



DEPARTMENT OF THE NAVY

JOINT BASE PEARL HARBOR-HICKAM
850 TICONDEROGA ST STE 100
PEARL HARBOR HI 96860-5102

JBPHH 5510.36

JB00

JOINT BASE PEARL HARBOR-HICKAM INSTRUCTION 5510.36

Subj: JOINT BASE PEARL HARBOR-HICKAM INFORMATION AND
SECURITY PROGRAMS

Ref: (a) SECNAV M-5510.36
(b) SECNAV M-5510.30
(c) OPNAVINST 5239.1C
(d) CNICINST 5239.1
(e) IA Publication 5239-22
(f) DOD 5220.22M
(g) OPNAVINST 3432.1A

Encl: (1) Information Security/OPSEC Indoctrination Briefing

1. Purpose. To provide supplemental guidance per references (a) through (f) and standardized procedures for the implementation of quality information and Security Information and Security Programs (ISPS) within Joint Base Pearl Harbor-Hickam (JBPHH).

2. Scope. This instruction applies to all JBPHH and installation personnel. This instruction does not replace but is to be used in conjunction with references (a) through (f).

3. Background. References (a) through (f) provide policy guidance for the effective management of the Department of Defense (DOD) and Department of the Navy (DON) ISPS. Reference (g) provides guidance on OPSEC for Navy commands.

4. Discussion

a. For the purpose of this instruction, the term "classified material" applies to classified correspondence, messages, publications, working papers, information stored on the Secure Internet Protocol Router Network (SIPRNET) information technology networks and computer media. "Classified information" pertains to official information that has been

determined to require, in the interest of national security, protection from unauthorized disclosure to persons without favorable security clearance eligibility and the need-to-know (NTK).

b. No individual will be given access to classified information or assignment 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, as detailed in Chapter 6 of reference (b), to gather information pertinent to these determinations. A favorably adjudicated PSI determines the eligibility for an individual to access classified information and they have a NTK. A person's NTK is based on the necessity for access to, knowledge of, or possession of classified information in order to carry out official military or other government duties.

c. JBPHH Chief Staff Officer (CSO)/Installation Commanding Officer (ICO) will determine those position functions under his/her control that require access to classified information and may authorize access to the incumbents of such positions who have officially been determined to be eligible by the appropriate adjudicative authority.

d. No one has the right to have access to classified information solely because of rank, position, or security clearance eligibility. An individual's eligibility for a security clearance does NOT mean automatic access to classified information. Access to classified information is a separate and local determination made by the ICO, based on official NTK, established eligibility, and about whom there is no known unadjudicated disqualifying information. An individual's security clearance and access to classified information will be consistent with the policy to protect such information in the interest of national security and closely monitored by the Command Security Manager (CSM). Personnel security clearances, in excess of mission requirements, will be administratively withdrawn or downgraded.

5. Command Management/Responsibility

a. JBPHH CSO and ICO are responsible for effective management and execution of the ISPS outlined in references (a) and (b).

b. CSM is to be designated in writing and serves as Commander's principle advisor and direct representative in matters pertaining to the security of classified information held at the command, the eligibility of personnel to access classified information, and the ability to be assigned to sensitive duties.

c. Assistant Security Managers (ASM) may be assigned per the requirements of reference (a) and take direction from the CSM in providing support to the ISPS program.

d. CSM will be designated as the GENSER/Collateral Top Secret Control Officer (TSCO) if the command handles Top Secret information and is responsible for the proper control, accountability, protection, distribution, and destruction within the command and its transmission outside the command.

e. CSM will conduct periodic program reviews and assist visits of staff offices and installations that maintain classified material or SIPRNET accounts for evaluating and documenting the security management posture. Included in these reviews will be accounting, control, safeguarding, marking, destruction, dissemination, and management of classified material.

f. Each JBPHH staff code (that has classified material) and CO will designate a Classified Material Custodian (CMC), who is responsible for the accounting, control, safeguarding, marking, destruction, and dissemination of classified material for their program.

6. Command Security Education Program (CSEP). The CSEP will consist of the following:

a. Security Indoctrination Briefing to be conducted during new military and civilian personnel command check-in process.

b. Security Orientation Briefing. Each individual who will require access to classified information will complete this briefing prior to being granted access to the command's classified information, material, and assets.

c. Refresher Security Briefing. Once a year, all personnel will receive a Total Workforce Management System (TWMS) notice to complete this training via TWMS "self-service."

d. Counterintelligence Awareness Briefing. Annually, personnel who possess a Secret or higher security clearance shall attend a counter-espionage briefing by Naval Criminal Investigative Service (NCIS). Training will be set-up by the CSM.

e. Special Briefings. Based on access requirements and in performance of official duties, a special briefing is required for CMC, classified material couriers, and personnel planning on foreign travel. For foreign travel, personnel are required to seek the special briefing requirement with the CSM at least 3 weeks prior to traveling.

f. OPSEC indoctrination briefing. All newly assigned personnel, both military and civilian, will complete an OPSEC Indoctrination Briefing upon check-in to the command.

g. Security Debriefing. Personnel who have access to classified information must receive a security debriefing by the CSM under the following conditions:

(1) Prior to termination or retirement of active military service or civilian employment and for a temporary separation of 60 days or more.

(2) When a security clearance is revoked for cause.

(3) When a security clearance is administratively withdrawn.

