



**BUREAU OF NAVAL PERSONNEL
and
NAVY PERSONNEL COMMAND
SECURITY PROGRAM**



DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON TN 38055-0000

BUPERSINST 5510.61E
BUPERS-00T5
17 Apr 2026

BUPERS INSTRUCTION 5510.61E

From: Chief of Naval Personnel

Subj: BUREAU OF NAVAL PERSONNEL COMMAND SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.36B
(b) OPNAVINST 3432.1A
(c) SECNAVINST 5510.30C
(d) OPNAVINST 5510.60P
(e) OPNAVINST 5510.165B
(f) BUPERSINST 5211.7A
(g) DoD Directive 5205.02E of 20 June 2012
(h) DoDM 5205.02 DoD Operations Security (OPSEC) Program Manual
(i) SECNAVINST 5510.37B
(j) JP 3-55
(k) CJCSI 3213.01D
(l) SECNAVINST 3070.2A
(m) DoD Instruction 5200.48

1. Purpose. To establish policy and provide guidance for information, operations, and personnel security as implemented by the Bureau of Naval Personnel (BUPERS) Command Security Program. Major revisions to this instruction include clarification so that no foreign national personnel will be granted system access to any BUPERS Millington or Navy Personnel Command (NAVPERSCOM) systems, nor will they be granted unescorted access to BUPERS Millington or NAVPERSCOM buildings. It also replaced mental health stigmatizing language concerning suicide and mental health conditions.
2. Cancellation. BUPERSINST 5510.61D.
3. Scope and Applicability. This instruction supplements the basic guidance of references (a), (b), and (c). Provisions of this instruction apply to all BUPERS and NAVPERSCOM military, civilian, and contract personnel and activities located on board Naval Support Activity Mid-South. BUPERS personnel located in Washington, DC are subject to provisions of reference (d).
4. Objective. To ensure maximum uniformity and effectiveness in the application of the Chief of Naval Personnel (CHNAVPERS) policies for BUPERS Information, Operations, and Personnel Security Programs (PSP) compliance per references (a) through (m).

5. Discussion. An effective command information security program (ISP) and PSP must receive attention and direction from all echelons within the chain of command. Properly trained and equipped personnel must carry out the BUPERS Millington/NAVPERSCOM Security Program.

6. Responsibilities

a. All BUPERS commanders, commanding officers, and officers in charge are responsible for compliance and implementation of references (a) through (l) within their commands and their subordinate activities.

b. Each individual (military, civilian, or contractor) employed by the Navy is responsible for compliance with references (a) through (l).

7. Action. BUPERS commanders, commanding officers, and officers in charge must ensure a comprehensive command security program is developed and implemented per references (a) through (l) within their organization. Careful consideration must be given to ensure all personnel employ continuous evaluation measures to mitigate insider threats per references (b) and (e).

a. Commands must ensure the results of all required self-inspections, security violation investigations, and operations reporting requirements are forwarded through the chain of command per references (a) through (c).

b. Development of all security program areas, with a focus on ISP and Operations Security Program (OSP), must also incorporate the requirements delineated in reference (f) to ensure all types of sensitive information are properly handled and safeguarded.

c. Commands must generate a critical information and indicators list (CIIL) and ensure all assigned personnel are aware of the sensitive information handled by the command. Appendix A is BUPERS Millington/Navy Personnel CIIL and serves as an example for subordinate commands to follow.

d. Commands are to provide a copy of their security program instruction, along with their security managers' and operations security managers' names and letters of designation to BUPERS Security Manager (BUPERS-00T5), 5720 Integrity Drive, Millington, TN 38055-5340.

8. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned for the standard subject identification codes (SSIC) 1000 through 13000 series per the records disposition schedules located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at <https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx>.

17 Apr 2026

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local records manager or the DON/AA DRMD program office.

9. Review and Effective Date. Per OPNAVINST 5215.17A, BUPERS-00T5 will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of War (DoW), Secretary of the Navy (SECNAV), and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

10. Forms. See appendix B for forms applicable to this instruction.



K.M. KENNEDY

Deputy Chief of Naval Personnel

Releasability and distribution:

This instruction is cleared for public release and is available electronically only via BUPERS Web site, <https://www.mynavyhr.navy.mil/References/BUPERS-Instructions/>.

TABLE OF CONTENTS

CHAPTER 1 - GENERAL REGULATIONS AND ORGANIZATION

0101. Scope.....	1-1
0102. Command Responsibility and Authority	1-1
0103. Security Manager/Officer Responsibilities.....	1-1
0104. Assistant Commanders Navy Personnel Command (ACNPC) and Special Assistant (SA) Responsibilities.....	1-3
0105. Security Inspections and Security Assist Visits.....	1-4
0106. Security Servicing Agreements (SSAS)	1-4
Exhibit 1 - Security Assistant Designation Letter.....	1-5

CHAPTER 2 - SECURITY AWARENESS AND EDUCATION

0201. General.....	2-1
0202. Scope.....	2-1
0203. Responsibilities.....	2-1
0204. Security Training Requirements	2-1

CHAPTER 3 - LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

0301. General.....	3-1
0302. Reporting Loss or Compromise	3-1
0303. Preliminary Inquiry.....	3-1

CHAPTER 4 - COUNTERINTELLIGENCE MATTERS

0401. Matters To Be Reported.....	4-1
0402. Liaison With Investigative Agencies	4-1
0403. Suicide Or Attempted Suicide	4-2
0404. Unauthorized Absentees	4-2

CHAPTER 5 - CLASSIFICATION MANAGEMENT

0501. Classification Management Policy	5-1
0502. Security Classification Guides.....	5-1
0503. Downgrading, Declassification, And Upgrading.....	5-1
0504. Marking Requirements.....	5-1
0505. Warning Notices	5-1

CHAPTER 6 - CONTROL OF CLASSIFIED INFORMATION

0601. General.....	6-1
0602. Access To Classified Information.....	6-1
0603. Classified Information Control	6-2
0604. Accountability And Control.....	6-2
0605. Copying Classified Documents.....	6-4
0606. Handling Precautions and Office Practices.....	6-4
0607. Control Of Classified Working Papers or Preliminary Drafts	6-5
0608. North Atlantic Treaty Organization (NATO) Material.....	6-5
0609. Classified Contract Management.....	6-6

CHAPTER 7 - SECURITY STORAGE

0701. Security Container Custodian	7-1
0702. Combinations	7-1
0703. Classified Information Storage	7-1
0704. Classified Storage Equipment.....	7-1
0705. Locking Procedures	7-1
0706. Daily Security Inspection.....	7-1

CHAPTER 8 - TRANSMISSION AND TRANSPORTATION

0801. General.....	8-1
0802. Transmission And Receipt of Classified Information	8-2
0803. Electronic Transmission of Classified Information	8-2
0804. Processing Classified Information on BUPERS Millington/NAVPERSCOM Computers.....	8-2
Exhibit 8A - Authorization To Transport Classified Information	8-3
Exhibit 8B - Authorization To Hand- Carry Classified Information Aboard Commercial Passenger Aircraft.....	8-4

CHAPTER 9 - DESTRUCTION OF CLASSIFIED INFORMATION

0901. General.....	9-1
0902. Destruction Reports	9-1

CHAPTER 10 - EMERGENCY PLANNING

1001. General.....	10-1
1002. Secure The Information	10-1
1003. Remove The Information.....	10-1

1004. Destroy The Information..... 10-2
1005. Implementing Authority..... 10-2

CHAPTER 11 - VISITS AND MEETINGS

1101. General..... 11-1
1102. Incoming Visits..... 11-1
1103. Outgoing Visits..... 11-1
1104. Visits To Contractor Facilities..... 11-2
1105. Visits By Representatives of The General Accounting Office (GAO)..... 11-2
1106. Visits By Foreign Nationals..... 11-2
1107. Visits To Foreign Countries..... 11-2
1108. Classified Meetings..... 11-3

CHAPTER 12 - PERSONNEL SECURITY

1201. General..... 12-1
1202. Responsibilities..... 12-1
1203. Position Sensitivity..... 12-1
1204. Requirements For Access and Clearance Eligibility..... 12-1
1205. Continuous Evaluation of Eligibility..... 12-2
1206. Proof of U.S. Citizenship for Security Clearance/Access..... 12-3
1207. Temporary And One-Time Access..... 12-3
1208. Denial Or Revocation of Clearance/Access for Cause..... 12-3
1209. Suspension Of Access for Cause..... 12-3
1210. Terminating, Withdrawing or Adjusting Access..... 12-3
1211. Security Termination Statement..... 12-4
1212. Clearance Of Personnel Not Regularly Assigned..... 12-4

CHAPTER 13 – OPERATIONS SECURITY

1301. General..... 13-1
1302. Responsibilities..... 13-3
1303. Countermeasures..... 13-6
1304. Internet Use..... 13-7
1305. Summary..... 13-8

CHAPTER 14 - BUILDING SECURITY REGULATIONS

1401. General..... 14-1
1402. Security Hours..... 14-1

1403. Background 14-1
1404. Common Access Card (CAC)..... 14-1
1405. Admittance 14-1
1406. Property Passes 14-2
1407. Loss Of Property, Thefts, And Other Irregularities 14-2
1408. Photography And Audio Recording Equipment/Devices 14-3

Appendix A - BUPERS Millington/Navy Personnel Command Critical Information And
Indicators List A-1

Appendix B - Forms Availability B-1

CHAPTER 1 GENERAL REGULATIONS AND ORGANIZATION

0101. Scope. This instruction establishes command security policies, responsibilities, and procedures to ensure all national security information (NSI) classified under authority of Executive Order 12958 is protected from unauthorized disclosure. No individuals will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made regarding their loyalty, reliability, and trustworthiness. A personnel security investigation (PSI) is conducted to gather information pertinent to these determinations. In the absence of specific reference to requirements within this instruction or other separate directives, provisions of references (a) through (d) apply.

0102. Command Responsibility and Authority

1. Chief of Naval Personnel (CHNAVPERS) is designated to administer the Information Security Plan, Operations Security Program (OSP), and Personnel Security Program (PSP) Bureau of Naval Personnel (BUPERS).
2. Deputy CHNAVPERS (DEP CHNAVPERS) is dual-hatted as Commander, Navy Personnel Command (COMNAVPERSCOM) and is responsible for the overall Security Program management for BUPERS/NAVPERSCOM Millington personnel and subordinate commands.
3. BUPERS Director, Business Operations (BUPERS-00T) will be assisted by the BUPERS Director, Security Division (BUPERS-00T5) in administering and enforcing the BUPERS Millington/NAVPERSCOM Security Program.
4. BUPERS-00T5 and subordinate personnel are responsible for the formulation, implementation, and enforcement of security programs, their effectiveness, and compliance with higher authority directives. BUPERS-00T5 is dual-hatted and is designated as security manager and security officer, per references (a) and (b), for BUPERS Millington and NAVPERSCOM.

0103. Security Manager/Officer Responsibilities

1. In addition to duties outlined in references (a) through (c), BUPERS-00T5 is responsible for the following:
 - a. BUPERS-00T5 is the principal advisor on the Information Security Program (ISP), OSP, and PSP in the command, and is responsible to COMNAVPERSCOM, via BUPERS-00T, for management, formulation, implementation, and enforcement of security policies and procedures for protection of classified information. Additionally, BUPERS-00T5 will assess the Security Program administration at all subordinate commands once every 3 years and present the findings through the BUPERS Office of the Inspector General (BUPERS-00IG).

b. BUPERS-00T5 duties are outlined in references (a) and (b) and are assisted by:

(1) BUPERS/NAVPERSCOM Antiterrorism/Force Protection and Security Awareness Officer (BUPERS-00T5C). BUPERS-00T5C is also designated as command mail manager and is responsible for:

(a) Establishing and maintaining an active security education program. The education program will be based on procedures and guidelines per references (a) and (b) and chapter 2 of this instruction;

(b) Conducting required training for orientation, security refresher, and foreign travel briefings;

(c) Coordinating, scheduling, and conducting any required annual security awareness training and coordinating the annual counterespionage briefing for all personnel having access to information classified as Secret or above;

(d) In the absence of the security manager, is designated as the assistant security manager.

