System (JPAS).
- ✓ The command report must be as detailed as possible and should include all available information pertinent to the DON CAF determination.
- ✓ Keys to an active program are security education of reporting requirements in the form of management support, confidentiality and employee assistance referrals.

JCAVS

- ✓ Validates Security clearance eligibility
- ✓ Determines the status of PSI requests
- ✓ Records NDAs & Attestations
- ✓ Records Interim Security Clearance
- ✓ Records command access
- ✓ Processes Incoming and Outgoing Visit Requests
- ✓ Provides ability to constantly update access and related information in real time
- ✓ Provides ability to constantly communicate with other Security Management Offices and CAFs
- ✓ Provides ability to manage Personnel actions, run reports and receive notifications

Granting Temporary Access

Only grant temporary access if the Personnel Security Investigation (PSI) does not support level of access required

No Investigation
OR
Higher level Investigation is required
(i.e., has Secret, needs Top Secret)

MUST HAVE

- ✓ Current SECRET or CONFIDENTIAL eligibility based upon a, NACLC, or ANACI within the last 10 years
- ✓ No break in service exceeding 24 months
- ✓ Local Record Check & PSI review
- ✓ SSBI submitted

Purpose of A Personnel Security Investigation

No individual will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made regarding his/her loyalty, reliability and trustworthiness.

- ✓ Suitability for Federal Employment Eligibility
  - ➢ Classified Access
  - ➢ Sensitive Duty Assignments
  - ➢ Other Duty Assignments
- ✓ Resolve Suitability/Eligibility Issues

The scope of the investigation conducted will be commensurate with the level of sensitivity of the access required or position occupied. PSIs will not normally be requested for any civilian or military personnel who will be retired, resigned, or separated with less than 1 year service remaining.

Suspension of Local Command Access

- ✓ When questionable or unfavorable information becomes available concerning an individual who has been granted access, the CO may suspend access.
- ✓ Suspension of access may only be used as a temporary measure.
- ✓ Notify the individual in writing
- ✓ Notify DON CAF within 10 days
  - ➢ "Report Incident" (via JPAS)
  - ➢ "Suspend Access" (via JPAS)
- ✓ Remove from access lists & visit certifications
- ✓ Notify co-workers of suspension
- ✓ Change combinations
- ✓ Cancel or hold transfer orders
- ✓ A command report of suspension of access will automatically result in suspension of the individual's clearance eligibility by the DON CAF

Department of the Navy Central Adjudication Facility (DON CAF)

Clearance Eligibility Granting Authority

Once granted eligibility valid provided:

- ✓ Compliance with standards
- ✓ No Break in service (24 months)
- ✓
- ✓

Clearance Prohibitions

- ✓ Non-sensitive positions
- ✓ Inadvertent access
- ✓ Unclassified duties in Restricted Area
- ✓ Access prevented by escort
- ✓ Facility Access Determination Program
- ✓ Congress, Supreme Court
- ✓ State Governors

Access to Classified Information

- ✓ Access to classified information may be granted only if allowing access will promote the furtherance of the DON mission.
- ✓ Access to classified information will be limited to the minimum number of individuals necessary to accomplish the mission and must be based on need-to-know.
- ✓ The level of access authorized will be limited to the minimum level required to perform assigned duties.
- ✓ No one has a right to have access to classified information solely because of rank, position, or security clearance eligibility.

Department Office of Hearings and Appeals (DOHA)

The Defense Office of Hearings and Appeals (DOHA), the largest component of the Defense Legal Services Agency, provides hearings and issues decisions in personnel security clearance cases.

- ✓ Individuals desiring to present a personal appeal must request a DOHA hearing within 10 days of receipt of Letter Of Determination (LOD).
- ✓ DOHA will normally schedule the personal appearance to be accomplished within 30 day of receipt of request.
- ✓ Travel costs for the individual presenting a personal appeal to DOHA will be the responsibility of the individual's command.
- ✓ The individual may be represented by counsel or other personal representative at the their expense.

Requests for postponement of the personal appearance can be granted only for good cause as determined by the DOHA.MOVE next para to the PSAB to the PSAB.

Personnel Security Appeals Board (PSAB)

The Department of the Navy Personnel Security Appeals Board (PSAB) is responsible for deciding appeals from DON personnel on unfavorable personnel security determinations made by the DON CAF.

- ✓ The PSAB will be comprised of three members at the minimum military grade of O-6 or civilian grade of GS-14.
- ✓ One member of the board will have a security background and serve as the President of the Board. At least one member will be in the military grade of O-6.
- ✓ An attorney is available for all legal questions, guidance or opinions requested by the PSAB.
- ✓ An Executive Director to administer operations of the PSAB will be appointed.
- ✓ The appellant will be notified of the PSAB decision via their CO. The appellant will generally be notified of the PSAB decision within 5 days of the board meeting. The written notification will provide the reasons that the PSAB either sustained or overturned the original determination of the DONCAF

The value of a command perspective on the PSAB deliberations cannot by overstated. Since appeals presented to DOHA do not have the benefit of a command endorsement, commands are strongly encourage to submit a position paper directly to the PSAB.