7. Security Violations/Incidents. Incidents of security violations will be reported to the CSM immediately upon discovery. Violations after normal working hours, the Command Duty Officer (CDO) will be notified who will immediately contact the CSM via recall numbers. Security containers or spaces found open will be guarded until the responsible custodian listed on

the SF700 of the container arrives. Every effort will be made to secure the classified material involved, (i.e., locking back into security container, or securing the material in the ROC). In all cases, the CSM will be notified to make arrangements for a complete inventory. When a security violation occurs, the following actions will be completed:

a. CSM will review and determine the type of security violations that occurred (e.g. loss, compromise, or possible compromise) and initiate a full inventory of the classified library.

(1) If it is determined that a compromise or possible compromise has occurred, a designated official will be appointed by the CSO/ICO to conduct a Preliminary Inquiry (PI) into the circumstances surrounding the incident. For the purposes of electronic spillages (ES) from a DON Information Technology (IT) system, a PI is mandatory, regardless if it meets the criteria of paragraph 12-7 of reference (a). Further a JAGMAN investigation is still required if the PI results is serious disciplinary action or prosecution is contemplated against any person(s) believed responsible for the compromise of classified information. The PI must be completed within 72 hours. If it is determined that a compromise or possible compromise did not occur, the inquiry will be terminated and no further investigative action is necessary. If, from the inquiry, it is determined that compromise, possible compromise, or a significant security weakness did occur, a JAGMAN investigation will be initiated by the CSO/ICO.

(2) If it is determined that a security regulation was violated but no compromise occurred, the CSM will ensure an investigation is conducted into the incident and corrective action is taken.

(3) All preliminary inquiries and JAGMAN investigations relevant to security violations/incidents will be forwarded to the CSO/ICO via the CSM for review. CSM endorsement shall include recommended corrective action.

b. JBPHH military personnel are subject to disciplinary action under the Uniform Code of Military Justice, or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of reference (a).

c. JBPHH civilian personnel are subject to criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of reference (a).

d. JBPHH personnel will report any incident affecting national security, involving themselves, their dependents, and others to the CSM or local NCIS. The CSM notify the NCIS Regional Office of such incidents so that effective counterintelligence measures can be taken. Incidents coming under this category include:

(1) Possible acts of sabotage, espionage, deliberate compromise, and other subversive actions.

(2) Requests through other than official channels, for classified or otherwise sensitive information from anyone regardless of nationality.

(3) Circumstances indicating that a staff member may be the target of exploitation by a foreign entity.

(4) Suicide or attempted suicide by command members who have had access to classified information.

(5) Unauthorized absence of staff member(s) who have had access to classified information and whose activities, behavior, or associations may be inimical to the interest of national security.

8. Classification Management. Information that requires protection against unauthorized disclosure in the interest of national security must be classified in one of three following designations: Top Secret, Secret, or Confidential. The authority to originally classify information as Top Secret, Secret, or Confidential rests with the Secretary of the Navy (SECNAV) and his designees.

a. All of the classified documents generated by authorized JBPHH personnel contain derivative classified information vice original classified information. Derivative classified information is paraphrased, restated, or incorporated information that has already been classified by an Original Classification Authority (OCA). Classified information extracted from a classified source will retain the classification marking exactly as shown on the source material.

Also, by means of access to the SIPRNET individuals have the capability of derivatively classifying information. Derivative classifiers are required to be trained by the CSM prior to exercising their authority. Training will help facilitate proper classification decisions and reduce the proliferation of electronic spillages on IT systems. Any questions concerning proper classification, markings, downgrading of instructions, etc., will be referred to the CSM for resolution. The CSM will review all command-generated classified documents for proper classification and markings, as required by references (a) and (b).

9. Accounting and Control. Classified information must be afforded a level of accounting and control commensurate with the degree of damage the national security that might result from unauthorized disclosure. The following protective standards have been established for classified material received, maintained, and developed by JBPHH.

a. Top Secret. If Top Secret material, correspondence, or message is received, it will be receipted for, routed, and dispatched by the CSM (i.e, serves as TSCO). The material will be reviewed and appropriately marked, and administrative control will be in accordance with reference (a). All Top Secret material will have a continuous chain of custody and will be stored in an approved Top Secret security container.

b. Secret and Confidential. All Secret and Confidential material (other than messages) will be receipted for, opened, logged, reviewed by appropriate markings, routed, and dispatched by the Program addressee's designated CMC. Secret and Confidential material will be receipted by Command Admin. Administrative control will be carried out per reference (a). During normal working hours the originator of an outgoing classified message is responsible for ensuring the markings/classification/declassification of the message is correct. The CSM will review for proper marking, if needed, per reference (a). After normal working hours, the message releaser is responsible for ensuring the markings, classification, and declassification of the message is correct. Classified messages and documents can only be processed on an approved classified IT system. Classified messages will be hand-carried through the chop chain. An appropriate classified level coversheet shall cover the message at all times.

c. An inventory of all classified material holdings within the command will be conducted upon change of command, relief or transfer of CMC, or when other circumstances warrant. A report of inventory will be submitted to the CSM and any discrepancies noted. Listings of classified holdings will be made and enclosure to the inventory report.

d. Classified Marking. Reference (a) provides detailed guidance for marking of correspondence and information processed on the SIPRNET, accounting and control, declassifying, and the destruction of classified storage IT media.

(1) IT Marking. Magnetic storage media and IT systems used for classified processing must be labeled using Standard Form color-coded label that clearly indicate the classification level.