(2) BUPERS/NAVPERSCOM Personnel Security (BUPERS-00T5D). BUPERS-00T5D is also designated as Top Secret Control Officer and North American Treaty Organization (NATO) Control Officer and is responsible for:

(a) Classified information control per reference (a);

(b) Processing BUPERS/NAVPERSCOM personnel (military and civilian) security investigations and investigations for public trust positions for contract personnel per reference (b);

(c) NATO briefing, debriefing, and information control per reference (a);

(d) Maintaining the ISP per reference (a);

(e) Maintaining list of position sensitivity and information technology (IT) designations per reference (b);

(f) Providing command security check-in and out process and building access for BUPERS/NAVPERSCOM personnel;

(g) Processing command visit requests (incoming and outgoing) and base access requests for incoming visitors;

- (h) Verifying personnel security clearances based on eligibility; has delegated authority to grant military and civilian personnel access to classified information;
- (i) Issuing courier cards or courier letters;
- (j) Executing security termination statements for individuals terminating active military service or civilian employment; and
- (k) Verifying type of security investigation, clearance level, and IT level designation using OPNAV 5239/14 System Authorization Access Request (SAAR).
- (l) Providing oversight and guidance for subordinate commands in areas related to personnel security and system management.

(3) Key Management Infrastructure (KMI)/Communications Security (COMSEC) Material System (CMS) Custodian (BUPERS-00T5H). BUPERS-00T5H is assigned as the command KMI manager. The KMI manager is responsible to the staff communications security material system responsibility officer (SCMSRO) and BUPERS-00T5 for management of the command KMI/COMSEC account per Electronic Key Management System (EKMS)-1 and is responsible for inventorying safes and safe combinations.

0104. Assistant Commanders, Navy Personnel Command (ACNPC) and Special Assistants (SA) Responsibilities

1. Designate a department security assistant in writing (see exhibit 1). Security assistants will be the focal point of all ISP, OSP, and PSP matters within their areas and are responsible for:
 - a. Receiving, storing, inventorying, reproducing, handling, dispositioning, and distributing classified information up to Secret;
 - b. Maintaining a listing of all personnel (military and civilian) showing the authorized access approved by BUPERS-00T5. Personnel listing must be continually evaluated by the security assistant to ensure personnel are eligible for access to classified information or assignment to sensitive duties. Discrepancies to personnel listing must be coordinated with BUPERS-00T5;
 - c. Forwarding NAVPERS 5520/6 Request for Security Access to BUPERS-00T5, via e-mail, for all personnel that need access to classified information; and
 - d. Being familiar with National Industrial Security Program for contract employees per reference (b), article 8-8.

2. Submit names of each department security assistant (including designated assistants with the specific duties they are authorized to perform) to BUPERS-00T5. This information, in the form of a consolidated list, is issued annually. Deletions and additions must be submitted in writing as they occur.

0105. Security Inspections and Security Assist Visits

1. Formal security inspections will be conducted by BUPERS-00T5 once every 3 years per BUPERS Inspector General (BUPERS-00IG) inspection schedule and results identified using reference (a) and reference (b).

2. Security assist visits will be conducted by BUPERS-00T5 upon request by any ACNP or SA. Security assist visits will be accomplished informally, and an informal report will be completed at the conclusion visit and forwarded to the requesting ACNPC or SA.

0106. Security Servicing Agreements (SSA). BUPERS-00T5 will have SSAs in writing when specified security functions are performed for other commands. These SSAs will be (as appropriate) for security functions being performed (e.g., information security (INFOSEC), personnel, and physical).

BUPERSINST 5510.61E
17 Apr 2026

5510
BUPERS or PERS Code
Date

Exhibit 1
A Designation as Department Security Assistant Letter

From: Director, ACNP or Special Assistant (BUPERS or PERS Code)

To: Rank, rating, or grade and full name of person being appointed

Subj: DESIGNATION AS DEPARTMENT SECURITY ASSISTANT

Ref: (a) BUPERSINST 5510.61D
(b) SECNAVINST 5510.36B
(c) SECNAVINST 5510.30C

1. Per reference (a), you are appointed as department security assistant for Bureau of Naval Personnel (BUPERS) (BUPERS-Code)/Navy Personnel Command (NAVPERSCOM) (PERS-Code). Your period of appointment will be from ____ until _____. You will be notified of any change in this appointment.
2. You will be required to become thoroughly familiar with references (a), (b), and (c) as applied to your department.
3. For effective management of the program, you will:
 - a. Serve as the department head's advisor and direct representative in matters pertaining to security, and serve as communications link between your department and BUPERS-00T5;
 - b. Develop written department security procedures, including an emergency plan. These procedures must be consistent with reference (a), chapter 10;
 - c. Coordinate and implement a security education program within your department;
 - d. Ensure threats to security, compromise, and other security violations are promptly reported to BUPERS-00T5;
 - e. Ensure your department's compliance with accounting and control of classified information including receipt, distribution, inventorying, reproducing, and dispositioning;

Exhibit 1 (Cont'd)
A Designation as Department Security Assistant Letter

Subj: DESIGNATION AS DEPARTMENT SECURITY ASSISTANT

- f. Forward visit clearance requests to BUPERS-00T5 within 30 days of visit;
- g. Ensure requests for carrying classified information outside the command are forwarded to BUPERS-00T5 for authorization;
- h. Ensure required protection is taken to prevent unauthorized disclosure of classified information to include meetings, carrying classified information, or casual discussion;
- i. Ensure you have an inventory of all General Services Administration-approved security containers (safes) within the department and a list of primary personnel responsible; and
- j. Ensure combinations to all security containers are safeguarded. SF 700 Security Container Information card will be completed with part 2 stored in a security container in BUPERS-00T5 security containers. SF 702 Security Container Check Sheet will be kept with each safe and secure room, showing when opened, closed, and checked. OPNAV 5510/21 Security Container Records form must be in all security containers and SF 701 Activity Security Checklist must be used to ensure daily checks for security containers are accomplished. Form completion is to be largely accomplished by the users, but will be checked and verified by the designated security assistant or other appointed departmental personnel.

SIGNATURE

Copy to:
NAVPERSCOM (BUPERS-00T5)

CHAPTER 2 SECURITY AWARENESS AND EDUCATION

0201. General. To establish policy, provide guidance, and set forth uniform standards for a security education and training program. A security education program must ensure that all personnel understand the need and procedures for protecting classified information.

0202. Scope

a. The success of the Information Security Program (ISP) and the PSP is dependent on a vigorous security education and training program. BUPERS Millington/COMNAVPERSCOM places strong emphasis on and promotes a continuing security education program within the command that increases effectiveness of security regulations and directives, instills security awareness in all personnel, and ensures a uniform interpretation and application of security standards. Security education applies to all personnel entrusted to protect classified information or who has access to Department of the Navy (DON) information systems.

b. BUPERS-00T5 is required to provide security education and training to all personnel having access to classified information or DON information systems. Some primary tools available to educate personnel are indoctrination, general military training (GMT), on-the-job training (OJT), command security personnel, and the internet. Effective use of these tools will ensure all personnel understand the need and procedures for protecting classified information and DON information systems. The goal is to develop fundamental security habits as a natural element of each task.

0203. Responsibilities. Supervisors, in coordination with BUPERS-00T5, are responsible for determining security requirements for their functions and ensuring personnel under their supervision understand security requirements for their particular assignment. OJT is an essential part of a command security education, and supervisors must ensure such training is provided. Department security assistants and BUPERS-00T5 will assist supervisors with this training. BUPERS-00T5 is responsible for planning, implementing, enforcing, and supervising the command's security education and training program.

0204. Security Training Requirements

1. Training. The following requirements will be standard for all command personnel:

a. Upon checking onboard, all personnel will receive orientation in basic principles of security and information systems.

b. All personnel assigned duties involving classified information will be immediately given a command security orientation brief.

c. All personnel will receive continuous security awareness through OJT and GMT by their supervisors, department security assistants, and information assurance managers (IAM).

d. Annual security refresher and counterintelligence briefings will be given to all personnel having authorized access to classified information.

2. Training Knowledge

a. Orientation. Through indoctrination, all personnel will know the following:

(1) Certain information, essential to national security, requires protection from disclosure to unauthorized persons;

(2) Classified information will be marked to show level of classification;

(3) Only those who have been officially and specifically authorized may have access to classified information;

(4) Personnel will be continually evaluated regarding their eligibility to access classified information, to be assigned to a sensitive position in support of continuous evaluation, and to combat the insider threat;

(5) Classified information must be stored, destroyed, and protected during transfer from one area to another, including electronic transfer per reference (a);

(6) Any compromise or other security violation must be reported to BUPERS-00T5;

(7) Any attempt by an unauthorized person, regardless of nationality, to solicit classified information must be reported;

(8) Command security structure (i.e., command security manager, Top Secret control officer, special security representative, IAM, department security assistant, etc.);

(9) Any special security precautions within the command, (i.e., restrictions on access to spaces or to certain equipment);

(10) Command security procedures for badging, security checkpoints, destruction of classified information, visitors, INFOSEC, command local area network (LAN), etc.;

(11) Their obligation to report suspected security violations or INFOSEC violations;

(12) Their obligation to report information that could impact security clearance eligibility of an individual who has access to classified information; and

(13) Procedures to follow in the event of an active shooter.

b. OJT. OJT is the phase of security education when security and information systems procedures for assigned position are learned. Supervision of the OJT process is critical. Supervisors are ultimately responsible for procedural violations or for compromises that result from improperly trained personnel. Expecting subordinates to learn proper security and information systems procedures by trial and error is not acceptable. OJT must be a daily practice at BUPERS/NAVPERSCOM.

c. GMT. Protection of classified information and information systems security GMT is mandatory for all personnel. Department security assistants and department training officers will coordinate this training with BUPERS-00T5.

d. Intranet. BUPERS-00T5 will maintain a Web site on the intranet providing all hands with available training opportunities and current command security and information systems policy and guidance.

3. Briefings

a. Refresher Briefings. Refresher briefings will cover:

(1) New security policies and procedures and continuous evaluation;

(2) Counter-intelligence reminders regarding reporting contacts and exploitation attempts and foreign travel issues; and

(3) Command-specific security concerns or problem areas. Results of self-inspections, inspector reports, or security violation investigations that provide valuable information for use in identifying command weaknesses.

b. Counterintelligence Briefings. These briefings will be coordinated with the local Naval Criminal Investigative Service (NAVCRIMINVSVC) and will contain updated information pertaining to foreign intelligence activities attempting to obtain classified information and will advise personnel of penalties for engaging in espionage activities.

c. Special Briefings. Special briefings will be required for the following circumstances:

(1) Foreign Travel Briefing. BUPERS-00T5 will conduct foreign travel briefings for all BUPERS/NAVPERSCOM personnel traveling overseas on official business. For BUPERS/NAVPERSCOM personnel transferring overseas, the briefing/training will also be provided to family members over the age of 14. Upon return of the travelers, they must report any incident, no matter how insignificant it may have seem, that could have security implications.

