



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

BUPERSINST 5450.56A
BUPERS-07

5 MAY 2014

BUPERS INSTRUCTION 5450.56A

From: Chief of Naval Personnel

Subj: REPORTING RELATIONSHIPS, ROLES, AND RESPONSIBILITIES
OF THE BUREAU OF NAVAL PERSONNEL COMMAND INFORMATION
OFFICER

Encl: (1) References
(2) CIO Roles and Responsibilities
(3) Definitions

1. Purpose. To define the reporting relationships, roles, and responsibilities of the Bureau of Naval Personnel (BUPERS), Command Information Officer (CIO) (BUPERS-07), and to delegate the authorities necessary to draft and implement policy related to the management of information technology (IT) assets and resources. Enclosure (1) lists applicable references.

2. Cancellation. BUPERSINST 5450.56.

3. Applicability. This instruction applies to all activities that fall under BUPERS and manage/own IT assets or resources that are funded under Budget Submitting Office 00022.

4. Discussion

a. Reference (a) states the command information officer (abbreviated as command IO or CIO) serves an important role as the principal advisor to his or her commander for issues regarding information management (IM) and alignment of IT investments to business priorities and assigned missions. The effective execution of this role requires the BUPERS CIO (BUPERS-07) be charged with management oversight of the BUPERS element of the enterprise information environment (EIE). This component of the EIE is a critical enabler of business processes that provides administrative support to the Navy mission and individual Sailors. To ensure availability, access, accuracy, and agility, the BUPERS CIO (BUPERS-07) must be empowered to draft and implement policy designed to protect and mature the BUPERS information environment, including the processes that

5 MAY 2014

govern the acquisition and use of IT services, systems, applications, databases, and the supporting infrastructure.

b. BUPERS CIO (BUPERS-07) shall promulgate policy to govern the execution of the following day-to-day functions as they relate to the acquisition, development, procurement, management, modification, improvement, enhancement, and retirement of IT assets or services: information resources management, configuration management, risk management, program management, project management, performance management, data management, knowledge management, portfolio management (to include Department of Defense (DoD)/Department of the Navy (DON) compliance), quality assurance, information assurance (IA), contract administration, enterprise architecture (EA), and capital planning and investment control.

5. Policy

a. Reporting Relationships. The following reporting relationships are established to comply with DON policy and to facilitate the management of IT-related functions and policy execution throughout BUPERS activities:

(1) BUPERS CIO

(a) Per reference (a), shall report to the Chief of Naval Personnel when performing duties as the CIO and to the DON Deputy CIO (Navy) when supporting matters pertaining to DON IM/IT policy.

(b) Per reference (b), BUPERS CIO (BUPERS-07) shall support the Office of the Chief of Naval Operations (OPNAV), Information Management Division (N156), in performing IM/IT planning, programming, budgeting, and execution activities.

(c) Per reference (b), BUPERS CIO (BUPERS-07) shall assist each functional area manager (FAM) in the development and management of IT asset portfolios to ensure strategic alignment, standardization, investment concurrence, and compliance with other IT-related DoD/DON mandates and initiatives.

(d) Per reference (c), BUPERS CIO (BUPERS-07) shall report to the Navy operational designating approving authority in matters pertaining to IA policies, controls, and

5 MAY 2014

certification and accreditation processes as they apply to systems during acquisition, development, and test and evaluation phases.

(2) BUPERS echelons 3 and 4 command IT leadership

(a) In addition to their normal reporting relationship, each BUPERS echelon 3 and 4 command IT director/IT department head or equivalent shall report to the BUPERS CIO (BUPERS-07) on matters pertaining to the implementation and execution of DoD, DON, or BUPERS IM/IT policy.

(b) Per reference (c), each BUPERS echelon 3 and 4 command information assurance manager (IAM) shall report to BUPERS, IAM (BUPERS-073) on matters pertaining to designated IA roles and responsibilities.

b. Roles. BUPERS CIO (BUPERS-07) shall promulgate policy to support the roles of the CIO outlined in reference (a) and listed in enclosure (2).

c. Responsibilities. BUPERS CIO (BUPERS-07) shall promulgate policy to support the functions of the CIO outlined in reference (a) and reproduced in enclosure (2). Additional responsibilities assigned by the Deputy Chief Naval Personnel include:

(1) Designate a maintenance coordinator to provide BUPERS IT system scheduled maintenance and availability information and to facilitate the reporting and resolution of outage events.

(2) Per reference (d), conduct quarterly program reviews to monitor the execution and programming posture of BUPERS IT systems and programs of record. (Note: references (e) through (q) support the definitions found in enclosure (3)).

(3) Per reference (r), manage and oversee the activities of the BUPERS Information Assurance Internal Audit Program to facilitate compliance and an improved security posture.

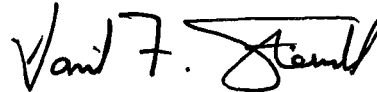
(4) Designate a business continuity coordinator to manage and mature the BUPERS Continuity and Contingency Program as outlined in reference (s).