(2) Accounting and Control. Classified IT storage media and output will be controlled in a manner equivalent to that provided classified documents of a similar classification. This includes classified laptops, removable hard-drives, CD-ROMs, etc.

(3) Declassifying. Declassified IT media must still be marked, safeguarded, and controlled at the highest level of classification recorded on them before they are declassified. Current policy is that once a media has been used for classified storage, the media will retain the markings and be used for classified processing, only, until destroyed.

e. Annual Clean-out. Every first Wednesday of October, a "clean-out" of unneeded classified material stored in security containers will be conducted. Specific attention and effort will be focused on the disposition and destruction of unneeded classified material. A report of inventory will be submitted to the CSM and any discrepancies noted. Listings of classified holdings will be made an enclosure to the inventory report. Declassified material will be destroyed by authorized means, (e.g., National Security Agency/Central Security Service (NSA/CSS) approved Cross-cut high security shredder or Infostroyer CD destruction sander) per reference (a).

10. Classified Meetings. Meeting or discussions involving classified information shall only be conducted in spaces approved as Open Secret Storage (OSS)/ Controlled Access Areas (CAA)/ Restricted Access Areas (RAA). Meeting organizers shall

ensure appropriate security measure are in place to protect classified information and meeting attendees are cleared to the level of classified information and have a NTK.

11. Configuration, Control, Management, and Security of Classified Information Systems.

a. There are three approved categories of classified workspaces at JBPHH: Mission Essential (essential for the JBPHH mission), Mission Support (supports the JBPHH mission), and General Purpose (used for classified office automation functions, i.e., email, correspondence, etc). Locations of these workspaces are as follows:

(1) Mission Essential Locations.

(a) JBPHH

- 1. Bldg 1200, Emergency Operations Center

(2) Mission Support Locations

(a) JBPHH

- 1. Bldg 150
 - a. Antiterrorism Force Protection Room 104
 - b. Port Operations Room 114
- 2. Bldg 278, Rooms 110, 110A, and 207

(3) Individual SIPRNET information systems are authorized for Officers, and Senior civilian staff.

(4) Other locations. Most of the daily SIPRNET use occurs in the Mission Essential and Mission Support classified workspaces. Classified spaces not list above will be reviewed to determine their role in supporting the JBPHH mission, number of users served, and if approved locations can serve the needs of the customer base. The Directorate that manages the space must be prepared to make substantial justification for continued sustainment of a classified workspace. The JBPHH CSM will make a recommendation to the CSO/ICO on maintaining the classified

workspace and if it should be added into the Mission Essential, Mission Support, or General Purpose category.

b. Visitor Access. Visitor access to all mission essential and mission support locations shall maintain a visitor log for all visitors from outside the command. Classified spaces shall be sanitized prior to allowing uncleared visitors inside and uncleared visitors shall be escorted at all times.

c. Configuration Management. Any changes to a classified workspace, information system, or information system infrastructure must be carefully reviewed. Unauthorized changes may lead to non-compliance with DOD classified information security policies and may result in decertification and removal of authorization to operate a classified workspace. Commanding Officer, Naval Facilities Engineering Command (NAVFAC) Hawaii is responsible for ensuring project plans for military construction (MILCON) and building renovations involving classified workspaces and/or infrastructure are reviewed by the NRH Configuration Control Board (CCB), CSM, and Information Assurance Manager (IAM).

d. Safeguarding

(1) Removable storage media (thumb drives, external hard drives) are prohibited from connecting to classified information systems.

(2) Classified material, including any information system (i.e., laptop computers and removable storage media including CD-ROMs, floppy disks, and Universal Serial Bus (USB) drives) removed from storage shall be marked accordingly and kept under constant surveillance by authorized personnel or stored in an approved security container.

(3) Classified information discussed in telephone conversations shall only be over secure communications circuits approved for transmission of information at the specific level of classification. When discussing classified information over the telephone, the ability of others in the area to overhear what is being said must always be considered.

e. Classified account holders must at a minimum, log in to their SIPRNET account at least monthly. Failure to do so will result in the account being marked as inactive and deactivated.

The deactivation process is automated and users will not receive prior notification of this action.

12. Incoming Classified Material

a. Procedures. All classified material received in the Command's Admin Office will be reviewed for appropriate dissemination, and control after consulting with the Admin Officer, Executive Assistant, or CSM. Each program code CMC will be responsible for accounting, control, dissemination, and safeguarding of classified material received and stored within the program's classified container(s).

b. Registered/Certified/Express Mail

(1) All registered mail addressed to the command will be routed through Admin Office personnel to see if it contains accountable classified material.

(2) Admin will review all material, sign, and immediately return the enclosed record of receipt card (received with Secret material). Should any discrepancy be found, the CSM is notified and a discrepancy report is sent to the originator.

(3) Incoming Mail Log. The following entries shall be made in the appropriate incoming mail control log:

- (a) Registered/Certified/Express Mail Number.
- (b) Originator.
- (c) Date Received.
- (d) Description (subject unclassified).
- (e) Control Number Assigned.
- (f) Signature.

(4) An OPNAV Form 5216/10 Correspondence/Material Control Form (MCF) shall be completed on all classified material received for routing other than messages. To maintain MCF forms as unclassified control documents, classified titles shall NOT be used on MCFs. The hard copy is retained for two years following the destruction of classified material with which they pertain.

c. Classified Messages. Only mission essential or classified messages of command interest will be retained and logged/controlled as part of the command classified inventory. All message traffic, except Top Secret, is received using the standard messaging system.

