



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

BUPERSINST 5239.4A
BUPERS-07
15 Jul 2021

BUPERS INSTRUCTION 5239.4A

From: Chief of Naval Personnel

Subj: DATA TRANSFER

Ref: (a) SECNAVINST 5211.5F
(b) 5 U.S.C. §552a
(c) DoD Instruction 5400.11 of 29 January 2019
(d) DoD Directive 8140.01 of 5 October 2020
(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, 14 May 2007
(j) SECNAVINST 5720.44C
(k) BUPERSINST 4491.1A
(l) DoD Instruction 1000.30 of 1 Aug 2012.

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, as well as all data transfer activities interacting with enterprise systems and applications. A visual depiction of the compliance review process is located in enclosure (1). For inquiries and media requests, please refer to the following:

(1) Freedom of Information Act inquiries: <https://www.mynavyhr.navy.mil/References/FOIA/>.

(2) Congressional inquiries: <https://www.navy.mil/Navy-Office-of-Legislative-Affairs>.

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

c. This instruction was revised to establish a uniform process to account for and review data transfers as it applies to all information systems within the BUPERS enterprise, as well as all data transfer activities interacting with enterprise systems and applications. Updated the requirements for contractor-owned or –operated systems and the addition of a statement regarding limitations on test data sets.

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 resulting in movement of data by any means will be submitted for compliance review and must be substantiated by valid business need.

b. Initiate the compliance review process at the earliest opportunity, see enclosure (1).

c. BUPERS information systems will not establish new data transfers until a compliance review has been completed and approved.

d. 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 manager of the system to which any of these conditions apply.

e. 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.

f. 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.

g. 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.

4. Roles and Responsibilities

a. CDS - Acts as the functional data manager and name space coordinator supporting BUPERS, Personnel Management, Training, and Education Functional Area Manager.

(1) Directs the effective administration of the BUPERS Data Management Program.

(2) Develops and promotes data strategies, policies, practices, standards, architecture, procedures, and metrics to include, but not limited to:

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

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

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

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

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

(f) Reviews, approves, and develops processes and procedures for using data generated from non-BUPERS systems.

b. Enterprise Information Management Team (EIMT) - Has overall responsibility to research and make recommendations to line of business data stewards requesting data transfer. EIMT has the following responsibilities in facilitating the compliance review:

(1) Prior to the release of data, ensure all requirements of law, DoD, and Department of the Navy (DON) are met.

(2) E-mail NAVPERS 5239/9 Compliance Review Checklist for Data Transfer and Request, to the requestor upon receipt of an approved Enterprise Information Management - Service Request via SharePoint. For guidance on submitting the Enterprise Information Management Service Request, refer to reference (k).

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

(4) Identify the authoritative source system from which the requested data will be supplied.

(5) Route completed NAVPERS 5239/9, with the recommendation of “approve” or “disapprove,” as well as any additional comments, to the CDS and system manager.

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

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

(8) E-mail 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. An official who has overall responsibility for a system of records. The system manager may serve at any level in the 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) Review NAVPERS 5239/9, requested data elements, as well as all supporting documentation provided by the EIMT to determine approval or disapproval.

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

(3) Annotate the adjudication of the request for data on NAVPERS 5239/9.

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

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

(6) Upon completion of the compliance review, a memorandum of understanding 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 of the source system by the information assurance manager will be requested.

f. Privacy Program Manager. When privacy concerns related to personally identifiable information (PII), SORNs, privacy impact assessments, or social security number (SSN) justification memorandums are identified, request a review by the privacy program manager of the source system. At discovery, report all suspected or confirmed PII incidents or breaches to the BUPERS Privacy Program Manager.