5 MAY 2014

(5) Designate a personally identifiable information (PII) coordinator to act as the command's central point of contact for PII-related functions, namely the reporting and processing of PII breaches.

6. Point of Contact. BUPERS (BUPERS-07) can be contacted at (901) 874-3081/DSN 882.

7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per Secretary of the Navy Manual M-5210.1 of January 2012.



DAVID F. STEINDL
Rear Admiral, U.S. Navy
Deputy Chief of Naval Personnel

Distribution:
Electronic only, via BUPERS Web site
<http://www.npc.navy.mil>

5 MAY 2014

REFERENCES

- (a) DON CIO Memo, Roles, Relationships, and Core Competencies of Department of the Navy Command Information Officers Policy of 25 Jan 08
- (b) SECNAVINST 5000.36A
- (c) NAVNETWARCOM Designation Letter, Appointment of Developmental Designating Accrediting Authority (DDAA) and Research, Development, Test, and Evaluation (RDT&E) (RDAA) of 15 Jul 2009 (NOTAL)
- (d) BUPERSINST 5230.5
- (e) Defense Acquisition System Glossary of Defense Acquisition Acronyms and Terms, 12th Edition (<https://dap.dau.mil/aphome/das/Pages/DAUOnlineGlossary.aspx>)
- (f) Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources of 28 Nov 2000
- (g) DoD Directive 8115.01 of 10 October 2005
- (h) DoD Directive 8500.01E of 24 October 2002
- (i) 44 U.S.C. §3506
- (j) CJCS Instruction 3170.01G, Joint Capabilities Integration and Development System of 1 Mar 2009
- (k) 40 U.S.C. §11101
- (l) DON CIO memo, DON Knowledge Management Strategy of 20 Oct 05
- (m) DoD Instruction 5000.02 of 25 November 2013
- (n) DON Applications and Database Management System (DADMS) User Guide: Registration and Disposition Process for the United States Navy Networks/Servers, Network Devices, and Server Applications Revision 3 (Version 3) (NOTAL)
- (o) DoD Extension to: A Guide to the Project Management Body of Knowledge (PMBOK) of Jun 2003
- (p) 44 U.S.C. §2901
- (q) National Institute of Standards and Technology (NIST) Special Publication 800-30, Risk Management Guide for Information Technology Systems of Jul 2002
- (r) BUPERSINST 5239.3
- (s) BUPERSINST 5230.8A

5 MAY 2014

CIO ROLES AND RESPONSIBILITIES

According to reference (a), CIOs of Navy echelon 2 subordinate commands shall:

- Serve as the principal advisor to their commander for issues regarding IM and alignment of IT investments to business priorities and assigned missions.
- Oversee the effective use of information resources across their organizations to successfully meet the goals and objectives required for delivery of required capabilities.
- Support the alignment of business processes through implementation of enterprise architecture (EA) and IT planning procedures, and for the protection of mission critical and mission essential systems through strengthened cyber security management and technical controls in accordance with policy and guidance.
- Serve as, or team with, command competency leaders to ensure core IT workforce training, certification, education, and management requirements are identified and supported, and consistent with DON direction.
- Ensure that information resources are managed in an efficient and effective manner by developing and monitoring resource investments through a capital planning and investment control process.
- Provide the information required to develop and submit IT budget exhibits. Ensure that IT systems, for which funding is requested, are compliant with statutory, regulatory, and DoD business transformation requirements.
- Ensure that IT inventory information for all assets, including computer equipment, telecommunications, software licenses, and excess or surplus computer equipment, is current and provided to the appropriate DON Deputy CIO.

5 MAY 2014

- Align business processes through the implementation of EA. Implement and maintain required architecture products and associated standards. Ensure those architectures and standards are consistent with DON, DoD, and Federal architectures and direction.
- Enforce policy to secure information, information systems, and networks.
- Develop local policy in support of information resources management.
- Formally establish and maintain a reporting relationship with IA managers for all networks, systems, applications, and databases under their control.
- Ensure protection of personal data in accordance with DON Deputy CIO (Navy and Marine Corps) privacy guidance.
- Support the implementation of the use of electronic records management as directed by the appropriate DON Deputy CIO.
- Coordinate with and provide oversight to the appropriate DON service functional area manager in the evaluation of business and warfighting processes, review of functional applications, and functional area strategic plan objectives and related documentation.
- Align and fully integrate organizational IT strategy with the overarching DON IM and IT strategic plan.
- Carry out those duties required by the additional roles and responsibilities assigned to them by their commander.