13. Outgoing Classified Material

a. The basic purpose of applying classification markings to documents and other material is to communicate to the recipient the degree of protection required. Standard classification markings, as specified in reference (a), will be used by all initiators of classified materials. JBPHH does not have OCA, therefore, all classified material originated with JBPHH will be derivative classified material.

b. When preparing classified material for mailing, the following guidelines shall be followed:

(1) Classification authority and downgrading instructions shall be indicated on the first page of all classified material. This includes cover letter and each enclosure that can be used separately. For example: If the cover letter is classified and it transmits three classified enclosures, the cover letter will have classification authority and downgrading instructions on its first page, and each enclosure will also have on its first page the classification authority/downgrading instructions for the material it contains. If the cover letter is marked "Unclassified upon removal of enclosure(s)," it does not require downgrading instructions and declassification.

(2) Prepare a Record of Receipt Card (OPNAV 5511/10) for each Secret material being mailed.

14. Working Papers

a. Working papers are documents, including drafts, notes, charts, maps, photographs, etc., created or accumulated to assist in producing a finished document. Working papers that contain classified information shall be:

(1) Dated when created.

(2) Marked with the highest classification of contents.

(3) Protected at the level of classification.

(4) Destroyed when they are obsolete, suspended, or no longer needed for reference.

b. Working papers will be accounted for, controlled, and marked in the same manner as a finished document when one or more of the following occurs:

(1) Released outside the command.

(2) Retained for more than 90 days.

(3) Retained in file permanently.

(4) Contains Top Secret information.

15. Reproduction/Printing of Classified Material. The number of reproduced or printed Secret and Confidential Material from a SIPRNET printer must be kept to the absolute minimum required to accomplish the mission.

a. The reproduction of classified material is authorized in the following locations using the copier or printer authorized to print up to SECRET material:

(1) Bldg 150: Rooms 104, 114.

(2) Bldg 1200: EOC

(3) Bldg 278, Room 207.

b. Each program requiring the reproduction of classified information will designate a limited numbers of staff personnel appropriately cleared, as authorized to reproduce classified material.

c. Classified information reproduced and printed must have administrative security controls in place. Security controls of reproduced and printed copies of classified material are the same as the originals and must maintain administrative control in accordance with reference (a). Reproduced copies must show the classification and other special markings that appear on the originals. Any samples, waste, or over-runs resulting from the reproduction process must be shredded by a cross-cut security

shredder approved by NSA/CSS, as identified by the CSM approval sign affixed to the machine. After reproducing the classified material, or if the machine malfunctions, a check of the reproducing machine and surrounding area will be conducted to ensure that all copies and originals are accounted for. Reproduced or copied material will be controlled by an OPNAV Form 5216/10 MCF for routing and record of destruction.

16. Secure Rooms (SR)/OSS/CAA/RAA.

a. Open storage areas constructed per Exhibit 10A of reference (a) shall be designated in writing by the CSM. The CSM is responsible for designating in writing the command's CAA and RAA associated with the protection of classified material and SIPRNET connectivity. Designation of a CAA or RAA will comply with the requirements of reference (e). It is a designation that the physical security standards for a CAA or RAA have been met. It is not certification of the Protected Distribution System (PDS) as that is the responsibility of the IAM. The CAA or RAA are for areas through which PDS carrying classified information traverse, such as SIPRNET. The CSM coordinates with the IAM and Security Officer to ensure connectivity; physical security protection devices such as Intrusion Detection System (IDS) and maintaining access control procedures are implemented and followed by room custodians.

b. Personnel working with classified material, hard copy or SIPRNET systems shall restrict the access to their space while present. All classified material including classified laptop IT systems must never be left unattended and must be stored in a GSA approved security container or SR/OSS when not in use.

c. Command and personal electronic devices such as cell phones, cameras, IPADs, laptops, any transmitting wireless device, etc., are not authorized at anytime in rooms designated SR/OSS/CAA and RAA while classified processing in progress.

d. Unrestricted Areas. All other areas within JBPHH are authorized as general visiting areas and controlled by the Program Code owning the space.

17. Destruction of Classified Material. The following procedures will apply for the destruction of classified material in accordance with reference (a).

a. Top Secret Material. Top Secret material will be destroyed by the CSM/TSCO only.

b. Secret and Confidential Material. Classified material will be destroyed by authorized means in accordance with reference (a).

(1) Shredded by a cross-cut high security shredder approved by NSA/CSS, as identified by the CSM approval sign affixed to the machine.

(2) CD's will be destroyed using the Infostroyer CD destruction sander located in Bldg 150, Room 316 (Command Admin).

(3) Other authorized means identified in reference (a).

(4) Commercial shredding services will **NOT** be used for the destruction of classified material.

18. Visitor Control to Classified Spaces/Meetings. Requests for classified visits to the command will be coordinated through the CSM's office by the Program to be visited. Request for classified visits will be done through the DoD Joint Personnel Adjudication System (JPAS) only. Unclassified visitor access visits will be coordinated with the Program Code.

19. Physical Security. Program CMCs will ensure the following security procedures are followed:

a. Security Containers

(1) Programs shall contact the CSM before acquiring a security container to ensure it meets mandatory protection requirements. Security containers shall have a JBPHH container number posted on the front of the container for identification purposes; the number will be assigned by the CSM. The programs CMC, in coordination with the CSM, shall ensure all containers are marked before they are put into use for storing classified material and that the number is removed when such usage ceases. Relocation of classified containers must be reported to the CSM for inventory control purposes.