5. Compliance Requirements. NAVPERS 5239/9 are used to facilitate the compliance reviews process and ensure proper documentation of data movement. The following information is required:

a. Requesting system will provide:

- (1) Point of contact
- (2) Program manager
- (3) Technical manager
- (4) Security lead information
- (5) Name of the system
- (6) Physical location of system

b. Law, Regulation, or Policy

- (1) Will support the business need
- (2) Requesting system will provide justification of the data required
- (3) In the event the requesting system is contractor-owned or –operated, a copy of the governing contract and or applicable statement of work will be requested for review to ensure compliance with Privacy Act of 1974, section 552a (m) and for the inclusion of 48 CFR chapter 1, Federal Acquisition Regulation (FAR) clauses within the contract.

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) DoD 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) Submit a draft SV-6 as part of the compliance review, describing the requirements of the data transfer.

(b) Submit a final SV-6, describing the actual implementation of the new data exchange 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 may provide existing SV-6 information to facilitate updating the comprehensive SV-6.

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

e. One-Time 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. Current system limitations prevent the data compliance team from providing test data sets.

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 ID
- (2) DoD Information Technology Portfolio Registry ID
- (3) Enterprise Mission Assurance Support Service ID
- (4) DON Applications and Database Management System ID
- (5) SORN ID

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

(1) Requesting PII must include an approved privacy impact assessments with NAVPERS 5239/9.

(2) Requesting SSNs must include an approved SECNAV RCS 5213/1 with NAVPERS 5239/9 (see reference (1)).

(3) If privacy and health information in support of research or a study protocol is requested, include an approved Institutional Review Board or Human Research Protection Office adjudication letter with the 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 Employee PII Handling Statement of Understanding verifying that they will protect PII, per 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, the compliance review is 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. All correspondence should be routed to the Data Transfer and Compliance Coordinator at e-mail: MPTE_EIM@navy.mil.

7. Records Management

a. Records created as a result of this instruction, regardless of media and format, 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>.

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

8. Review and Effective Date. Per OPNAVINST 5215.17A, BUPERS-00D will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency and consistency with Federal, Department of Defense, Secretary of the Navy, 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 guidance in OPNAV Manual 5215.1 of May 2016.

9. Forms

a. SECNAV 5213/1 SSN Reduction Review is available at: <https://www.secnav.navy.mil/doni/NFOL/Forms/AllItems.aspx?RootFolder=%2Fdoni%2FNFOL%2FSECNAV%2FSECNAV%20Forms&FolderCTID=0x012000365D27B574A66144834C11A9CDABB889&View=%7BB4E89F14%2D5AE1%2D4D83%2DB85E%2DC63169BF9E34%7D>.

b. The following NAVPERS forms are available at: <https://www.mynavyhr.navy.mil/References/Forms/NAVPERS/>.

