



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

BUPERSINST 5239.4  
BUPERS-07  
24 Aug 2018

BUPERS INSTRUCTION 5239.4

From: Chief of Naval Personnel

Subj: DATA TRANSFER

Ref: (a) SECNAVINST 5211.5E  
(b) 5 U.S.C. §552a  
(c) DoD Directive 5400.11 of 29 October 2014  
(d) DoD Directive 8140.01 of 11 August 2015  
(e) DoD Instruction 5400.16 of 14 July 2015  
(f) DoD Instruction 8580.02 of 12 August 2015  
(g) BUPERSINST 5211.7A  
(h) DoD Instruction 1000.30 of 1 August 2012  
(i) DoD 5400.11-R, DoD Privacy Program, May 2007  
(j) SECNAVINST 5720.44C  
(k) BUPERSINST 4491.1  
(l) GENADMIN DON CIO WASHINGTON DC 192101Z REV 10/2016

Encl: (1) Compliance Review Process Model  
(2) Systems Interface Description (SV-1) Example  
(3) Systems Resource Flow Matrix (SV-6) Example

1. Purpose

a. To protect Bureau of Naval Personnel (BUPERS) data per references (a) through (l).

b. To establish a uniform process to account for and review data transfers as it applies to all information systems within the BUPERS enterprise and all data transfer activities interacting with enterprise systems or applications. A visual depiction of the Compliance Review Process can be found in enclosure (1). For inquiries and media requests please refer to the following:

(1) Freedom of Information Act inquiries: <http://www.secnav.navy.mil/foia/Pages/default.aspx>.

(2) Congressional inquiries: <http://www.navy.mil/navydata/people/ola/ola-info.html>.

(3) Media Request: Refer to reference (j) for further guidance.

2. Scope and Applicability. This instruction applies to all BUPERS military and civilian personnel and Department of Defense (DoD) contractors.

3. Policy. It is BUPERS policy, per reference (a), that appropriate administrative, technical, and physical safeguards are observed to ensure records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected. The following requirements apply to the transfer of any BUPERS' data:

a. Requests for data transfers from any person, agency, organization or contracted institution that requests movement of data via any means will be submitted for compliance review and must be substantiated by a vetted business need.

b. In order for the Enterprise Information Management Team (EIMT) to gain a complete understanding of the business need driving the data request, the compliance review process must be included at the earliest opportunity (see enclosure (1)).

c. Compliance reviews for data requests that are greater than 60 days old will be closed if a response or feedback from the originator has not been received.

d. New data transfers will not be established with BUPERS information systems until a favorable compliance review has been completed.

e. Compliance reviews for existing data interfaces will be performed in parallel with the renewal or extension of a system's authority to operate (ATO), interim authority to operate (IATO), interim authorization to test (IATT), or when an interface control document (ICD) is updated, or at the request of the chief data steward (CDS), technical manager, or system manager of the system to which any of these conditions apply.

f. Data compliance approval expires whenever the following occurs:

(1) The information system has any change within the data interface architecture or in its security posture.

(2) When information systems perform updates or recertification of their ATO or IATO.

(3) Unless renewed, the system manager will terminate all persistent interfaces upon the expiration or termination of the system's ATO or IATO.

g. If a system is found to be non-compliant, existing data transfers will be terminated and will not be restored until evidence of compliance has been demonstrated.

#### 4. Roles and Responsibilities

a. CDS

(1) Act as the functional data manager and name space coordinator supporting BUPERS, Personnel Management and Training and Education functional area manager.

(2) Direct the effective administration of the BUPERS Data Management Program.

(3) Develop and promote data strategies, policies, practices, standards, architecture, procedures, and metrics to include, but not limited to:

(a) Developing standard operating procedures for all repeatable and essential data processes.

(b) Reviewing and making recommendations for any transfer of data, information exchange, or interface requests from a BUPERS system of record.

(c) Overseeing the review of all updates to and development of BUPERS systems and applications, memorandums of agreement (MOA), and ICD.