(2) The CSM is the custodian of all security container combinations maintained at the command. Combinations to all

security containers, SR/OSS spaces shall be changed upon transfer of personnel with access to the combination, or if a security violation/discrepancy has occurred, or annually, whichever comes first. Once the new combination has been set and tested, the Security Container Information Form (SF 700) will be completed and stamped with the highest classification for which the container provides protection. This record of combination will be sealed in the SF 700 and delivered to the CSM for storage. The CSM will only release the SF 700 to the CSO, or authorized custodians, as listed on the SF 700. The CSM will coordinate all security container lock combination changes.

(4) The SF 700 shall be posted inside the locking drawer of each classified material security container, listing the name of the custodian and alternate custodians. Security Container Check Sheet (SF 702) shall be affixed to the top or side of the security container and used to record all openings, closings, and end-of-day check. During the end-of-day check, the classified security container must be checked to make sure all classified material is properly secured, drawer closed, the dial of the combination lock rotated at least four complete times in the same direction, and level pulled down to ensure container locked properly. Security Container Check Sheet (SF 702) will be annotated with "NOT OPENED," initialed and dated in the "checked by" block.

b. Security Checks. As required by reference (a), a security check will be conducted at the end of "each" working day for each office that has a classified security container to make sure all classified material is properly secured. The SF 701, Activity Security Checklist, shall be used to record such checks. Individuals conducting security checks will make sure that:

(1) All classified material is stored in the manner prescribed.

(2) Burns bags are properly stored or destroyed.

(3) Classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts, and similar papers have been properly stored or destroyed.

(4) Security containers have been locked by the responsible custodian and SF 702 form annotated.

c. Procurement of new security containers, locks, or destruction equipment must be approved by the CSM prior to purchase.

20. Hand Carrying of Classified Material

a. Individuals hand-carrying classified material within the command building will use the appropriate cover sheet, SF 705, 705, 05 706, as applicable, to protect against the casual observation during transit.

b. To hand-carry classified material to another command/activity, a Courier Card briefing must be completed and Courier Authorization Card (CAC) issued by the CSM. To preclude potential security violations involving classified material within a personally owned vehicle, every effort should be made by the authorized courier to obtain a government vehicle while traveling with classified material by way of public roads. To hand-carry classified material onboard commercial aircraft, the person required to transport must have a Courier Card and a specific Letter of Authorization prepared by the CSM and signed by the CSO/CO. Every effort must be made to transfer classified information via a SIPRNET IT system. CACs will be issued to assigned personnel who routinely hand-carry classified material in the course of their official duties. The classified material will be double- wrapped. A briefcase or other container can be considered the outer wrapping. The inner wrapping will be stamped with the classification of the material contained therein and covered by a classification cover sheet (i.e. SF 703, 704, or 705, as applicable). If the classified material is to be transferred to another command/activity that is being hand-carried, the requirements of Chapter 9 of reference (a) will be followed.

c. Personnel must obtain authorization by the CSO/CO or CSM to hand-carry classified material while in a travel status, and only when the appropriate Program has verified that the material:

(1) Is required at the traveler's destination.

(2) Is unavailable at the command to be visited.

(3) Cannot be transmitted by a SIPRNET IT system or other authorized means due to time or other constraints.

d. The CSM will provide sequentially numbered CACs, DD Form 2501, for use by personnel who will be hand-carrying classified material. The DD 2501 will be issued to an individual and will expire three years from the date of issue. Prior to issuance of a DD 2501, the Courier must receive a "JBPHH Courier Authorization Briefing" from the CSM.

e. CACs will be issued to assigned personnel who routinely hand-carry classified material in the course of official duties.

21. Personnel Security.

a. All personnel security actions for JBPHH personnel shall be serviced through the JBPHH Security Manager and NRH Personnel Security Specialist. Personnel security functions for JBPHH military, civilian and NAF employees are consolidated in BLDG 3456, 620 Main St, Honolulu, HI, 96818.

b. Personnel, military, and civilian assigned to JBPHH will be granted security clearance only when access is necessary to perform assigned duties and only at the level identified "NTK," established eligibility by the DOD Central Adjudication Facility (DOD CAF) or other approved adjudicating authority and executed Classified Information Nondisclosure Agreement (SF 312) and whom there is no known un-adjudicated disqualifying information.

c. NTK is a preventative measure to identify and deter unauthorized access. Knowledge, possession of, or access to classified information is not provided to any individual solely by virtue of the individual's office, rank, or position. Although access can only be authorized for individuals with established security clearance eligibility at or above the level of classified information required, having security clearance eligibility **DOES NOT** equate to NTK.

d. Personnel security clearance determination for access to classified information will be the responsibility of the CSM. Supervisors will submit a "JBPHH Security Clearance Request" form 5521/8 to the CSM requesting security clearance for assigned military or civilian personnel or for personnel which a change in their security clearance is required. Per reference (b), the CSM will conduct a Continuous Evaluation Program (CEP) check of any un-adjudicated disqualifying or derogatory information pertaining to the individual and make a decision on

the individual's continued ability to maintain access to the command's classified material, consistent with the requirements of reference (b). Any dispute between the Program and CSM relative to not granting security clearance to support their mission will be forwarded to the CSO/ICO for final determination.

e. Prior to being granted temporary (also referred to as interim clearance or interim access) or final security clearance, JBPHH personnel must execute an SF 312, Orientation and CEP Briefing.