(2) New Requirement Briefing. Whenever security policies or procedures change, personnel whose duties would be impacted by these changes must be briefed as soon as possible.

(3) Program Briefings. Briefings that are specified or required by other program regulations (e.g., NATO, Single Integrated Operation Plan - Extremely Sensitive Information (SIOP-ESI), sensitive compartmented information (SCI), etc.).

4. Debriefings

a. A debriefing will be given to all personnel who no longer require access to classified information as a result of:

- (1) Transfers from one command to another when TS/SCI access will be removed;
- (2) Terminating active military service or civilian employment;
- (3) Temporarily separating for a period of 60 days or more, including sabbaticals, leave without pay, or transfer to the Inactive Ready Reserves (IRR);
- (4) Expiration of a limited access authorization (LAA);
- (5) Inadvertent substantive accesses to information that the individual is not eligible to receive;
- (6) Security clearance eligibility revocation; and
- (7) Administrative withdrawal or suspension of security clearance and SCI access eligibility for cause.

b. Debriefings will include all classified information in the possession of individual being returned and a complete review of SF 312 Classified Information Nondisclosure Agreement and Espionage Act, including penalties for disclosure. The individual must report any attempt by an authorized person to solicit classified information to NAVCRIMINVSVC, Federal Bureau of Investigations (FBI), or nearest Department of War (DoW) component without delay.

5. Security Termination Statements. Every security debrief, except when a person is transferring from one command to another, requires an OPNAV 5511/14 Security Termination Statement. Individuals must read and execute this statement at the time of debriefing and a witness to the person's signature must also sign the statement.

6. Duties and Responsibilities

a. BUPERS-00T5. BUPERS-00T5 manages the security education and training plan and reports directly to COMNAVPERSCOM via BUPERS-00T.

b. Department Heads. Department heads ensure all department personnel carry out the provisions of this instruction and provide necessary assistance to department security assistants and department IAMs in the execution of their duties.

c. Department Security Assistants. Department security assistants are responsible for:

(1) Providing security training for all personnel and assisting supervisors in OJT of command personnel regarding protection of classified information;

(2) Implementing a department security awareness training plan that will include monthly GMT for all personnel; and

(3) Coordinating with BUPERS-00T5 for training requirements.

d. All Hands. All hands must continuously monitor daily practices and habits. Ensure procedures set forth in this instruction are being performed and contact BUPERS-00T5 when there are any questions concerning security. Security awareness is an all-hands effort.

7. Reports. BUPERS-00T5 will provide BUPERS/COMNAVPERSCOM with an annual security training report, when requested, that includes dates of scheduled training, subject of security training, number of personnel required to attend, and number of personnel that were required to attend, but who did not.

CHAPTER 3
LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

0301. General. A loss or compromise exists whenever classified documents, information, or equipment are lost, disclosed to unauthorized persons, subjected to possible compromise, or when regulations for safeguarding such information are violated, whether or not actual loss or compromise occurs.

0302. Reporting Loss or Compromise. Any individual having knowledge of a suspected loss or compromise or unauthorized disclosure of classified information or other violations of security (deliberate or inadvertent) within BUPERS Millington/NAVPERSCOM will immediately report the facts to BUPERS-00T5. When a loss or compromise of classified information has occurred, BUPERS-00T5 will report loss or compromise to BUPERS-00T and NAVCRIMINVSVC. In the event of a spillage of classified materials on the Internet, the information assurance manager (IAM) will also be notified to initiate electronic spillage reporting procedures.

0303. Preliminary Inquiry. When a report of loss or compromise of classified information has been made, BUPERS-00T5 will submit a draft preliminary inquiry officer (PIO) appointment letter to BUPERS Office of Legal Counsel (BUPERS-00J) to assign a PIO, in writing, as the command official to conduct a preliminary inquiry per reference (a). The preliminary inquiry will be initiated and completed within 72 hours.

CHAPTER 4 COUNTERINTELLIGENCE MATTERS

0401. Matters To Be Reported

1. Basic Policy. Certain matters affecting national security must be reported to Naval Criminal Investigative Service (NAVCRIMINVSVC) so that appropriate counterintelligence action can be taken. All command personnel, whether they have access to classified information or not, will report to BUPERS-00T5 or to the nearest command, any activities of sabotage, espionage, international terrorism, or deliberate compromise involving themselves, their family members, co-workers, or others. Examples of request to be reported include attempts to obtain names, duties, personnel data or characterizations of Department of the Navy (DON) personnel, technical orders, manuals, regulations, base directories, personnel rosters or unit manning tables, and information about designation, strength, mission, combat posture, and development of ships, aircraft, and weapon systems. BUPERS-00T5 will, in turn, notify NAVCRIMINVSVC.

2. Foreign Travel

a. All command personnel possessing a security clearance are required to report to BUPERS-00T5 all personal foreign travel in advance of traveling. Supervisors will keep this reporting requirement in mind when they approve leave for their personnel and ensure individuals report to BUPERS-00T5. Personnel will be reminded of this reporting requirement during orientation security briefings and annual refresher security briefings.

b. See chapter 2, subparagraph 0204.3c(1), of this instruction for information regarding a foreign travel briefing.

c. When travel patterns (i.e., numerous expensive trips abroad or very frequent travel) or failure to report such travel indicate the need for investigation, BUPERS-00T5 will refer the matter to NAVCRIMINVSVC for action.

3. All personnel who possess a security clearance are to report to BUPERS-00T5 any form of contact with any individual, regardless of nationality, whether within or outside scope of individual's official activities in which illegal or unauthorized access is sought to classified or otherwise sensitive information. Personnel must report if they are concerned that they may be targets of exploitation. BUPERS-00T5 will review and evaluate the information and promptly report to NAVCRIMINVSVC.

0402. Liaison With Investigative Agencies. In all matters pertaining to processing security investigations or other investigations, BUPERS-00T5 will maintain official liaison with NAVCRIMINVSVC. All inquiries and visits by representatives of law enforcement or investigative agencies will be referred to BUPERS-00T5 and BUPERS-00J prior to making any disclosures.

0403. Suicide Or Attempted Suicide. When any individual who has access to classified information dies or attempts to die by suicide, the individual's department security assistant or supervisor must forward all available information to BUPERS-00T5 for reporting to NAVCRIMINVSVC with an information copy to the Defense Counterintelligence Security Agency Central Adjudication Services (DCSA CAF). Report will, at a minimum, set forth the nature and extent of classified information to which the individual had access and circumstances surrounding the suicide or attempted suicide.

0404. Unauthorized Absentees. When any individual who has access to classified information is in an unauthorized absentee status, the individual's department security assistant will notify BUPERS-00T5. Department security assistant will conduct an inquiry to determine if there are any indications from the individual's activities, behavior, or associations that their absence may be inimical to the interests of national security. Results of this inquiry will be submitted to BUPERS-00T5. If the inquiry reveals such indications, BUPERS-00T5 will report all available information to NAVCRIMINVSVC for action.

CHAPTER 5 CLASSIFICATION MANAGEMENT

0501. Classification Management Policy

1. Executive Order 12958 is the basis for classifying national security information (NSI).
2. Information classified by a Department of the Navy (DON) original classification authority (OCA) must be declassified when it no longer meets standards for classification in the interest of national security.
3. Reference (a) provides a detailed summary of classification levels and classification management.
4. BUPERS/NAVPERSCOM is not designated as an OCA.

0502. Security Classification Guides. Classification guides are approved personally and in writing by an official with appropriate OCA and cognizance over the information involved.

0503. Downgrading, Declassification, And Upgrading. Only OCAs are authorized to declassify, downgrade, and upgrade classified information. This is not to be confused with administrative responsibility of a holder of classified information to downgrade or declassify as directed by classification guides or instructions on a document. Further guidelines are provided in reference (a).

0504. Marking Requirements. All classified information handled by BUPERS/NAVPERSCOM must be clearly marked with appropriate classification level and all required "associated markings" per reference (a). This derivative classification will be made at the level that corresponds to the highest level of classification of any source documents. Declassification dates will reflect the latest date from any source material.

0505. Warning Notices. Warning notices advise holders of a document of additional protective measures such as restrictions on reproduction, dissemination, or extraction. Further guidelines are provided in reference (a).

CHAPTER 6 CONTROL OF CLASSIFIED INFORMATION

0601. General. Bureau of Naval Personnel (BUPERS) BUPERS-00T5 will, per reference (a), control dissemination of classified documents and control unclassified information originated or received by BUPERS Millington/NAVPERSCOM.

0602. Access To Classified Information

1. Only those individuals (military, civilian, and contractor employees under a classified contract) with proper adjudicated security investigation, level of clearance, and need to know have access to classified information in the performance of their duties. No person has access to classified information strictly on their position. If a person requires access to classified information to perform his or her duties, the department security assistant must send a request to BUPERS-00T5 requesting authorization for access to classified information. When the request is received by BUPERS-00T5, it will be reviewed for proper adjudicated security investigation and level of clearance, and (if a civilian Government employee) the request will be checked for a sensitivity code to determine if the civilian position is a non-critical-sensitive or critical-sensitive position. If the civilian is in a non-sensitive position, access to classified information will be denied until position is reclassified to non-critical- or critical-sensitive by the department.
2. Only personnel with proper clearance and access authorized by BUPERS-00T5 may have access to information technology (IT) systems processing classified naval messages.
3. The command duty officer is authorized to view messages up to and including Secret messages in the performance of his or her duties while only in a watch status. Unless authorized by BUPERS-00T5, this does not authorize the person to handle classified information within his or her department.
4. Courier cards are not required for hand-carrying classified information within and between BUPERS Millington/NAVPERSCOM buildings. To hand-carry classified information within the command, use the appropriate standard form cover sheet for a classified document attached to a message in a file folder, envelope, or inside a briefcase to prevent inadvertent disclosure when hand-carrying is authorized.
5. When traveling outside the command, BUPERS-00T5 will provide written authorization to all individuals escorting or hand-carrying classified information. This authorization may be the DD 2501 Courier Authorization Card or included on official travel orders, visit requests, or a courier authorization letter. Any of these written authorizations may be used to identify appropriately cleared Department of War (DoW) military and civilian personnel approved to escort or hand-carry classified information (except for SCI and special access programs (SAP)). Reference (a) provides additional provisions for authorization to escort or hand-carry classified information.

0603. Classified Information Control. Accountability and control of classified information and other accountable documents begin with their origin or receipt at the command. BUPERS-00T5 is the central control point and is responsible for overall control of Secret and Confidential information within BUPERS/NAVPERSCOM. BUPERS-00T5 controls all Top Secret information originated and received by the command.

0604. Accountability And Control

1. All Top Secret information is recorded by BUPERS-00T5. Top Secret received directly by an individual in BUPERS/NAVPERSCOM from any source must be immediately delivered to BUPERS-00T5. Accountability and control of all information by department security assistants, unless specifically exempted by BUPERS-00T5, is as follows:

a. Top Secret Information

(1) Dissemination of Top Secret information within BUPERS Millington/NAVPERSCOM is controlled strictly by BUPERS-00T5 and limited to persons possessing a Top Secret clearance, authorized access, and "need-to-know." Top Secret information will be accounted for at all times, from time of receipt until destroyed per reference (a).

(2) Top Secret information received from sources other than BUPERS-00T5 must be immediately delivered to BUPERS-00T5 for proper accountability.