5 MAY 2014

DEFINITIONS

Acquisition: The conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in or in support of military missions. (Reference (e))

Application: A software program designed to perform a specific function directly for the user or, in some cases, for another application. (Reference (b))

Capital Planning and Investment Control: A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes. (Reference (f))

Configuration Management: The technical and administrative direction and surveillance actions taken to identify and document the functional and physical characteristics of a configuration item (CI), to control changes to a CI and its characteristics, and to record and report change processing and implementation status. It provides a complete audit trail of decisions and design modifications. (Reference (e))

Contract Administration: All the activities associated with the performance of a contract from award to close-out. (Reference (e))

Database: A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that different programs can use them without concern for the data structure or organization. (Reference (b))

Data Management: A sub-set of IM dealing with the creation, use, sharing, and disposition of data as a resource critical to the effective and efficient operation of functional activities. It is the structuring of functional processes to produce and

5 MAY 2014

monitor the use of data within functional activities, information systems, and computing and communications infrastructures. (Reference (b))

Development: The process of working out and extending the theoretical, practical, and useful applications of a basic design, idea, or scientific discovery. Design, building, modification, or improvement of the prototype of a vehicle, engine, instrument, or the like as determined by the basic idea or concept. Includes all efforts directed toward programs being engineered for service use but which have not yet been approved for procurement or operation, and all efforts directed toward development engineering and test of systems, support programs, vehicles, and weapons that have been approved for production and service deployment. (Reference (e))

Enterprise Architecture (EA): The explicit description and documentation of the current and desired relationships among business and management processes and IT. It describes the "current architecture" and "target architecture" to include the rules and standards and systems life-cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life-cycle methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with Government Paperwork Elimination Act, end user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and IT, at an appropriate level of detail. (Reference (f))

Enterprise Information Environment (EIE): The common, integrated information computing and communications environment of the Global Information Grid (GIG). The EIE is composed of GIG assets that operate as, provide transport for and or assure local area networks, campus area networks, tactical operational and strategic networks, metropolitan area networks, and wide area networks. The EIE includes computing infrastructure for

5 MAY 2014

the automatic acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on DoD enterprise hardware, software operating systems, and hardware/software support that enable the GIG enterprise. The EIE also includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG. (Reference (g))

Information: Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (Reference (f))

Information Assurance: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Reference (h))

Information Management: The planning, budgeting, manipulating, and controlling of information throughout its life cycle. (Reference (c))

Information Resources: Information and related resources, such as personnel, equipment, funds, and information technology. (Reference (i))

Information Resources Management: The process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and IT. (Reference (c))

Information System: Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information, and includes computers and computer networks, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources. Notwithstanding the above, the term IT does

5 MAY 2014

not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term information system is used synonymously with IT (to include National Security Systems). (Reference (j))

Information Technology: With respect to an executive agency, any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment or of that equipment to a significant extent in the performance of a service or the furnishing of a product. Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a Federal contractor incidental to a Federal contract. (Reference (k))

Information Technology Workforce: Military (active and reserve) and Government civilian personnel who provide the workforce capabilities required to plan, budget, manipulate, control, and archive information throughout its life cycle; develop, acquire, implement, evaluate, maintain, and retire information, information systems, and IT, and the technology required to transmit information; develop the policies and procedures required to manage; and to apply the security measures, policies, and procedures that protect and defend information, information systems, and networks. (Abbreviated as IT, IM and IT, or IM/IT/IA). (Reference (a))

Knowledge Management: The integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance. (Reference (l))

Mission Critical Information System: A system that meets the definitions of information system and National Security System

5 MAY 2014

in the Clinger-Cohen Act, the loss of which would cause the stoppage of warfighter operations or direct mission support of warfighter operations. (Reference (m))

Mission Essential Information System: A system that meets the definition of information system in the Clinger-Cohen Act, that the acquiring component head or designee determines is basic and necessary for the accomplishment of the organizational mission. (Reference (m))

Network: A series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain sub-networks. In a network, a node is a connection point, either a redistribution point or an end point for data transmissions. In general, a node has programmed or engineered capability to recognize and process or forward transmissions to other nodes. The most common topology or general configurations of networks include the bus, star, token ring, and mesh topologies. Networks can also be characterized in terms of spatial distance as local, base, metropolitan, and wide area networks. (Reference (n))

Performance: Those operational and support characteristics of the system that allow it to effectively and efficiently perform its assigned mission over time. The support characteristics of the system include both supportability aspects of the design and the support elements necessary for system operation. (Reference (e))

Portfolio Management: The management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability. (Reference (g))

Procurement: Act of buying goods and services for the Government. (Reference (e))

Program Management: The process whereby a single leader exercises centralized authority and responsibility for planning, organizing, staffing, controlling, and leading the combined efforts of participating/assigned civilian and military personnel and organizations, for the management of a specific

5 MAY 2014

defense acquisition program or programs, throughout the system life cycle. (Reference (e))

Project: A planned undertaking having a finite beginning and ending, involving definition, development, production, and logistics support of a major weapon or weapon support system or systems. A project may be the whole or a part of a program. (Reference (o))

Quality Assurance: A planned and systematic pattern of all actions necessary to provide confidence that adequate technical requirements are established, that products and services conform to established technical requirements, and that satisfactory performance is achieved. (Reference (e))

Records Management: The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (Reference (p))

Risk Management (with regard to IT): The total process of identifying, controlling, and mitigating information system related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws. Reference (q))