(1) As part of the Human Resources Service Center (HRSC) HI applicant tentative job offer process for civilian positions requiring access to classified information in the performance of official duties, the CSM will conduct a CEP review to determine if access to the command classified material can be granted upon the prospective hire start date.

f. Once command access is granted, the security clearance eligibility becomes a security clearance (e.g., eligibility + access = security clearance). Security clearances will not be granted and retained for administrative convenience or for inadvertent or casual access.

g. Supervisors will ensure that a system of "continuous evaluation" of eligibility for their personnel's access to classified information is established within their areas of responsibility.

(1) A personnel security investigation is required for all government employees which examines of a sufficient amount of information regarding each individual to determine whether the individual is an acceptable security risk. When an employee is granted access, continuous evaluation for personnel security risks relies on all personnel within the command to report questionable or unfavorable information that may be relevant to a security clearance or background investigation determination to the supervisor or CSM. Examples of such behavior could include but not limited to are:

- Illegal Drug use
- Alcohol abuse/DUI
- Excessive indebtedness
- Acts of violence
- Theft

- Sabotage/Vandalism
- Threats
- Unexplained affluence (expensive cars, home, travel, dining out, entertaining, etc)
- Non-compliance with security requirements
- Mental, emotional, or personality disorders
- Sexual behavior that is criminal or reflects a lack of judgment or discretion
- Foreign influence concerns/close personal association with foreign nationals or nations
- Engagement in outside activities that could cause a conflict of interest
- Misuse of government IT systems

(2) Individuals are required to report to their supervisor or CSM for any situation or incident that could affect their continued eligibility for access to classified information or favorable background investigation determination. The ultimate responsibility for maintaining eligibility to access classified information or a favorable background investigation rests with the individual. Additionally, co-workers have an obligation to advise their supervisor or Security Manager when they become aware of potentially unfavorable information that could impact their co-workers security clearance or background investigation determination. Failure to report any incident becomes an incident itself and could affect the employee's future command favorable background investigation which is a condition of employment.

h. Command personnel security clearance information is recorded in JPAS, TWMS, and local SMO data base. The individual and Program's Authorized Managers, supervisors, and administrators may view security clearance and investigative information via TWMS.

i. When a requirement exists for a personnel security investigation, reinvestigation, or a Periodic Reinvestigation (PR), the CSM will notify affected personnel via email.

j. If a clearance is not needed for official duties, it will be administratively withdrawn by the CSM. This does not affect the individual's security clearance "eligibility." Security clearance eligibility indicates the member has a favorably adjudicated PSI, and there is no known un-adjudicated disqualifying or derogatory information, the member is eligible for the clearance level supported by the PSI.

k. Position Sensitivity. In order to provide the appropriate level of background investigation and suitability adjudication, positions are designated according to potential risk. 5 CFR, 732.201 requires that National Security positions, hereafter referred to as sensitive positions, be formally designated for federal civilians according to the position whose occupant could bring about, by virtue of the nature of the position, an adverse effect on national security. There are three sensitivity levels and one non-sensitive level. Sensitivity levels must be designated as Special-Sensitive, Critical-Sensitive, or Non-Critical Sensitive. This must be done in accordance with Chapter 5 of reference (b). A Civilian Position Sensitivity (PS) Checklist will be completed for each civilian position and placed in their security file.

l. Unfavorable Personnel Security Determinations. DOD CAF is the single DOD authority for making favorable and unfavorable eligibility determinations. The employing command is responsible for making the basic employment suitability determinations and evaluating potential nexus issues using personnel suitability regulations, however, only the DOD CAF can make a determination that an employee is ineligible to occupy a sensitive national security position based on reference (b).

(1) When an unfavorable personnel security eligibility determination is being contemplated by the DOD CAF, they will issue to the individual concerned a Letter of Intent (LOI) to revoke or deny security clearance eligibility. The LOI advises the individual of the proposed action, the reasons therefore and the rebuttal process associated with the proposed action. The CSM will serve as the command security official responsible for acknowledging receipt and complying with instructions contained in correspondence (DOD CAF LOI, Letters of Denial (LOD), or CNO (09N2) Personnel Security Appeals Board (PSAB) letters), related to unfavorable determinations appropriate.

(a) The CSM will immediately present the LOI to the individual and assume a direct role in facilitating their "due process." Determine the individual's intent regarding a response to the LOI and immediately complete and return the Acknowledgement and Receipt of the LOI accompanying the LOI, to the DOD CAF indicating whether the individual intends to submit a response to the contemplated action and whether the command has granted an extension of time to submit the response. The LOI advises the individual that if they choose not to respond,

absence an approved extension, or if the response is untimely, they will forfeit their right to appeal.

(b) Assist personnel who are undergoing the unfavorable determination process, by explaining the personnel security eligibility determination process, providing the appendix (g) adjudication criteria used by DOD CAF and providing guidance on obtaining pertinent information used in the DOD CAF proposed determinations.

(c) Review the information contained in the LOI to determine whether the individual's access to classified information should be suspended while the unfavorable determination process continues. Individuals with interim or temporary access will have their access removed immediately. All suspension actions will be accomplished as specified in Chapter 9 of reference (b).