(d) Overseeing the retention and storage of all approved MOAs, ICDs, and security interface agreements.

(e) Reviewing and making recommendations to business enterprise architecture data and information viewpoint conceptual and logical data models.

(f) Reviewing, approving, and developing processes and procedures for using data generated from non-BUPERS systems and how they are to be used within BUPERS.

b. EIMT. Has overall responsibility to research and make recommendations to the point of contact for the requesting system. EIMT has the following responsibilities in facilitating the compliance review:

(1) Ensuring all requirements of law, DoD, and DON are met prior to the release of information.

(2) Emailing NAVPERS 5239/9 Compliance Review Checklist for Data Transfer and Request to the requestor upon receipt of an approved Enterprise Information Management - Service Request through SharePoint. For information on how to submit the Enterprise Information Management Service Request, refer to reference (k).

(3) Analyzing NAVPERS 5239/9 and associated documents to validate compliance with DoD and DON requirements per references (a) through (e).

(4) Identifying the source information system from which the requested data is to be supplied.

(5) Upon completion of NAVPERS 5239/9 by the EIMT, forward it, with the recommendation to “approve” or “disapprove,” and any additional comments to the CDS and system manager. The CDS and system manager will review the form and provide a recommendation to “approve” or “disapprove” the requested data.

(6) Notifying the BUPERS enterprise architect of new data transfers or changes to existing data transfers of BUPERS data.

(7) Monitoring established data transfers for continued compliance through the periodic review of ICDs.

(8) Emailing disapproved NAVPERS 5239/9 to the applicable system manager to terminate the data transfer of a system that is found non-compliant.

c. System Manager. A system manager is an official who has overall responsibility for a system of records. The system manager may serve at any level in DON and is indicated in the published System of Records Notice (SORN). If more than one official is indicated as a system manager, initial responsibility resides with the manager at the appropriate level (i.e., for local records at the local activity) as defined by reference (a). In addition to the responsibilities found in references (a) and (c), a system manager has the following responsibilities in the compliance review process:

(1) Reviewing NAVPERS 5239/9 and the requested data elements, along with the supporting documents provided by the EIMT, to determine approval or disapproval.

(2) Establishing MOA, memorandums of understanding (MOU), ICDs, data processing system requests, or request for information services as required to establish fulfillment of the data transfer requests.

(3) Annotating the adjudication of the request for information on NAVPERS 5239/9.

(4) Forwarding the final ICD to the EIMT upon system interface implementation.

(5) Terminating any data transfer(s) of a system(s) that are found non-compliant.

(6) Upon completion of the compliance review, an MOU and or ICD will be developed between organizations to formalize agreements for usage and disposal of the data. These documents will be reviewed annually and updated every 3 years in conjunction with the renewal of the system's ATO.

d. Technical Manager. Responsible for the successful development and delivery of a business capability by managing technical risks and opportunities, making key software design and implementation decisions with the development teams, scheduling tasks that include tracking dependencies, managing change requests, and guaranteeing quality deliveries.

e. Information Assurance Manager. In the course of the compliance review process, should information assurance or security concerns arise; a review by the information assurance manager of the source system will be requested.

f. Privacy Program Manager. In the case of any privacy concerns with regards to personally identifiable information (PII), SORNs, privacy impact assessments (PIA), or social security number (SSN) justification memorandums, a review by the Privacy Program manager of the source system will be requested. All suspected or confirmed PII incidents or breaches will be reported upon discovery to the BUPERS Privacy Program Manager

5. Compliance Requirements. NAVPERS 5239/9 was developed to facilitate compliance reviews and ensure a record is maintained for an information system requesting BUPERS data. The form requests the following information:

a. Requesting system will provide the EIMT

- (1) Point of contact, program manager, technical manager, and security lead information
- (2) Name of the system
- (3) Physical location of system

b. Law, Policy, or Instruction

- (1) Will support the business need
- (2) Requesting system will provide justification of the data need

c. Data Transfer and Architecture Information. A system that is requesting an interface will provide a brief description of the architecture and data transfer including, but not limited to, the following:

- (1) The network the system interface will reside on.
- (2) Department of Defense Architectural Framework (DoDAF) Systems Interface Description (SV-1), enclosure (2).
- (3) DoDAF Systems Resource Flow Matrix (SV-6), detailing data that is requested from BUPERS information system, enclosure (3).