(3) OPNAV 5511/13 Record of Disclosure will be completed, listing all personnel viewing Top Secret information. SF 703 Top Secret Cover Sheet must be attached to cover each Top Secret document and OPNAV 5216/10 Correspondence/Material Control Sheet, attached to the document for material control. When Top Secret information is checked out and removed from BUPERS-00T5 office spaces, the OPNAV 5216/10 will document the routing.

(4) Top Secret information must be returned to BUPERS-00T5 daily, prior to 1500. Exceptions to this requirement may only be made by BUPERS-00T5, only if essential and only if approved storage is available.

(5) When Top Secret information is to be prepared, BUPERS-00T5 must be contacted prior to commencing preparation. BUPERS-00T5 will provide OPNAV 5216/10, SF 703, OPNAV 5511/13, and a residue envelope. BUPERS-00T5 will assign a Top Secret accountability number. All rough drafts, diskettes, etc., must be placed in the residue envelope and returned to BUPERS-00T5, along with smooth copies. Number and mark Top Secret information per reference (a).

(6) Top Secret information will not be reproduced.

(7) Destruction of Top Secret information is the exclusive responsibility of BUPERS-00T5. Accordingly, all Top Secret information to be destroyed must be delivered to BUPERS-00T5.

b. Secret Information

(1) Secret documents will only be released to persons having the required access. Documents to be transferred from one office to another will always be hand-carried and properly safeguarded.

(2) SF 704 Secret Cover Sheet is used to cover each Secret document and OPNAV 5216/10 must be attached to the document.

(3) When Secret information is required to be transmitted, it will be prepared for transmission per reference (a).

c. Confidential Information. SF 705 Confidential Cover Sheet and OPNAV 5216/10 are affixed to all Confidential information received (except messages) by BUPERS-00T5 prior to routing. Departments receiving Confidential information will provide security protection for all Confidential information received, originated, transmitted, or stored to the extent required by this instruction.

2. Classified Messages. Top Secret messages are handled in the same manner described above for Top Secret information. All NATO messages received by the command will be handled by BUPERS-00T5. The receiving office code is responsible for handling, distributing, and disposing of incoming Secret and Confidential messages. Identification markings on a message are the word "Secret" or "Confidential" at the head and foot of each page of the message. Generally, size and color of this marking is the same as the text. Secret and Confidential messages received from NAVPERSCOM Message Center are not controlled by BUPERS-00T5. It is the responsibility of the department security assistant to receive messages to examine each one carefully to affix a Secret or Confidential Material Control Record and a Secret or Confidential cover sheet appropriately. All classified message traffic (Secret and Confidential) being sent to BUPERS Millington/ NAVPERSCOM will be received and processed via the Navy Marine Corps Intranet Secret Internet Protocol Router Network (SIPRNET). Only personnel that have been authorized by BUPERS-00T5 will be granted access to classified IT systems.

3. Naval Warfare and Tactical Publications

a. BUPERS/NAVPERSCOM employees who have appropriate clearance may check out naval warfare and tactical publications from their department security assistants, when available. Classified publications must be stored in appropriate authorized security containers for the level of classification when not being used. BUPERS-00T5 will distribute publications (once received) to appropriate department security assistants. Department security assistants must maintain control of classified publications and allow only those individuals with proper security clearance and need-to-know to view contents. Publications will be destroyed by BUPERS-00T5 when no longer needed.

b. All information in these publications, regardless of classification, is considered privileged information, and (if unclassified) is to be treated as For Official Use Only (FOUO). The person who has one of these publications is personally responsible for accountability, safeguarding, and maintenance of the publication in the same manner as other classified information.

0605. Copying Classified Documents

1. No classified materials will be copied without coordinating the action through the communications security (COMSEC) manager and BUPERS-00T5.
2. Top Secret documents will not be detached from routing sheets or duplicated without proper approval from BUPERS-00T5. Information originating outside of DoW will not be reproduced without consent of the originating agency.
3. Each Assistant Commander, Navy Personnel Command (ACNPC) or special assistant (SA) will contact BUPERS-00T5 if they need to copy classified information; and copying of classified information is only for essential material and limited to exact quantities for the task involved.
4. Destruction of classified information will be per reference (a).
5. Reproduced copies of classified documents, as well as waste, samples, etc., will be controlled in the same manner as the original document.
6. Copies that are reproduced using typical office copiers can leave legible images on plastic surfaces. These images can transfer to plastic binders or plastic document protectors after lengthy contact. Classified document cover sheets will be used to preclude transferring classified images to plastic materials.

0606. Handling Precautions and Office Practices. The following precautions will be observed by BUPERS/NAVPERSCOM personnel to prevent deliberate or casual access to classified information by unauthorized persons:

1. Keep classified documents stored per reference (a).
2. If it is necessary to vacate the office, all classified information must be returned to its stowage container and locked or left in the custody of persons cleared for access to subject matter.
3. Receive visitors in areas devoid of classified information, whenever possible, unless the purpose of the visit is to discuss such information.
4. Protect all working information containing classified information (e.g., rough drafts, stencils, stenographic notes, and papers) in the same manner as original classified documents, until no longer required and destroyed.

5. Do not discuss classified information over any unsecured telephone or internal communications systems.
6. Immediately report any loss, compromise, or suspected compromise to BUPERS-00T5. During non-working hours, report any loss to the BUPERS/NAVPERSCOM duty officer. For classified documents lost while in a travel status where no U.S. military activity exists in the area, notify the nearest NAVCRIMINVSVC or FBI field office, as well as BUPERS-00T5, by the quickest means possible.

0607. Control Of Classified Working Papers or Preliminary Drafts

1. The terms classified working papers or preliminary draft include, but are not limited to, the following: all written information (handwritten, printed, or typed); rejected copies; magnetic recordings; all photographs, negatives, exposed or printed films; and all punched cards or tapes, etc. developed in connection with the handling, processing, production, and utilization of classified information. Working papers containing classified information will be:

- a. Dated when created;
- b. Marked on each page with the highest classification of any information contained in the document. This derivative classification is based upon the classification of the material used to prepare the working document and will be marked with the same declassification date as the original classified material used;
- c. Protected following guidance for the classification assigned; and
- d. Destroyed when they have served their purpose. Classified notes from a training course or conference are considered working papers.

2. Top Secret working papers will be prepared, controlled, and accounted for in the same manner as the finished document. Also, working papers meeting the following description should be controlled as if they were finished documents.

- a. Working papers released by the originator outside BUPERS/NAVPERSCOM, transmitted electronically or transmitted through message channels within BUPERS/NAVPERSCOM,
- b. Retained more than 90 days from date of origin, and
- c. Filed permanently.

0608. NATO Material

1. DON documents incorporating NATO information must be marked per reference (a).

2. All personnel requiring access to NATO information must first be cleared for access to an equivalent level of classified information. Personnel who are to have access to NATO information must be aware of the appropriate NATO security regulations and the consequences of negligence. The NATO Control Officer will brief all personnel requiring access to NATO information and complete OPNAV 5511/27 Briefing/Re-briefing/Debriefing Certificate to certify briefing. BUPERS-00T5 will retain a completed OPNAV 5511/27 Briefing/Re-Briefing/Debriefing Certificate.

0609. Classified Contract Management

1. Only contractors assigned to a classified contract who have the appropriate clearance eligibility and need to know will be granted access to classified materials in support of the Industrial Security (IS) Program requirements.

2. BUPERS/NAVPERSCOM Contract Specialist (BUPERS-00T3C) will ensure DD 254 Department of Defense Contract Security Classification Specification is affixed to all classified contracts prior to solicitation and finalized upon contract award. The applicable classified contract contracting officer representative (COR) with security specialist training will complete and sign the DD 254 in coordination with BUPERS-00T5 per reference (a). The final DD 254 will be maintained on file by the applicable COR and the security manager. Additional procedures for contract management are stipulated in NAVPERSCOM ADMINMAN-M 5000.1 (administrative manual), article 4200-020.

3. BUPERS-00T5 is responsible for overall IS Program management and ensuring all contract personnel have valid clearance eligibility favorably adjudicated from a National Agency Check with Local Agency Checks (NACLIC)/Tier-3 (T3) investigation (or higher), as all positions within BUPERS/NAVPERSCOM have been designated as non-critical sensitive or higher. Visit notifications for contract employees will be delivered by the contract company facilities security officer (FSO) to BUPERS-00T5 and updated and maintained as delineated in chapter 11, section 1102 in this manual.

4. The assigned COR must ensure the assigned trusted agent (TA) enters the appropriate contractor information in the Trusted Agent Sponsorship System (TASS) upon verification of the visit notification in Joint Personnel Adjudication System (JPAS) and required clearance eligibility by BUPERS-00T5. This annotation will be made on the TASS form for each member prior to the contractor being sponsored by the TA for a common access card (CAC). Duration of the CAC sponsorship for each contractor in TASS must not exceed the duration of the applicable contract. The TA is responsible for ensuring TASS is updated with any contract extensions to enable CAC renewal. BUPERS-00T5 is responsible for updating and submitting building access requests for all new and updated contract personnel requests.

CHAPTER 7 SECURITY STORAGE

0701. Security Container Custodian. Department security assistants must ensure security containers located within their spaces have a principal custodian and an alternate designated for each security container. This designation is indicated on SF 700 affixed to inside of the drawer containing combination lock. Custodians and other persons listed on SF 700 must possess a security clearance and access equal to or higher than classification level of information stowed in container. Principal custodian bears primary responsibility for compliance with security procedures for container and its contents per reference (a).

0702. Combinations

1. Combinations for security containers will be changed when required per reference (a).
2. Only individuals with proper clearance and access equal to or higher than classification level of information in container and a need to know will change combinations. NAVPERSCOM Security Management Branch (BUPERS-00T5) personnel will change any combination or assist office code in changing its security container combinations. Once the combination has been changed, SF 700, parts 2 and 2A, will be given to BUPERS-00T5 for storage in security container located in BUPERS-00T5.

Note: When combinations are recorded, such records will be marked with the highest classification level being protected.

0703. Classified Information Storage. When not in actual use or under immediate surveillance of an authorized person, classified information will be secured and stored per reference (a).

0704. Classified Storage Equipment. Standards for classified storage equipment will be per reference (a).

0705. Locking Procedures. Security containers will be locked and secured per reference (a).

0706. Daily Security Inspection

1. All BUPERS Millington/NAVPERSCOM codes handling classified information will establish a double-check system to ensure that at the end of each working day:
 - a. All classified information is properly stowed in authorized security containers;
 - b. No classified information is left in or on desks, tables, files, etc.;

- c. Wastebaskets should be checked to ensure they contain no classified information;
- d. Classified shorthand notes, computer disks/compact disks (CDs), rough drafts, and similar papers have been properly stowed;
- e. Desk blotters and computer disks/CDs are protected in the same manner as required for highest level of classification for which they have been used; and
- f. Security containers and secure Rooms that contain classified information are locked and properly secured. A record of above assignments and inspections will be maintained using SF 701 Activity Security Checklist in each office handling classified information. SF 702 must be prominently posted on each security container.

CHAPTER 8 TRANSMISSION AND TRANSPORTATION

0801. General

1. Transmission and transportation of classified information will be per reference (a).

a. Individuals who have proper clearance, access, and need-to-know may hand-carry classified information within the command and between buildings as part of their normal duties. Individuals will use a cover sheet, file folder, or briefcase to prevent inadvertent disclosure of classified information when movement is from one building to another, in an elevator, or through public areas. If movement requires transportation other than walking, classified information will be double-wrapped. A briefcase may be considered as the outer wrapping.

b. Personnel hand-carrying classified information outside the command will obtain courier authorization (in writing) from BUPERS-00T5 prior to removing the classified information. Courier authorization may be in the form of a letter or a DD 2501 issued by BUPERS-00T5. Personnel discovered carrying classified information without written authorization will be detained until BUPERS-00T5 is notified and takes charge of the situation. Exhibit 8A will be used to request authorization to transport classified information. If transporting classified information via commercial passenger aircraft and a letter requesting authorization is required, employees must have an authorized courier letter or a DD 2501 signed by BUPERS-00T5 (exhibit 8B).

c. The following conditions will be met if classified information needs to be transported outside the command:

(1) A determination is made that necessary classified information is not available at the activity involved.