1. If the DOD CAF makes an unfavorable determination, the individual will be notified in writing, via the CSM, citing all factors that were successfully mitigated by the individual's response to the LOI and what unfavorable factor(s) remains to cause the unfavorable determination. The LOD will be sent via the command with a copy to Navy Personnel Command (NAVPERSCOM) (PERS-483) for military members, as appropriate. The final decision will be reflected in JPAS.

2. The LOD will inform the recipient of his/her appeal rights. Upon receipt of the LOD, the command must ensure the individual no longer occupies a sensitive position and has no further access to national security information, as the individual has been determined to no longer meet the requirements for access to national security classified information. The CSM will ensure final DOD CAF unfavorable personnel security eligibility determinations are immediately coordinated with the Program Supervisors and Human Resources Specialists so that necessary actions are quickly taken to officially remove personnel accordingly from access to classified information and assignment to sensitive duties.

3. Continuously evaluate command personnel with regard to their eligibility for access to classified information and/or assignment to a sensitive position, applying the criteria outlined in Exhibit 10A of reference (b).

a. Forward all potentially disqualifying information to DOD CAF via JPAS. DOD CAF will review the information and reevaluate the individual's clearance eligibility using the appendix (g) adjudicative guidelines.

b. Ensure individuals are appropriately referred to command assistance programs: Civilian Employee Assistance Program (CEAP) and Military and Family Services Center (MFSC) as issues dictate.

c. Suspend individual's access to classified information for cause when warranted, and notify the DOD CAF within 10 days upon receipt of supporting documentation. Once access is suspended and reported to DOD CAF, it may only be reinstated by the DOD CAF.

22. Industrial Security. CSO shall establish an industrial security program, in accordance with Chapter 11 of reference (a) if their command engages in classified procurement with U.S. industry, educational institutions or other cleared U.S. entities, both at the prime and sub-prime level, hereafter referred to as "contractors," or when cleared DOD contractors operate within areas under their direct control. Command security procedures shall include appropriate guidance, consistent with reference (a), to ensure classified information released to industry is safeguarded.

a. The National Industrial Security Program (NISP) for safeguarding information classified under reference (a) that is released to industry. Reference (f) implements the requirements of the NISP within the DOD. Provisions of this policy manual relevant to operations of contractor employees entrusted with classified material shall be applied by contract or other legally binding instrument.

b. Contractors may perform work on and visit shore installations in one of the following ways:

(1) When the ICO determines that the contractor is a short or long-term visitor, he shall require that the visitor comply with command security regulations and the CSM shall include them in the command security education program.

(2) When the contractor is a tenant aboard the installation, i.e., has sole occupancy of a facility or space controlled and occupied by the contractor, the host command may

assume responsibility for security oversight over classified work carried out by the cleared DOD contractor employees in these facilities. The command is responsible for all security aspects of the contractor operations in the facility. Oversight cannot be split between the ICO and Defense Security Service (DSS). The contractor is considered a tenant and is obligated to comply with DOD regulations and applicable portions of reference (f).

(3) Coordinate with JBPHH Program Managers to review Statement of Work (SOW) to ensure access to or receipt and generation of classified information is required for contract performance.

(4) Ensure that a Contract Security Classification Specification (DD 254) is incorporated into each classified contract. Validate security classification guidance, complete, and sign the DD 254.

(a) Coordinate review of the DD 254 and classification guidance.

(b) Issue a revised DD 254 and other guidance as necessary.

(c) Resolve problems related to classified information provided to the contractor.

(d) Provide, in coordination with the Program Manager, any additional security requirements, beyond those required by the National Industrial Security Program Operating Manual (NISPOM), in the DD 254, or in the contract documents itself.

(e) Initiate all requests for Facility Clearances (FCL) action with the DSS. Verify the FCL and storage capability prior to release of classified information.

(f) Coordinate, in conjunction with the appropriate transportation element, a suitable method of classified shipment when required.

c. Contractor Fitness Determination for Public Trust Positions. Contractors who access sensitive unclassified information and does not require clearance eligibility from a DON IT-II (Limited Privileged) and IT-III (Non-Privileged)

systems (e.g., NMCI), and prior to CAC-issuance will require, at a minimum, favorable advanced Federal Bureau of Investigation (FBI) fingerprint results. A subsequent favorably adjudicated National Agency Check plus Written Inquiries (NACI) or higher level scope: National Agency Check with Law and Credit Check (NACLIC), Access National Agency Check with Inquiries (ANACI) investigation, as applicable will be completed for U.S. citizens, adjudicated, recorded, and maintained in JPAS by the DOD CAF. Contractors will be subject to a NACLIC investigation for DON IT-II (Limited Privileged) public trust positions.

d. Background vetting for CAC-eligible Contractors. Homeland Security Presidential Directive (HSPD-12) and one of its more influential directives, the DTM 08-003 requires the CAC-eligible contractor population be background vetted.

(1) The CSM will notify JBPHH Program Managers, Contractor Verification System (CVS) Trusted Agents, Contracting Officer Representatives (CORs), Contractor's Facility Security Officer (FSO) and contractors of the investigative results and DOD CAFs adjudicative decision by written correspondence.

(2) Deny or restrict admittance to command areas, as deemed appropriate, when disqualifying information regarding the contractor is obtained from results of the background investigation. The CSM will notify JBPHH Program Managers, Contractor's FSO, and Contractor via written command correspondence.