(a) A draft SV-6 must be submitted as part of the compliance review, describing the requirements of the data transfer being requested.

(b) A final SV-6, describing the actual implementation of the new data exchange must be submitted to the EIMT upon acceptance of the work by the customer.

(c) In cases where the data transfer being complied will involve the transfer of data to a system (vice an organization or individual), the final SV-6 must be comprehensive; it will **detail ALL of the data exchanges from ALL systems, both in and out of the system, to**

which the BUPERS data is being transferred. Upon request, the EIMT can provide existing SV-6 information to facilitate updating the comprehensive SV-6.

d. Cyberspace Workforce. The requesting system will provide an email from its respective information system security manager stating that the information assurance workforce operating the system is compliant with reference (d).

e. One-Time Data Transfer. A request for a one-time data transfer will provide a brief description of, but not limited to, the following:

- (1) Storage and destruction criteria of the data requested.
- (2) List of specific data elements requested.
- (3) Transfer method of the data.

f. Systems under Development. Test data should be used for systems under development to mitigate any problems that might arise due to a lack of an IATT, IATO, or ATO.

g. Certification and Accreditation Documentation. The requesting information system will provide the appropriate information assurance documentation as required by NAVPERS 5239/9. Any information system requesting a connection to BUPERS systems must be certified and accredited. This DoD risk management framework process will take into consideration the system mission, environment, and architecture while assessing any operational impact on the DoD infrastructure.

h. Defense Business System or Database Registration. The requesting information system will provide the following, as applicable:

- (1) DoD Information Technology Portfolio Registry-Department of the Navy (DITPR-DON) ID
- (2) DoD Information Technology Portfolio Registry (DITPR) ID
- (3) Enterprise Mission Assurance Support Service (eMASS) ID
- (4) DON Applications and Database Management System (DADMS) ID
- (5) SORN ID

i. PII. For further guidance refer to reference (g).

- (1) When PII is requested, an approved PIA must be included with NAVPERS 5239/9.

(2) When SSNs are requested, per reference (1) an approved SECNAV 5213/1 SSN Reduction Review must be provided in conjunction with the NAVPERS 5239/9.

(3) When privacy and health information is requested in support of research or a study protocol, an approved Institutional Review Board or Human Research Protection Office adjudication letter must be included with the submitted NAVPERS 5239/9.

(4) All documents (paper and electronic) containing PII must contain the privacy warning "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

(5) Recipients of PII are required to sign NAVPERS 5211/16 Statement of Understanding verifying that they will protect PII in accordance with all laws, policies and directives, and that they will not modify or share data unless approval is granted from the CDS to do so.

j. Requesting Information System Category. This section requires a selection of one of the following:

(1) State or local agency

(2) Federal information system external to the DoD

(3) External information systems outside of the Federal domain under contract with a Federal organization

(4) DoD information system or service-specific information system

k. When the compliance review has been completed and approved by the source system manager, it will be distributed to the appropriate parties. Upon receipt of the approved compliance review, the requestor will submit a work request via Requirements Change Management Solution (RCMS) to initiate the extraction and movement of data. If the requestor does not have access to the RCMS tool, the EIMT will submit the work request on their behalf.

6. Point of Contact. Data Transfer and Compliance Coordinator (901) 874-3663; all correspondence should be routed to the following email address: [MPTE\\_EIM@navy.mil](mailto:MPTE_EIM@navy.mil).

## 7. Records Management

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

b. Data collected to support reports created, regardless of media or format must be destroyed within five business days following delivery or briefing of report; this is to ensure that only the timeliest data is used.

8. Review and Effective Date. Per OPNAVINST 5215.17A, BUPERS Command Information Officer (BUPERS-07), will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after effective date unless reissued or canceled prior to the 5-year anniversary date, or an extension has been granted.