(2) Time does not permit information to be transmitted by normal channels.

(3) Appropriate correspondence (serialized and dated) is prepared and processed through BUPERS-00T5. Confidential information need not be processed through BUPERS-00T5, but must meet all other requirements for Secret. (Note: When classified information is not transported beyond the boundary of the command and is removed for temporary use, it must be returned to BUPERS-00T5's custody within the same day. If classified information is being removed from the command, all other provisions of this chapter will apply.) When classified information is removed under these conditions, department security assistants must maintain a list of information being carried and accounting conducted immediately upon return by the custodian. Any discrepancies, including loss or possible compromise, must be reported immediately to BUPERS-00T5.

(4) Classified information must not be opened, read, studied, displayed, or used in any manner in public places or conveyances.

(5) When classified information is carried in a private, public, or government conveyance it will not be stowed in any detachable storage compartments such as trailers, luggage racks, etc.

(6) Classified information must be in physical possession of the individual at all times if proper storage at a U.S. Government activity or appropriately cleared contractor facility is not available. Classified information will not be left in such places as locked automobiles, hotel rooms, hotel safes, train compartments, private residences, public lockers, etc.

(7) When return of classified information is required, the traveler will request the activity to return information via appropriate authorized channels per reference (a). If the activity retains Secret information, the traveler is required to obtain a receipt, which is delivered to BUPERS-00T5.

0802. Transmission and Receipt of Classified Information

1. Transmission of classified information will be per reference (a).

2. Receipt System

a. Top Secret information is transmitted under a continuous chain of custody.

b. An acknowledgement receipt between commands covers Secret information. Failure to sign for and return a receipt to sender may result in a report of possible compromise.

c. Receipts for Confidential information are not required, except when transmitted to a foreign government, including embassies in the United States.

d. Sender of information will attach receipt to the inner cover. A postcard receipt form, such as an OPNAV 5511/10 Record of Receipt may be used for this purpose. Receipt forms will be unclassified and contain only information necessary to identify information being transmitted. Receipts will be retained for at least 2 years.

0803. Electronic Transmission of Classified Information. Secure telephone equipment (STE) is a telephone unit providing reliable, low-cost secure voice and data capability for conducting official business involving classified information. To permit access to an STE, the individual must be eligible for access to classified information at the Secret level.

0804. Processing Classified Information on BUPERS Millington/ NAVPERSCOM Computers. Classified information will not be processed on any command IT without the direct approval of BUPERS-00T5. BUPERS/NAVPERSCOM personnel requiring access to classified Navy and Marine Corps Intranet (NMCI) SIPRNET systems must forward OPNAV 5239/14 System Authorization Access Request (SAAR) to BUPERS-00T5 via their supervisor. Once BUPERS-00T5 receives OPNAV 5239/14, BUPERS-00T5 will verify to see if the person requesting access has the appropriate security clearance eligibility and access authorization.

Exhibit 8A
Authorization to Transport Classified Information

Ser 5510
BUPERS-00T5
Date

From: Commander, Navy Personnel Command

Subj: AUTHORIZATION TO TRANSPORT CLASSIFIED INFORMATION

Ref: (a) SECNAVINST 5510.36B
(b) BUPERSINST 5510.61E

1. Per references (a) and (b), the below individual has authorization to transport classified information.
 - a. Full name, rank/rating/grade, and command name
 - b. Description of the personal identification the individual will present (e.g., State driver's license number or government identification card)
 - c. Description of the material being carried (e.g., three sealed packages, 9" X 8" X 24"), addressee, and sender
 - d. The point of departure itinerary, destination, and known transfer points
 - e. A date of issue and expiration date
 - f. BUPERS/NAVPERSCOM Security Manager's (name, title, and signature) must be on the face of each package or carton
 - g. BUPERS/NAVPERSCOM Command Duty Officer telephone number: (901) 874-3071/ DSN 882.
2. If a return trip is necessary, the host security official at the original destination must conduct all necessary coordination and provide an endorsement to the original courier authorization letter to include the updated itinerary.
3. Confirmation of this authorization may be obtained by calling NAVPERSCOM Security Manager (BUPERS-00T5) at (901) 874-3091/DSN 882.

NAME (BUPERS/NAVPERSCOM Security Manager)
By direction

Exhibit 8B
Auth. to Hand-Carry Classified Info. Aboard Commercial Passenger Aircraft

Ser 5510
BUPERS-00T5
Date

From: Commander, Navy Personnel Command

Subj: AUTHORIZATION TO HAND-CARRY CLASSIFIED INFORMATION ABOARD
COMMERCIAL PASSENGER AIRCRAFT

Ref: (a) SECNAVINST 5510.36B
(b) BUPERSINST 5510.61E

1. Per references (a) and (b), the below individual has authorization to transport classified information.
 - a. Full name, rank/rating or grade, and command name
 - b. Description of the personal identification the individual will present (e.g., State driver's license number or government identification card)
 - c. Description of the material being carried (e.g., three sealed packages, 9" X 8" X 24"), addressee, and sender
 - d. The point of departure itinerary, destination, and known transfer points
 - e. A date of issue and expiration date
 - f. BUPERS/NAVPERSCOM Security Manager's name, title, and signature must be on the face of each package or carton
 - g. BUPERS/NAVPERSCOM Command Duty Officer telephone: (901) 874-3071/DSN 882
2. If a return trip is necessary, the host security official at the original destination must conduct all necessary coordination and provide an endorsement to the original courier authorization letter to include the updated itinerary.
3. Confirmation of this authorization may be obtained by calling BUPERS/NAVPERSCOM Security Manager (BUPERS-00T5) at (901) 874-3091/DSN 882.

NAME (BUPERS/NAVPERSCOM Security Manager)
By direction

CHAPTER 9

DESTRUCTION OF CLASSIFIED INFORMATION

0901. General. Destruction of classified information will be carried out per reference (a). Secret and below classified information will be destroyed using authorized shredders located in NAVPERSCOM buildings 453, 768, 769, and 791. Authorized classified material shredders will be labeled as such. Cross-strip shredders are not authorized to be used to destroy classified materials. Classified compact disks are authorized to be destroyed by BUPERS-00T5 only. All Top Secret information will be returned to BUPERS-00T5, building 769, room 184, for destruction by the BUPERS/NAVPERSCOM Top Secret Control Officer.

0902. Destruction Reports

1. A record of destruction is required for Top Secret information. Use of OPNAV 5511/12 Classified Material Destruction Report is no longer required. Record destruction of Top Secret and any special types of classified information (if required) by any means, as long as the record includes complete identification of information destroyed and the date of destruction. Two witnesses who have authorized access to the information being destroyed must execute the record of destruction. Retain Top Secret records of destruction for 5 years. Records of destruction are not required for waste products containing Top Secret information.

2. Records of destruction are not required for Secret and Confidential information, except for special types of classified information per reference (a).

CHAPTER 10 EMERGENCY PLANNING

1001. General

1. Emergencies may be categorized as accidental or hostile. Natural disasters such as fire or flood are examples of accidental emergencies, whereas enemy attack or civil uprising would be defined as hostile actions. In an accidental emergency, action must be directed toward maintaining continuous control and accountability of all classified and privileged information. During hostile action, it must be assumed that information itself is a target and all actions must be directed toward preventing a compromise.
2. When confronting an emergency situation, three basic alternatives are available:
 - a. Secure the information
 - b. Remove the information, and
 - c. Destroy the information
3. Execution of any of these alternatives must be done in such a manner to minimize the risk of loss of life or personnel injury.

1002. Secure The Information. In case of either an accidental or hostile emergency, securing information is the primary means of protecting BUPERS Millington/NAVPERSCOM classified and privileged information. All personnel having custody of such information will immediately store the information in its authorized container, being certain to securely lock the container. Upon return to the area, all containers will be inventoried immediately, and the results reported to the department security assistant. Discrepancies will be brought to the immediate attention of the cognizant Director, Assistant Commander, Navy Personnel Command (ACNPC) or special assistant (SA) and BUPERS-00T5.

1003. Remove The Information

1. Because of the nature of the mission of BUPERS/NAVPERSCOM, removal of all classified and privileged information is the least likely emergency action to be taken. Local contingency planning does not envision evacuation of the area, except in the most severe circumstances, which would necessarily entail emergency destruction of all classified information. In the unlikely event that removal of information is ordered, only the most sensitive information should be removed. Classified information must be transported in a government vehicle, and the courier must be directed to maintain continuous accountability.

2. All Communications Security Material System (CMS) information will be removed and relocated to the COMSEC vault in building 769, room 184, if time permits. Key Management Infrastructure (KMI) Manager/COMSEC custodian must be contacted prior to the removal of any COMSEC information or equipment.

1004. Destroy The Information

1. Each department security assistant will be directed to implement the department emergency destruction plan upon notification to commence emergency destruction of classified and privileged information. The importance of beginning destruction sufficiently early to prevent loss of information cannot be overemphasized. The effects of premature destruction are considered relatively inconsequential when measured against the possibility of compromise.

2. Priorities for emergency destruction are as follows:

a. Priority One. Information, which, if captured, would cause exceptionally grave damage (Top Secret)

b. Priority Two. Information, which if captured, would cause serious damage (Secret)

c. Priority Three. Information, which if captured, would cause identifiable damage (Confidential)

3. "Priority One" and all COMSEC information will be returned to building 769, room 184, for destruction when possible.

1005. Implementing Authority

1. BUPERS/COMNAVPERSCOM will be the implementation authority for any emergency actions; however, the senior individual present in a space containing classified and privileged information may implement emergency procedures and deviate from established plans if urgency of the situation precludes awaiting emergency instructions.

2. Per EKMS-1, the KMI manager/COMSEC custodian, with authorization from the SCMSRO, is the only person authorized to initiate COMSEC information emergency destruction. ADMINMAN 2200-030 contains a detailed emergency action plan with checklists for each area and type of gear.

CHAPTER 11 VISITS AND MEETINGS

1101. General. For security purposes, the term visitor applies to any person who is not attached to or employed by BUPERS Millington/NAVPERSCOM or a person on temporary additional duty (TEMADD). Personnel on temporary duty (TEMDDU) orders or those personnel assigned on a quota to a school for a course of instruction are also considered visitors. Visit access to classified information is specified in reference (b). For unofficial visits, BUPERS/NAVPERSCOM employees must escort visitors at all times, and their access should be limited to common areas and passageways. Access to working spaces should be minimized due to the high concentration of sensitive information. In the event a visitor is taken into a working space for a special occasion, the sponsor and space supervisor are responsible for ensuring all sensitive information is properly stored and safeguarded.

1102. Incoming Visits

1. NAVPERSCOM Security Office (BUPERS-00T5) is the central control point for receiving and recording incoming visit requests from the Department of War (DoW), other government agencies, foreign representatives, and contractor activities, and is responsible for confirming all visitor and contractor security clearances when access to classified information will be required. The BUPERS/NAVPERSCOM office to be visited or having cognizance over the contract is responsible for ensuring visitors or contractors are informed of the necessity of forwarding a visitor request to BUPERS-00T5.