(a) Contractor's may obtain a copy of their background investigation from the Office of Personnel Management (OPM), under the Freedom of Information Act (FOIA).

23. Security Inspections

a. The CSM shall conduct an inspection semi-annually to ensure command compliance with DOD information security directives. Inspection results will be forwarded to JBPHH CSO, JBPHH Directorate, and ICO.

b. All personnel shall maintain good information security awareness through continuous demonstration of security practices outlined in references (a) through (g).

c. The CSM shall make random inspections of security containers and spaces to ensure daily checks are completed and documented.

24. Emergency Classified Materials Destruction Plan.

a. This section publishes procedures to be followed for safeguarding classified information and equipment during emergency situations. Emergency situations may be categorized as:

(1) Natural. An emergency which results from a natural disaster such as fire, flood or hurricane.

(2) Bomb Threats. All bomb threats must be closely evaluated and reported to the CDO to prevent unacceptable disruption to normal operations.

(3) Hostile or Dissident Action. An emergency which results from enemy action or hostile forces, mob or riot action.

b. Emergency destruction of classified material, including NATO classified material, held by JBPHH will be per the following procedures and as directed by the base commander. In extreme emergencies, the destruction of classified material may be initiated by the CDO. The following procedures will be implemented:

(1) During duty hours (0700-1630), Monday-Friday:

(a) Under normal circumstances, JBPHH will order the Emergency Destruction Plan implemented when it is considered that the forces and facilities at his disposal are inadequate to protect the subject materials from impending loss or capture. Should conditions prevent contact with the CSO/ICO, the Command Duty Officer (CDO) is authorized to initiate the plan without awaiting specific orders. The exercising of individual initiative in preparing for emergency action at all levels of command is desired.

(b) The Security Watch will restrict access to the building closing off all but the main entrance. All personnel entering the building will be checked for proper identification.

(c) The CDO shall immediately notify all individuals listed on the recall bill. If an individual on the recall bill can not be contacted, the next ranking individual having access to departmental classified information will be notified of the need to prepare for the possible destruction of classified material held in the department.

(d) In an extreme emergency, anyone within the department having access to classified information can be directed to implement destruction procedures in the absence of personnel listed on the recall bill.

(2) During non-working hours, the CDO will:

(a) Notify the CSO/ICO and the CSM.

(b) Execute the recall bill.

(c) The CSM, if available, will direct the safeguarding and destruction of classified material. If the CSM is not available, the CDO will direct the destruction of classified material as required.

(3) The destruction of classified material will be by burning in the dumpsters at the rear of Bldg 150.

c. Natural Disasters.

(1) General. Since emergencies of a natural nature would not normally subject the material to capture by enemy forces, securing of classified material as directed, should suffice.

(2) Protecting. When ordered to secure classified materials, all hands will ensure that classified documents are immediately placed in security containers. Under ideal conditions, all classified material will be returned for stowage.

(3) Fire. Command instructions provide detailed procedures for personnel discovering, reporting, or combating a fire within the JBPHH area. Upon notification of a fire all personnel, prior to evacuation, will secure all classified material. If it is not possible to safely secure the classified material, it will be left in place. Under no circumstances will

personnel risk death or injury to protect classified materials from fire. Base police will provide a perimeter guard for the building to control access to the area. This guard will continue until the fire has been extinguished and safety permits the CSM/SA to ensure that all classified materials have been totally destroyed. In the event firefighters or subsequent investigative personnel enter a classified space with exposed classified material, it shall be the responsibility of the officer directly in charge of that space to ensure that those firefighters/investigators are debriefed per current Navy security instructions.

d. Bomb Threats. Upon order to evacuate the building, all classified material will be secured. The primary consideration is the safety and welfare of all personnel. If it is not possible to safely secure or remove the classified material, it will be left in place. Under no circumstances will personnel risk death or injury to protect classified materials.

e. Hostile Action. When hostile action occurs, it must be assumed that classified material is an objective and all actions must be directed at keeping the materials from unauthorized personnel by means of protecting or destroying as conditions dictate.

25. Foreign/Local Nationals. Foreign/local nationals (non-U.S. citizens) are not allowed in classified spaces without an escort and without a purpose. Spaces shall be sanitized prior to escorting foreign/local nationals into any classified space. Under no circumstances shall foreign/local nationals be left unattended in a classified space or exposed to classified material, equipment, or information.

26. Forms. The following Security forms may be obtained through the Navy Supply System:

- a. OPNAV 5216/10, Correspondence Material Control, S/N 0107-LF-052-1650
- b. OPNAV 5511/10, Record of Receipt, S/N 0107-LF-008-8000
- c. OPNAV 5511/12 Classified Material Destruction Report, S/N 0107-LF-055-1160
- c. DD 2501, CAC, S/N 0102-LF-000-6900

- d. SF 700, Security Container Information Form
- e. SF 701, Activity Security Checklist
- f. SF 702, Security Container Check Sheet
- g. SF 703, Top Secret Cover Sheet, 7540-01-213-7901
- h. SF 704, Secret Cover Sheet, 7540-01-213-7902
- i. SF 705, Confidential Cover Sheet, 7540-01-213-7903


S. KEEVE

Distribution:

<https://g2.cnmc.navy.mil/tscnrh/JOINTBASEPEARLHARBOR-HICKAMHI/JBPHH%20Instructions/Forms/Instructions.aspx>
Electronic only, via JBPHH Gateway