9. Forms

a. SECNAV 5213/1 SSN Reduction Review can be obtained from DON Naval Forms Online at [https://navalforms.documentservices.dla.mil/formsDir/SECNAV\\_5213\\_1\\_4999.pdf](https://navalforms.documentservices.dla.mil/formsDir/SECNAV_5213_1_4999.pdf).

b. The following NAVPERS forms are available electronically at <http://www.public.navy.mil/bupers-npc/reference/forms/NAVPERS/Pages/default.aspx>:

(1) NAVPERS 5211/16 Statement of Understanding

(2) NAVPERS 5239/9 Compliance Review for Data Transfer and Request



J. W. HUGHES  
Deputy Chief of Naval Personnel

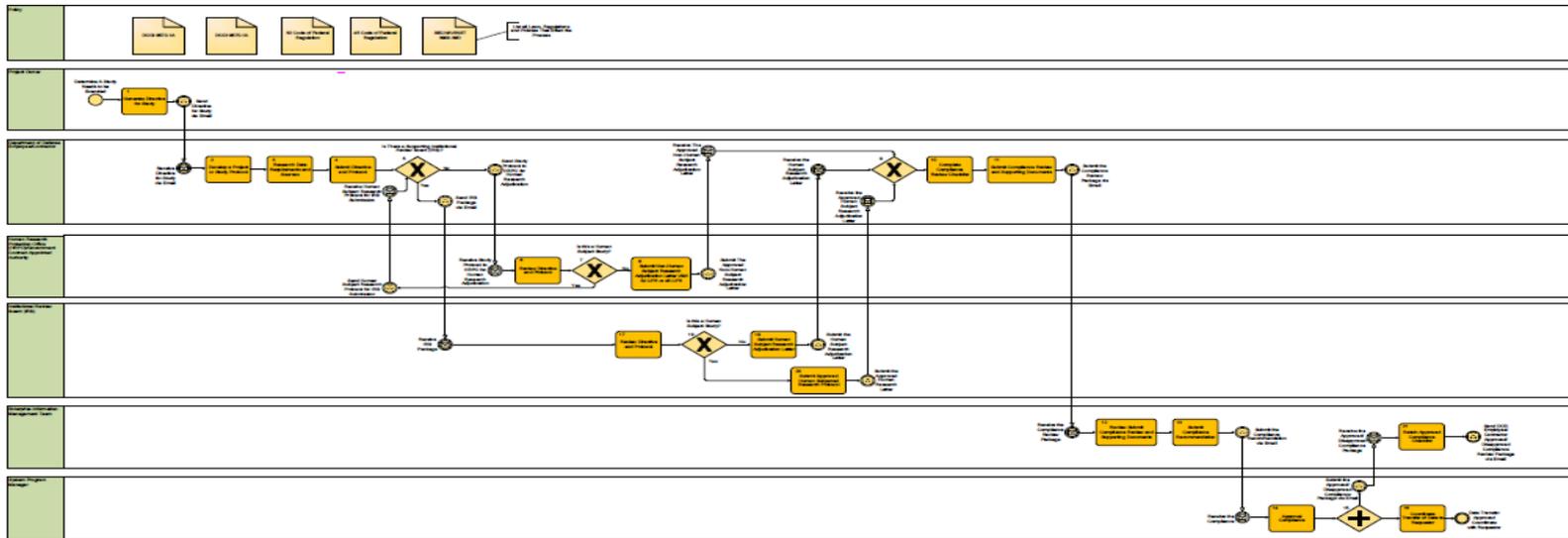
**Releaseability and distribution:**

This instruction is cleared for public release and is available electronically only via BUPERS Web Site, <http://www.public.navy.mil/bupers-npc/Pages> .

COMPLIANCE REVIEW PROCESS MODEL

Example:

<https://mpte.navy.deps.mil/sites/organizations/EIMB/Reference%20Documents/Conduct%20Compliance%20Review.pdf>



SYSTEMS INTERFACE DESCRIPTION (SV – 1) EXAMPLE