2. Upon receipt of an incoming visit notification in the Joint Personnel Adjudication System (JPAS), BUPERS-00T5 will forward an e-mail notification to the point of contact for concurrence or nonoccurrence with the proposed visit.

3. All long-term visit requests must be renewed annually. At no time will visitors or contractors be given access to classified information without proper verification and approval from BUPERS-00T5.

4. Visitors accessing secure spaces will be escorted and will log into and out of the space using the visitor log. The level 2 restricted access areas that require clearance verification for all visitors are building 453, room 327; building 768, rooms S107A and S305A; building 769, rooms 184C and 184D; and building 791, rooms D107B, F104, F204, and G101B.

1103. Outgoing Visits

1. Requests for visits by BUPERS/NAVPERSCOM personnel, which will necessitate their having access to classified information, will be made via encrypted e-mail. The e-mail will list the name and social security number of all personnel going on the visit, dates, and type of visit, classification of discussed material, Security Management Office (SMO) of the visited command, and the name, e-mail address and phone number of the designated point of contact (POC) at the visited command.

BUPERS-00T5 will enter the visit into Defense Information System for Security (DISS) if the security management office (SMO) of the visiting command is known. Requests for visits will be submitted in advance of proposed visits and in sufficient time to permit processing. Under no circumstances may personnel hand-carry their own visit request to the places being visited. BUPERS Millington/NAVPERSCOM departments making arrangements for sponsored visits that include personnel from other DoW or contractor agencies should notify those activities to forward security confirmation for their personnel to the activity to be visited.

2. Visit requests may be transmitted by the following means:

a. DISS will be used whenever the visited command has access to receive visit notifications in DISS.

b. Electronically transmitted via e-mail when the visited command does not have access to DISS. Visit requests via e-mail must be transmitted from BUPERS-00T5 to the security manager of the command to be visited. Additionally, procedures must be established to preclude electronic transmission by unauthorized personnel.

1104. Visits To Contractor Facilities. When personnel require access to classified information in connection with a visit to a contractor facility, the visit request is submitted per section 1103 above, with one exception, visit request must include contract or solicitation number. BUPERS Millington/NAVPERSCOM departments submitting a visit request to a contractor facility will forward the visit request to BUPERS-00T5 for approval. Under no circumstances are departments to make prior notification or verbal requests for visits. BUPERS-00T5 will assist departments with proper procedures for completing visit notifications in DISS.

1105. Visits By Representatives of the General Accounting Office (GAO). Properly cleared and identified representatives of GAO may be granted access to classified DON information in the performance of their assigned duties and responsibilities per reference (b). All GAO visit requests are kept on file in BUPERS-00T5.

1106. Visits By Foreign Nationals. Policy and procedures for visits by foreign nationals are contained in reference (b). These visits will be coordinated through BUPERS-00T5 to ensure proper coordination and control of foreign disclosure within DON. Foreign nationals will not be granted account access to any BUPERS/NAVPERSCOM systems, nor will they be granted unescorted access to any BUPERS/NAVPERSCOM buildings.

1107. Visits To Foreign Countries. When a DON activity proposes to sponsor an official visit to a foreign country, the sponsoring activity will ensure nominees are reliable and trustworthy, and if classified information is involved, they have been properly cleared to handle information of the security classification involved in the visit. If classified DON information is to be discussed with foreign nationals, prior authorization for such discussions must be obtained from the Navy International Programs Office. Further guidelines on this subject are contained in reference (b).

1108. Classified Meetings

1. Protection of classified information within a conference room is the responsibility of the office sponsoring the conference. All offices conducting meetings should be familiar with the guidelines of reference (a).

a. Classified meetings will not be held in spaces that have not been designated as level 2 restricted access areas. Top Secret information is not to be discussed in any command spaces. Joint Reserve Intelligence Center Millington is the only local command with a Top Secret meeting space.

b. No portable electronic devices, aside from SIPRNet laptops, are allowed in a classified meeting or space. All wireless capable equipped items are prohibited and must be secured outside of the space.

c. The office conducting the conference, briefing, or presentation will make an inspection at the conclusion to ensure no classified information remains in the room.

2. If foreign representatives are expected to attend a classified meeting, a command may not accept security sponsorship without approval of the Deputy Secretary of the Navy for Plans, Programs, and Implementation Security. Requests to sponsor meetings involving foreign representatives must be submitted not later than 45 days prior to the meeting date.

CHAPTER 12 PERSONNEL SECURITY

1201. General

1. No person will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made of their loyalty, reliability, and trustworthiness, and the individual has executed SF 312. Initial determination will be based on appropriate personnel security investigations (PSI) to access required or to other considerations of the sensitivity of duties assigned. No individual will be given access to classified information strictly because of his or her rank. Reference (b) provides guidance governing Department of the Navy (DON) PSP.
2. Only NAVPERSCOM Security Branch (BUPERS-00T5) is authorized to request PSIs for BUPERS Millington/NAVPERSCOM personnel.
3. PSI requirements are contained in reference (b). Only the minimum investigation to satisfy a requirement may be requested.

1202. Responsibilities. The granting of access to classified information is a command function. BUPERS-00T5 is authorized, in the name of COMNAVPERSCOM, to grant appropriate security access for BUPERS Millington/NAVPERSCOM personnel.

1203. Position Sensitivity

1. National security positions in the command that require use of, or access to, classified information under 5 CFR 732.201 are required to be assigned a position sensitivity level. Position sensitivity levels are special sensitive (SS), critical sensitive (CS), and non-critical sensitive (NCS).
2. Military, civilian, and contract employees performing duties on unclassified information technology (IT) will be assigned to one of three position sensitivity designations per DoDM 5200.02, Section 4; and reference (b).
3. Security clearances and investigative requirements for military, civilian, and contractor employees are predetermined based on degree of access required and category of sensitivity assigned to criteria for designating IT position category. All positions within BUPERS/NAVPERSCOM have been designated at IT level 2 NCS and require a favorably adjudicated Tier 3 clearance, or equivalent, at a minimum.

1204. Requirements For Access and Clearance Eligibility

1. All civilian and military personnel reporting aboard BUPERS Millington/NAVPERSCOM are required to check-in with BUPERS-00T5 in building 769, room 184.

2. During check-in process, all civilian and military personnel will be informed that they do not automatically have access to classified information. For access to classified information, each individual checking aboard must submit a request for access to classified information through their department security assistant. Need for access is evaluated and determined by position sensitivity and need-to-know. If an individual is in an SS, CS, or NCS position that requires access to classified information and has a need-to-know, the department security assistant or member's supervisor must submit NAVPERS 5520/6 Request for Security Access to BUPERS-00T5. Eligibility for access to classified information for military and civilian personnel assigned to BUPERS Millington/NAVPERSCOM is certified by BUPERS-00T5. Once determination has been made that an individual requires access to classified information and request for security access is received, BUPERS-00T5 will authorize access to view classified information only if the Defense Counterintelligence Security Agency Central Adjudication Services (DCSA CAF) has determined eligibility and security investigation is current. If investigation is not current, individual will be required to update investigation using National Background Investigation (NBIS) e-APP, per ADMINMAN 5520-010. The investigation will be initiated, reviewed, and submitted by BUPERS-00T5. BUPERS-00T5 may grant interim clearance for access when proper paperwork has been submitted and or released to the Office of Personnel Management.

3. All civilian and military personnel checking out and departing BUPERS Millington/NAVPERSCOM must check-out with BUPERS-00T5.

1205. Continuous Evaluation of Eligibility

1. Per reference (b), personnel security responsibilities do not stop once a favorable personnel security determination is made. Any person having knowledge or information that reflects adversely on an individual's loyalty, reliability, and trustworthiness from a security prospective will immediately report the full particulars and circumstances to BUPERS-00T5 for evaluation and or further investigation. Ideally, it is best if all personnel self-report any issues or concerns in the areas below.

2. Security assistants, command legal staff officials, and supervisors are cautioned that information which could place an individual's loyalty, reliability, and trustworthiness in question has to be evaluated from a security perspective and are hereby required to familiarize themselves with the adjudication policy in reference (b). Behavior indicating allegiance against the United States of America, exercising dual citizenship, sexual misconduct, misuse of IT systems, unexplained affluence, financial instability, alcohol and drug misuse, demonstrated behavioral conditions (affective lability, emotional dysregulation, excessive irritability, aggression, non-suicidal self-injury, psychosis, or neurocognitive dysfunction, or criminal conduct) is potentially significant to an individual's security status and information concerning these issues must be reported to BUPERS-00T5.

3. Co-workers have an equal obligation to advise their supervisors or BUPERS-00T5 when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position. Combatting the “insider threat” is an all-hands evolution and everyone must remain vigilant at all times to fulfil their roles within continuous evaluation. “Insider threat” awareness will be incorporated into departmental training plans and the annual Security Program assessment to ensure all hands are aware of the items to be vigilant for and proper reporting procedures per reference (e).

1206. Proof of U.S. Citizenship for Security Clearance and Access. Citizenship validation will be accomplished per reference (b), appendix I.

1207. Temporary And One-Time Access. Circumstances may arise in which temporary and one-time access to classified information is appropriate for personnel otherwise eligible for access involved, but who do not currently hold a security clearance at that level, and the assigned duties do not require access. Requests should be submitted to BUPERS-00T5, detailing reasons and length of time desired for temporary access. Reference (b), paragraphs explain one-time and temporary access requirements in detail.

1208. Denial or Revocation of Clearance and or Access for Cause. When a personnel security determination has been made that an individual does not meet or no longer meets criteria for a security clearance, the clearance will be denied or revoked for cause by DCSA CAF. Reference (b) provides an extensive explanation of the denial or revocation of security clearance for cause process.

1209. Suspension of Access for Cause. When questionable or unfavorable information becomes available concerning an individual who has been granted access to classified information, procedures in reference (b) apply.

1210. Terminating, Withdrawing, Or Adjusting Access

1. Access to classified information terminates when an individual transfers from the command. The process to terminate, withdraw, or adjust access will be per reference (b), chapter 9, paragraph 9-17. BUPERS-00T5 will debrief individuals per reference (b), chapter 4, paragraph 4-11, but execution of OPNAV 5511/14 is not required.

2. BUPERS-00T5 will administratively withdraw an individual's access when permanent change in official duties (e.g., rating change) eliminates the requirement for security clearance and access, and when the individual separates from DON or otherwise terminates employment. BUPERS-00T5 will debrief individuals as outlined in reference (b) and execute OPNAV 5511/14, which will be filed in individual's service record or official personnel folder. BUPERS-00T5 will forward an electronic incident report via the Joint Personnel Adjudication System (JPAS) to notify DON CAF that the individual no longer requires clearance and access.

3 When level of access required for an individual's official duties change, BUPERS-00T5 will adjust authorized access, accordingly, provided new requirement does not exceed level allowed by the security clearance. If level of access required will exceed level allowed by DCSA CAF security clearance certification, BUPERS-00T5 will request appropriate investigation and may consider interim clearance procedures per reference (b).

1211. Security Termination Statement

1. OPNAV 5511/14 is obtained from the following personnel prior to their separation:

- a. Civilian personnel retiring, resigning from Federal service, or temporarily separating for more than 60 days, including sabbaticals and leave without pay;
- b. Military personnel retiring, being released from active duty, or discharged; and
- c. When security is revoked for cause, see reference (b).

2. BUPERS-00T5 will execute signing OPNAV 5511/14 for BUPERS Millington/NAVPERSCOM military and civilian personnel. All civilian personnel's OPNAV 5511/14 will be filed in individual's official record, and military personnel's OPNAV 5511/14 will be forwarded to the personnel support detachment.

