



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

BUPERSINST 5510.61C
BUPERS-00Y
28 Jul 2017

BUPERS INSTRUCTION 5510.61C

From: Chief of Naval Personnel

Subj: BUREAU OF NAVAL PERSONNEL COMMAND SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.36A
(b) OPNAVINST 3432.1A
(c) SECNAVINST 5510.30B
(d) OPNAVINST 5510.60M
(e) OPNAVINST 5510.165A
(f) BUPERSINST 5211.7

Encl: (1) BUPERS Millington/Navy Personnel Command Critical Information Listing

1. Purpose

a. To establish policy and provide guidance for information, operations, and personnel security.

b. Major revisions to this instruction include expanding the command security program to include operations security; a new requirement for commands to general a critical information list (CIL); and expansion of command action requirements. This instruction has been completely revised and must be read in its entirety.

2. Cancellation. BUPERSINST 5510.61B.

3. Scope and Applicability. This instruction supplements the basic guidance for the Navy Information Security Program (ISP), reference (a); Operations Security Program (OSP), reference (b); and Personnel Security Program (PSP), reference (c). Provisions of this instruction apply to all military, civilian, and contract personnel, and to all activities within the Bureau of Naval Personnel (BUPERS) claimancy. BUPERS personnel located in Washington, DC will be 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, Industrial, Operations, and Personnel Security Programs.

5. Discussion. An effective command 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 command security program.

6. Responsibilities

a. Commanders, commanding officers, and officers in charge are responsible for compliance and implementation of references (a), (b), (c), and (e) within their commands.

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

c. All BUPERS commanders, commanding officers, and officers in charge are responsible for implementation of this instruction for their command and subordinate activities.

7. Action

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

b. 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).

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

d. Commands must generate a CIL and ensure all assigned personnel are aware of the sensitive information handled by the command. Enclosure (1) is BUPERS Millington/Navy Personnel CIL and serves as an example for subordinate commands to follow.

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

8. Records Management. Records created as a result of this instruction, regardless of media or format, must be managed per SECNAV Manual 5210.1 of January 2012.

9. Review and Effective Date. Per OPNAVINST 5215.17A, BUPERS-00Y will review this instruction annually on the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, SECNAV, and navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire

5 years after its issuance date unless reissued or canceled prior to the 5-year anniversary date, or an extension has been granted.



R. A. BROWN
Deputy Chief of Naval Personnel

Releasability and distribution:

This instruction is cleared for public release and is available electronically only via BUPERS Web site, [http://www.public.navy.mil/bupers-npc/reference/instructions/ BUPERSInstructions/Pages/default.aspx](http://www.public.navy.mil/bupers-npc/reference/instructions/BUPERSInstructions/Pages/default.aspx)

BUPERS MILLINGTON/NAVY PERSONNEL COMMAND CRITICAL INFORMATION
LISTING

All classified information must be maintained and stored in approved National Security information containers and safes.

Unclassified information identified as critical is described as “sensitive but unclassified” or as “personally identifiable information (PII).” All personnel handling PII must be qualified to handle and work with it. Examples of unclassified critical information are as follows:

- Board records (administrative, promotion, or selection)
- Budget or financial documentation
- Building plans and blueprints
- Contingency of operations plans
- Electronic Key Management System (EKMS)/Key Management Infrastructure administration documents
- Emergency plans
- Employee performance reports
- Employee suggestions and complaints
- Environmental impact statements
- Identification cards
- Information contained on command sharepoint and Web home pages
- Inspection results and investigative findings
- Instructions, directives, standard operating procedures, and operating manuals
- Information technology system records and databases
- Mail, unopened; and guardmail
- Manpower plans and documents
- Medical case information
- Meeting minutes or notes
- News releases and published articles
- Orders - detailer and placement notes
- Pay records
- Personnel photographs
- Personnel records
- Personnel staffing reports and manning documents
- Position vacancy documents and information
- Prisoner records and detainee operations reports
- Project plans and progress reports
- Safety reports
- Scope-of-work orders and contract documents

- Security clearance information
- Shipping requests or announcements
- Standard operating procedures
- Supply documents and purchasing requests
- Travel requests, trip reports, and travel arrangements
- Various recurring and in situ reports (monthly, annual, etc.)
- Work schedules and leave documents

*Critical information is information about friendly (U.S., allied, and or coalition) activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Critical information may be classified or unclassified. Another term for critical information is “essential elements of friendly information.” Such information, if revealed to an adversary prematurely, may prevent or complicate mission accomplishment, reduce mission effectiveness, or cause loss of lives or damage to friendly resources.