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

(2) NAVPERS 5211/16 Employee PII Handling Statement of Understanding



A. HOLSEY

Deputy Chief of Naval Personnel

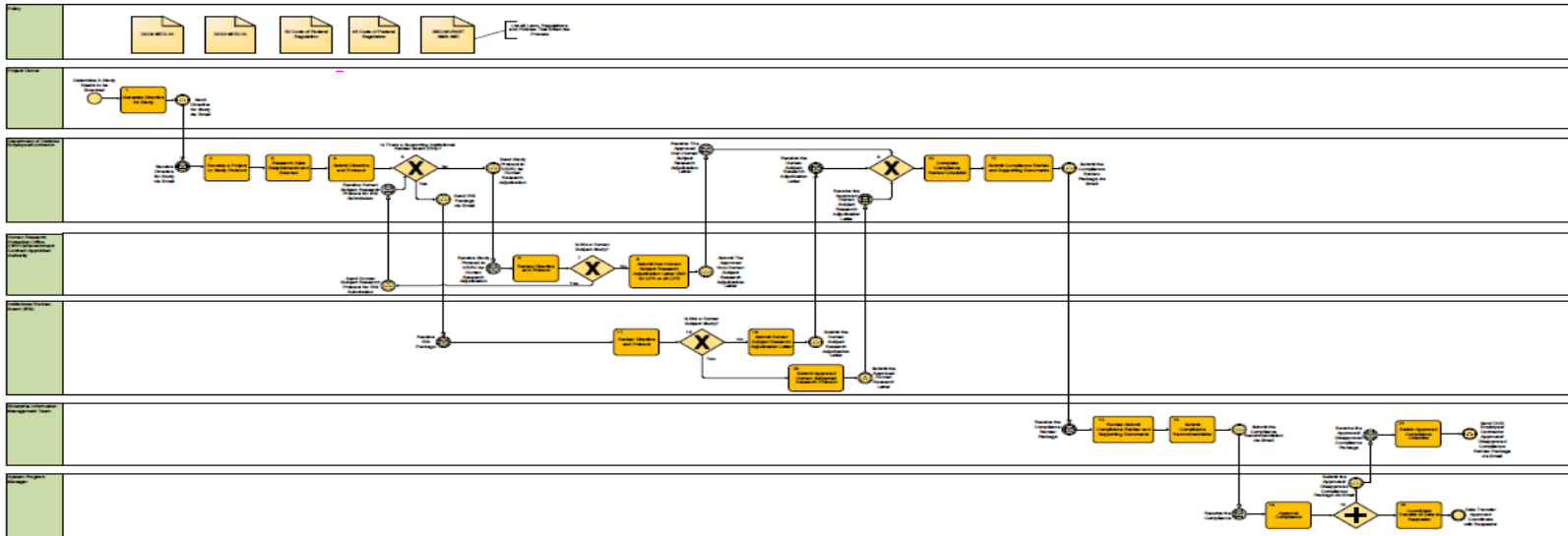
Releaseability and distribution:

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

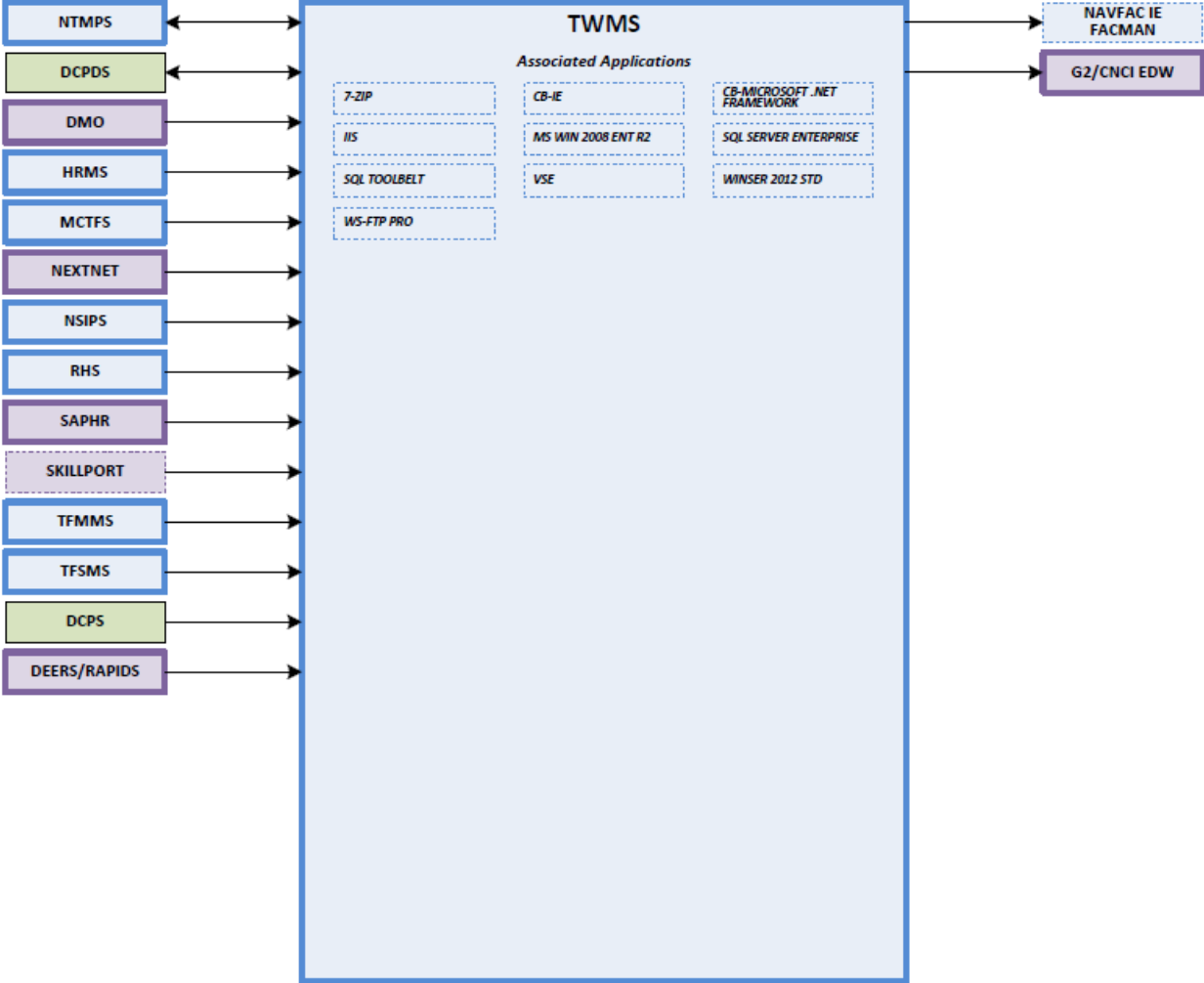
COMPLIANCE REVIEW PROCESS MODELS

Example:

<https://mpte.navy.deps.mil/sites/organizations/EIMB/DTC/Forms/AllItems.aspx?RootFolder=%2Fsites%2Forgанизations%2FEIMB%2FDTC%2FBUPERINST%205239%205F4%20Hyperlink%20Support%20Documents&FolderCTID=0x0120004951FDCC8ECE984FB1D007367AD836C0&View=-%7BC9CD4324%2D6DB7%2D4409%2DBB65%2D24DA514CA8D5%7D>



SYSTEMS INTERFACE DESCRIPTION (SV – 1) EXAMPLE



SYSTEMS RESOURCE FLOW MATRIX (SV – 6) EXAMPLE

https://mpte.navy.deps.mil/sites/organizations/EIMB/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/organizations/EIMB/DTC/BUPE RINST%205239_4%20Hyperlink%20Support%20Documents/SV-6%20System%20Data%20Exchange%20Matrix%20Template%2020190520.xlsm&action=default

Example of the Data Exchange

Change Properties	Operational Requirements	Producer			Consumer			Data Exchange			
Data Content ID (must be unique)	Data Exchange Description	Operational Requirement Identifier	Sending System Acronym	Sending System Function Name	Sending Performer	Receiving System Acronym	Receiving System Function Name	Receiving Performer	Interface Type	Interface sub-type	Encrypted Yes/No
ADE_0250	PUBcycleDEFpgrade		NEAS	Send Human Resources Data to External Destination	NEAS	ADE 2.0	Collect Human Resources Data from External Source	ADE 2.0	Automated Interface	Extract	No SI
ADE_0250	PUBcyclePROFpgrade		NEAS	Send Human Resources Data to External Destination	NEAS	ADE 2.0	Collect Human Resources Data from External Source	ADE 2.0	Automated Interface	Extract	No SI
ADE_0250	PUBcycleRSPpgrade		NEAS	Send Human Resources Data to External Destination	NEAS	ADE 2.0	Collect Human Resources Data from External Source	ADE 2.0	Automated Interface	Extract	No SI