1212. Clearance Of Personnel Not Regularly Assigned

1. In connection with disclosure of classified information to persons temporarily assigned temporary duty (TEM DU), temporary additional duty (TEM ADD), temporary active duty (TEM AC), and temporary active duty for training (ADT) personnel security clearances and accesses are required and will be granted per the following:

a. TEM ADD. Military personnel reporting for TEM ADD should be cleared by their commanding officer prior to reporting and their clearance and access status reported to BUPERS-00T5 in writing, either in their orders or by separate correspondence.

b. TEM DU. Military personnel reporting for TEM DU are, in most cases, reporting for briefing or instruction en route to a new duty station. Such clearance and access should be requested in advance of reporting, whenever practicable.

c. Training Duty. Navy reservists reporting for TEM DU for training must be cleared by their active duty command responsible for their records. The reservist's cognizant organization must specify the degree of clearance and or access required for training duty when acting upon the request for such duty. Attach NAVPERS 5520/6.

CHAPTER 13

OPERATIONS SECURITY (OPSEC)

1301. General

1. Operations security (OPSEC) is critical to the success of U.S. Navy activities. Maintaining OPSEC of inspection results detailing potential vulnerabilities, ongoing and finalized investigations with potentially sensitive information regarding individuals and commands, the confidentiality of hotline contacts, and ongoing special studies are essential in maintaining the effectiveness of BUPERS Millington/NAVPERSCOM and supports security across the Navy. OPSEC attempts to prevent the inadvertent compromise of unclassified or sensitive activities, capabilities, or intentions at every level during peacetime and war. The purpose of OPSEC is to reduce the vulnerability of friendly forces from successful adversary exploitation of critical information, including vulnerabilities at the command level, as well as individuals.

2. Critical information (CI) is information about Department of War (DoW) activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. CI is comprised of all controlled unclassified information (CUI) and any other information, if revealed to an adversary, may prevent or degrade mission accomplishment, cause loss of life, or damage friendly resources. If obtained, CI will either impact the success of the Navy or improve the likelihood of an adversary meeting their goals. The information BUPERS/NAVPERSCOM processes can lead to vulnerabilities in command policy, as well as individuals that can directly impact safety and security of commands and the accomplishment of missions. It is important to note that a majority of the CI that BUPERS/NAVPERSCOM handles belongs to other activities and commands within Department of the Navy (DON) and DoW.

3. To protect CI, all personnel must apply the OPSEC process and develop countermeasures that mitigate the risks of divulging CI. OPSEC measures are required for:

a. Operations and activities related to the preparation, deployment, and sustainment of the U.S. Navy in times of war, crisis, or peace. OPSEC applies to all activities that prepare, sustain, or employ forces, including personnel movement and planning;

b. The protection of information contained in operations and supporting plans and orders;

c. Information pertaining to other Navy commands considered CI per their OPSEC program;

d. Command inspections and area assessments;

e. Special studies and projects;

f. Hotline case information and the confidentiality of contacts;

1302. Responsibilities. Overall, the OPSEC Program implementation in daily operations is an all-hands responsibility. Specific responsibilities are:

1. Commanding Officer

- a. Designate an OPSEC Program manager (OPM) in writing. The commanding officer must provide sufficient resources, staff assistance, and authority to the OPM to implement, manage, and execute an effective OPSEC program.
- b. Identify OPSEC measures and coordinate execution with other commands as necessary.
- c. Approve the development of the CI and critical indicators list (CIIL) in support of the BUPERS Millington/NAVPERSCOM mission.
- d. Ensure the OPM attends the Navy or DoW OPSEC Program Managers Course.
- e. Ensure counter-intelligence training is coordinated and conducted annually per reference (i), for required personnel.
- f. Conduct annual OPSEC Program reviews.
- g. Ensure the OPM develops and maintains an OPSEC program.
- h. Ensure OPSEC training is conducted at command indoctrination and (at least) annually for all military, government, and contractor personnel.
- i. Promote an understanding and awareness campaign among BUPERS Millington/NAVPERSCOM personnel of the OPSEC process, command CI, adversary intelligence threats (in concert with the Navy Criminal Investigative Service (NAVCRIMINVSER) and command security manager), wireless communication vulnerabilities, and individual OPSEC responsibilities.
- j. Ensure the exercise of OPSEC oversight for government contracts per references (b) and (i).

2. BUPERS-00T5. The security manager has overall responsibility for coordinating information operations (IO) planning, synchronization and coordination of IO activities with relation to interaction with the Information, Personnel, and Physical Security programs.

3. BUPERS/NAVPERSCOM. Information System Security Manager (ISSM). The ISSM has overall responsibility for monitoring and enforcing information technology (IT) security and procedures and maintaining OPSEC with applicable IT systems within BUPERS/NAVPERSCOM and will serve as a key member of the OPSEC working group.

4. BUPERS Privacy Program Manager (BUPERS-07). The BUPERS Privacy Program manager will act as the lead for the privacy cadre and will be the liaison between BUPERS/NAVPERSCOM and external commands per reference (f). The Privacy Program manager will ensure OPSEC measures are in place to protect and properly mark CUI per reference (m), with particular focus on privacy and health information, formerly labeled sensitive personally identifiable information (PII) and Health Insurance Portability Accountability Act (HIPAA) information, within BUPERS/NAVPERSCOM and will serve as a key member of the OPSEC working group.
5. BUPERS/NAVPERSCOM Public Affairs Officer (PAO) (PERS-00P). PERS-00P is a key member of the overall OPSEC Program evaluation and enforcement and will serve as a member of the OPSEC working group. In support of the command of the OPSEC Program, the PAO will ensure all public media releases and Web sites are reviewed regularly for inadvertent CI disclosure.
6. OPSEC OPM. The security manager serves as the program manager and ensures the integration of OPSEC in all operations per references (g) and (l). The OPM is responsible for maintaining this instruction, chairing the OPSEC working group, and completing the duties outlined in references (c) through (h). The OPM must be in the grade of 0-4 or GS-12 or senior, have visibility into all BUPERS/NAVPERSCOM operations, and requires a single scope background investigation (SSBI)/Tier-5 (T-5). The following is a list of duties to be performed by OPM:
 - a. Establish a command OPSEC program that incorporates formal schools, training, planning, and evaluation tailored to the missions and functions of the command per references (g) through (k). Conduct program reviews per reference (g).
 - b. Advise the commander on OPSEC vulnerabilities and requirements.
 - c. Recommend OPSEC guidance and mitigations to the commander.
 - d. Maintain and update the command critical information and indicators listing (appendix A), approved by the commander. Ensure all BUPERS/NAVPERSCOM personnel are knowledgeable of designated CI and OPSEC measures in place to protect it.
 - e. Coordinate OPSEC requirements.
 - f. Coordinate the development of OPSEC-related portions of written documents to include investigations and inspections. Incorporate OPSEC into organizational processes where applicable.

- g. Participate in IO planning as a permanent member of the OPSEC working group. The OPSEC working group may be conducted concurrently with quarterly privacy cadre working group, affected per reference (f). If conducted concurrently, the OPM will co-chair the OPSEC and privacy cadre working group meeting with the Privacy Program manager, ensuring it reviews OPSEC requirements and assess operations per references (b) and (g).
- h. Consolidate any reported OPSEC violations for analysis and corrective or punitive action as required. OPSEC violations will be forwarded to the commander and discussed during the OPSEC working group.
- i. Coordinate appropriate intelligence and counter-intelligence support when required.
- j. Ensure BUPERS/NAVPERSCOM completes annual assessments and triennial surveys. Provide support and guidance to other OPSEC managers and coordinators for whom the OPM has oversight.
- k. Coordinate with external security program managers and critical infrastructure protection planners, if applicable.
- l. Coordinate with the Office of the Secretary of the Navy and the Office of the Chief of Naval Operations for OPSEC policy recommendations.
- m. Develop and maintain the BUPERS Millington/NAVPERSCOM OPSEC Program to include organizational policy and related guidance documents.
- n. Compile input to annual OPSEC and Operational Stress Control and Readiness (OSCAR) questionnaires, and submit when required.
- o. When necessary, participate in the review process of information for public release with NAVPERSCOM (PERS-00P).
- p. Ensure, at a minimum, initial and annual OPSEC refresher training is administered to all BUPERS/NAVPERSCOM military, civilian, and contractor personnel. Ensure new personnel are trained within 90 days of assignment.
- q. Display and disseminate OPSEC awareness information and materials.
- r. Ensure contractors use OPSEC to protect CI for contracts and subcontracts, as required.
- s. Ensure BUPERS/NAVPERSCOM CI is destroyed in a method that prevents recognition or reconstructions. This may be affected through use of National Security Agency approved shredders rated for at least Secret or through approved contract destruction methods.

t. Maintain an OPSEC turnover binder or share-drive folder.

(u.) Coordinate with other OPSEC managers located on board NSA Mid-South and all subordinate commands to implement OPSEC awareness, training, and assessments.

7. OPSEC Working Group

a. Working Group Chair. The OPM will chair the OPSEC Working Group and conduct an annual OPSEC assessment. At a minimum, the working group will review and update the CIIL, conduct analysis of OPSEC threats and vulnerabilities, assess the risks, make recommendations for implementing OPSEC measures, and conduct OPSEC training for the staff.

b. Working Group Membership and Representatives. As previously discussed, this meeting may be conducted in conjunction with the quarterly privacy cadre meeting. The working group will consist of the personnel listed below:

- (1) OPM
- (2) Security Manager
- (3) Information Systems Security Manager
- (4) Privacy Program Manager
- (5) Public Affairs Officer
- (6) NAVCRIMINVSVC (invited, but not required)

8. Contracting Officer's Representative (COR). The COR will ensure OPSEC training and safeguarding requirements are delineated in all contracts, unclassified or classified, prior to solicitation. Additional measures will be taken by the COR for classified contracts per chapter 6, section 0609 of this instruction.

1303. Countermeasures

1. To prevent inadvertent disclosure of unclassified sensitive information and specific CIL-related items, all personnel will conduct, at a minimum, the following:

a. Ensure personal actions do not divulge CI inappropriately. Avoid discussing sensitive matters on airlines, in restaurants, or in other public places in addition to phone, text, e-mail, or chat.

- b. Report suspected foreign intelligence service (FIS) encounters to the command security manager. FIS operatives may attempt to collect information via social engineering techniques such as e-mail phishing, telephone, or personal inquiries under the pretext of innocuous legitimate business or unduly persistent and invasive questions in social situations.
- c. All paper containing sensitive unclassified information, in either printed or handwritten form (including but not limited to reports, briefings, meeting notes, user manuals, or operating instructions), must be destroyed and not discarded in trash cans or recycling bins. Continuing destruction of classified paper per DoW security policy.
- d. When applicable, the command contract specialist and CORs must ensure classified and unclassified contract requirements properly reflect OPSEC responsibilities per references (b), (h), and (j).
- e. Encrypt non-classified internet protocol router network (NIPRNET) e-mails containing CUI (privacy) and (health), or items from the CIIL.
- f. Insist on the use of secure terminal equipment (STE) phones in secure mode, secure voice-over-Internet-protocol, and secure video equipment to communicate CI. Do not attempt to "talk around" sensitive or classified information. In addition, state "phone up/down" to inform surrounding personnel to discontinue discussions of sensitive but unclassified information or CIIL items until the phone call has ended.
- g. Critically question the placement of unclassified information on public or even protected networks. Determine if the information really needs to be there, balanced against the risk of disclosure, and if it is the only way in which it can be disseminated. OPSEC is more than just putting the right information on a given network, it is also a critical examination of what content needs to be there for mission success.
- h. Report all OPSEC violations to the BUPERS/NAVPERSCOM OPSEC and Security Program managers. All personnel should self-report OPSEC violations in order to mitigate possible consequences.

1304. OPSEC and Internet Use

1. Proper OPSEC training is paramount for responsible use of internet-based capabilities like texting, social media, user-generated content, social software, e-mail, instant messaging, and discussion forums. To avoid any disclosure of staff CI, all personnel should be cognizant of the risks of improper disclosure of information via internet-based capabilities. It is incumbent upon all divisions to ensure all hands maintain proper knowledge of the BUPERS/NAVPERSCOM CIIL, appendix A. In addition, all staff personnel must maintain awareness of the risks associated with using internet-based capabilities such as a possible increased vulnerability to protected personal information.

2. BUPERS/NAVPERSCOM encourages personnel to responsibly engage in unofficial internet postings about the Department of the Navy (DON) and DON-related activity. The Navy and Marine Corps perform a valuable service around the world every day and DON personnel are frequently in a position to share our successes with a global audience via the internet. DON personnel are responsible for all DON-related content they publish and should ensure this content is accurate, appropriate, and does not compromise mission security or success.
 3. DON personnel are responsible for adhering to DON regulations and policies when making unofficial posts. DON personnel should comply with regulations and policies such as personal standards of conduct, OPSEC, information assurance, PII, joint ethics regulations, and the release of information to the public. BUPERS Millington/NAVPERSCOM prohibits all personnel from disclosing any item on the staff CIIL.
 4. All personnel should be aware that the Internet is often used to gain information for criminal activities such as identity theft. By piecing together information provided on different Web sites, criminals can use the information to, among other things, impersonate DON personnel, steal passwords, and compromise DON networks. Therefore, when using the internet and social media, all personnel should be cautious and guard against cyber criminals and attackers by adhering to the proper security procedures.
 5. Care should also be given when considering information aggregation on the internet and in e-mails. It is possible that the combination of multiple items of unclassified CI within the same situation or context may result in the aggregated information becoming classified. It is generally advisable to move discussions of aggregated information to a classified channel to prevent inadvertent classified spillage.
1305. Summary. To prevent adversaries from gaining actionable intelligence about friendly operations, all BUPERS/NAVPERSCOM personnel must be vigilant in planning and executing OPSEC measures. To be most effective, OPSEC measures should be considered as early as possible during mission planning and then be appropriately revised to keep pace with changes in current operations and threats.

CHAPTER 14 BUILDING SECURITY REGULATIONS

1401. General. The term "building security" is used to identify regulations issued by Department of the Navy (DON) for protection of building spaces or facilities. These regulations are limited to control of access to building, property removal, and related matters.

1402. Security Hours. BUPERS Millington/COMNAVPERSCOM sets building security hours. Security hours are when doors are locked. During these hours, the common access card (CAC) must be used for admittance to BUPERS/NAVPERSCOM buildings. All assigned employees must present their CAC to the Electronic Badging and Entry System (EBACS) reader and be allowed access by using their PIN. While a door may remain open due to handicap entrance door delays, this does not alleviate each member from presenting their CAC and being authorized entry on the EBACS reader. The door does not need to be closed prior to presentation and acceptance of the CAC by the EBACS reader. If an employee uses one of these motorized entrances that has a time delay, they must ensure that anyone directly behind them presents their CAC and enters a personal identification number (PIN) prior to continuing into the workplace. The CAC may be conspicuously worn on outer garments while in BUPERS/NAVPERSCOM buildings for identification purposes, but is not required if external doors are secured and EBACS controlled for entry. It should be removed and properly secured prior to leaving the installation.

1403. Background. Per reference (d), a system of personnel identification is a required basic security measure at naval installations and activities. Positive identification provides a means for visually establishing authorization for personnel movement and actions. Personnel requiring access to BUPERS/NAVPERSCOM buildings are to be identified and access controlled during weekends, holidays, and during periods of increased force protection condition (FPCON) levels.

1404. CAC. All BUPERS/NAVPERSCOM military, civilian, and contractor personnel are required to possess a CAC. Contractor personnel must have on file with BUPERS-00T5 a valid visit request validated by their BUPERS/NAVPERSCOM trusted agent (TA)/contracting officer's representative (COR) point of contact.

1405. Admittance

1. Personnel requiring access to building level 2 restricted spaces must have approved access granted by BUPERS-00T5. A visitor control log will be used in restricted spaces to log all personnel who do not use their CAC to enter and exit the restricted space. Use of the CAC generates an electronic record of the entry and exit and serves as a log of the space entry and exit. Personnel who do not use a CAC must use the visitor control log. Personnel who use their CAC to log their entry must also use it to log their departure. Failure to use the CAC for departure will also result in a "Forced Door Alarm" and NSA Mid-South security will be forced to respond and investigate.

2. During normal working hours, anyone having the following un-expired badges is authorized access to BUPERS/NAVPERSCOM buildings for official business: DoW; NAVPERSCOM proximity badge; a photographic identification card issued by a U.S. Government agency, including retired military and military family members; or a valid identification listed below. If the individual is not an employee of BUPERS/NAVPERSCOM, a visitor with a visit notification that has been delivered to BUPERS-00T5, or does not have credentials from one of the agencies below he or she must be escorted at all times.

a. Visitors From Other Federal Agencies. Security representatives of the following agencies, after coordination is affected with NSA Mid-South Security, may be admitted to BUPERS/NAVPERSCOM buildings at any time to affect official duties upon presentation of their official agency credentials:

- (1) Federal Bureau of Investigations (FBI)
- (2) Military Intelligence (Army)
- (3) Naval Criminal Investigative Service
- (4) Office of Special Investigation (Air Force)
- (5) Secret Service (Treasury Department)
- (6) Department of Homeland Security (DHS)
- (7) Criminal Investigation Command (Army)
- (8) Defense Investigative Service (DIS)
- (9) Defense Protective Service (DPS)
- (10) Defense Criminal Investigative Service
- (11) Counterintelligence Credentials (USMC)
- (12) U.S. Marshall's Service
- (13) Department of Justice (DOJ)

3. Access to BUPERS/NAVPERSCOM spaces controlled by electronic access control must be approved and granted by BUPERS-00T5.

1406. Property Passes. BUPERS/NAVPERSCOM Integrated Logistics Division (BUPERS-00T2) issues property passes. No government property is to be removed from BUPERS/NAVPERSCOM without proper authorization from BUPERS-00T2. When government property is returned, BUPERS-00T2 must be notified. All government property carried by persons entering or leaving BUPERS/NAVPERSCOM buildings is subject to inspection by Naval Support Activity (NAVSUPPACT) Mid-South Security Department and BUPERS-00T5.

1407. Loss of Property, Thefts, and Other Irregularities

1. Loss or theft of Government or personal property, or evidence of tampering with office doors, desks, etc., must be reported to NAVSUPPACT Mid-South Security and BUPERS-00T5.
2. Persons creating a public nuisance, suspicious persons, or other irregularities occurring within BUPERS/NAVPERSCOM spaces will be reported to NAVSUPPACT Mid-South Security and BUPERS-00T5 immediately.

1408. Photography And Audio Recording Equipment and Devices

1. The use of any type of personal photography equipment (i.e., instamatic camera, video tape recorder, digital or film camera, or a cell phone camera) is strictly prohibited in all BUPERS/NAVPERSCOM buildings and spaces without the approval of the BUPERS-00T5 or NAVPERSCOM Public Affairs Officer (PERS-00P). Supervisors may permit use of personal photography equipment on special infrequent occasions such as retirement and award ceremonies. If an individual has government-issued photography equipment in his or her possession, this equipment is to be used for official use only.
2. The use of any type of personal audio recording device, (i.e., tape recorder, cell phone recorder, iPod, eavesdropping ear amplifier (except for use by personnel who have a hearing impairment), is strictly prohibited in all BUPERS/NAVPERSCOM buildings and spaces without the approval of BUPERS-00T5. If an individual has a government-issued audio recording device in his or her possession, this device is to be used for official use only.
3. When an individual plans to use government-furnished photography equipment and or an audio recording device while attending a conference, meeting, or other event, the individual in charge of the session must be made aware of the intended use and must grant his or her approval prior to the use of this equipment or device.
4. Cameras and audio recording devices (regardless of type, model, or brand) are serious information security risks. All command personnel must understand the security risk when using this type of equipment or device in the Government workplace. Personnel found using such equipment or device without approved authorization will have the equipment and or device confiscated and could possibly face disciplinary action.

APPENDIX A

BUPERS MILLINGTON/NAVY PERSONNEL COMMAND CRITICAL INFORMATION AND INDICATORS LISTING

Unclassified information described as personally identifiable information (PII) or Health Insurance Portability and Accountability Act (HIPAA) information must be safeguarded and destroyed per BUPERSINST 5211.7A as critical information (CI). All CI will be sent via encrypted e-mail and properly shredded in an approved shredder when no longer needed. The following unclassified information, also identified as CI, must be treated in the same manner:

- Anti-terrorism/force protection and law enforcement assessments, plans, and reports
- Board records (administrative, promotion, or selection) until approved and released; board deliberation materials will remain as CI, even after release of official board results
- Budget or financial documentation; includes current and future planning documents
- Contingency of operations (COOP) plans
- Full organizational roster and phone listings with names
- Inspection results and investigative findings
- Information technology system records and databases
- Mail (unopened) and guardmail
- Manpower force structure plans and documents
- Preliminary contractual deliberation materials
- Prisoner records and detainee operations reports
- Safety mishap reports
- Scope-of-work orders and contract documents
- Security access and clearance information
- Standard operating procedures
- Subordinate command CI
- Travel arrangements for senior personnel
- Various recurring and in situ reports (monthly, annual, etc.) that could be exploited by adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage and may prevent or complicate mission accomplishment, reduce mission effectiveness, or cause loss of lives or damage to friendly resources

APPENDIX B

FORMS

1. The following forms may be obtained from the Executive Services Directorate Web site at:
<https://www.esd.whs.mil/DD/DoD-Issuances>:
 - a. DD 254 Department of Defense Contract Security Classification Specification
 - b. DD 2501 Courier Authorization

2. The following forms may be obtained from the General Services Administration Web site at:
<https://www.gsa.gov/forms>.
 - a. SF 312 Classified Information Nondisclosure Agreement and Espionage Act
 - b. SF 701 Activity Security Checklist
 - c. SF 700 Security Container Information
 - d. SF 702 Security Container Check Sheet
 - e. SF 703 Top Secret (Cover Sheet)
 - f. SF 704 Secret (Cover Sheet)
 - g. SF 705 Confidential (Cover Sheet)

3. The following forms may be obtained from Navy Forms Online at:
<https://forms.documentservices.dla.mil/order/>:
 - a. OPNAV 5216/10 Correspondence/Material Control Sheet
 - b. OPNAV 5239/14 System Authorization Access Request (SAAR)
 - c. OPNAV 5511/10 Record of Receipt
 - d. OPNAV 5511/12 Classified Material Destruction Report

- e. OPNAV 5511/13 Record of Disclosure
 - f. OPNAV 5511/14 Security Termination Statement
 - g. OPNAV 5511/27 Briefing/Re-Briefing/Debriefing Certificate
4. NAVPERS 5520/6 Request for Security Access can be obtained from NAVPERSCOM Web site at <https://www.public.navy.mil/bupers-npc/reference/forms/NAVPERS/Pages/default.aspx>: