

Department of the Interior Departmental Manual

Effective Date: 8/8/15

Series: Organization

Part 112: Policy, Management and Budget

Chapter 24: Office of the Chief Information Officer

Originating Office: Office of the Chief Information Officer

112 DM 24

24.1 Purpose. This Departmental Manual chapter describes the functions and organizational structure of the Office of the Chief Information Officer (OCIO). The OCIO's mission and primary objective are to establish and manage a comprehensive information resource management (IRM) program for the Department of the Interior (DOI).

A. The basic elements of the IRM program include policy, planning, execution, oversight, enterprise service design, development, and delivery. The Chief Information Officer (CIO) authorities are consistent with the Federal Information Technology Acquisition Reform Act (FITARA) and include planning, programming, budgeting, and execution across the departmental information technology (IT) portfolio. This includes defining and implementing governance, standards, guidelines, metrics, and processes for ensuring compliance, in addition to the ownership of enterprise data management, geospatial technology, and IT shared services.

B. In partnership with selected DOI bureaus, OCIO provides commodity IT shared services to the Department based on core capabilities. This enables better leveraging of existing resources and competencies across the Department, while eliminating duplication of efforts in this arena and driving internal efficiencies. The OCIO operates selected IT shared services for the Department and leads implementation and governance for shared services such as hosting, cybersecurity, and electronic records management.

24.2 Authority. The primary authorities for the mission and function of the OCIO include:

A. Federal Information Technology Acquisition Reform Act (FITARA); Title VIII Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, [PL 113-291].

B. Information Technology Management Reform Act (ITMRA) also known as the "Clinger-Cohen Act of 1996" [Public Law 104-106 Division E].

C. The Government Performance and Modernization Act of 2010 [31 USC 1101].

D. The Paperwork Reduction Act [44 USC 35 § 3501-3520].

- E. The Federal Records Act, as amended [44 USC].
- F. The Privacy Act of 1974, as amended [5 USC 552a].
- G. The Freedom of Information Act, as amended [PL 104-232, 5 USC 552].
- H. The Intelligence Reform and Terrorism Prevention Act [PL 108-458, 50 USC 401].
- I. Rehabilitation Act of 1973, as amended [PL 105-220, 29 USC 794d].
- J. Section 508 of the Rehabilitation Act of 1973 [29 USC 794d].
- K. The E-Government Act (E-GOV) of 2002 [PL 107-347, 44 USC 36].
- L. The Federal Information Security Management Act (FISMA) of 2014 [44 USC 101].
- M. The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," OMB Circular A-123, "Management's Responsibility for Internal Control," OMB Circular A-11, "Preparation, Submission and Execution of the Budget," M-09-02, "Information Technology Management Structure and Governance Framework," M-11-29, "Chief Information Officer Authorities," and M-12-10, "Implementing PortfolioStat," and M-13-13, "Open Data Policy-Managing Information as an Asset."
- N. The Office of Management and Budget (OMB) Circular A-16, "Coordination of Geographic Information and Related spatial Data Activities."

24.3 Responsibilities. The OCIO is responsible for the following functions:

- A. Oversees the governance, management, and delivery of mission and business IT programs within DOI.
- B. Establishes policies and procedures for providing investment management, risk management, information security, privacy, and systems development life-cycle management, Information Resource Management (IRM) policy compliance, including periodic review of artifacts and development products for IT investments and activities developed within or for DOI bureaus and offices.
 - (1) Reviews and approves the selection and planning of IT and IT-related investments and acquisitions by bureaus and offices, including development projects, and contracts or agreements for goods or services prior to the commitment of any purchasing action.
 - (2) Reviews the approval all IT acquisitions prior to award.
 - (3) Certifies that IT investments are adequately implementing incremental development as defined in OMB capital planning guidance.

C. Assesses the requirements established for agency personnel regarding knowledge and skill in IRM and the adequacy of those requirements for facilitating the achievement of the established IRM performance goals, and assesses the extent to which the positions and personnel at the executive and management levels meet those requirements.

(1) Participates in the recruitment, approval, and selection of bureau and office leadership with IT and IRM functions, such as bureau and office Assistant Directors of Information Resources (ADIRs) or other individuals designated as appropriate.

(2) Jointly establishes an agency-wide critical element (or elements) with the Chief Human Capital Officer (CHCO) to be included in all bureau and office ADIR performance evaluations.

(3) Jointly conducts with the CHCO a survey of all bureau and office ADIRs in order to publish a dataset identifying all bureau officials with the title or duties of ADIR.

(4) Jointly establishes with the CHCO a set of competency requirements for IT staff including IT leadership positions, and develops and maintains a current workforce planning process to ensure the agency can:

(a) Anticipate and respond to changing mission requirements;

(b) Maintain workforce skills in a rapidly developing IT environment;
and

(c) Recruit and retain the IT talent needed to accomplish the mission.

D. Engages in bureau and office strategic management activities to ensure proper and appropriate integration of IT in development, implementation, operation, and oversight of IRM activities. Collaborates and partners with the Business Integration Office, Office of Financial Management, Office of Budget, and Office of Acquisition and Property Management in this effort.

E. Participates in decision processes for all annual and multi-year planning, programming, budgeting, and execution decisions, including management, governance, and oversight of processes related to IT.

F. Takes appropriate action to protect the confidentiality, integrity, and availability of all data and digital assets in DOI. This includes directing removal of compromised systems from the DOI network until vulnerabilities are resolved and risks are managed.

G. Develops and monitors Departmental compliance with policies, reporting, procedures, and guidance in OMB Circular A-130. Acting as an ombudsman, the OCIO considers alleged instances of bureau and office failure to comply with OMB Circular A-130 and recommends appropriate corrective action, taking all appropriate action as needed to protect the information assets and security of DOI.

H. Facilitates the adoption and implementation of a coordinated and effective geospatial asset management capability that will improve the support of mission-critical business requirements within DOI.

I. Responds to requests from and collaborates with the Office of E-Government and Information Technology (E-Gov), within OMB on IT-related activities including cross-agency priority goals, and other quarterly reviews and assessments on the consolidation of duplicative systems, lowering operational costs, terminating and turning around troubled projects, and delivering meaningful functionality while enhancing the security of information systems.

24.4 Organization. The OCIO is headed by the CIO. The CIO reports to the Secretary and receives operational guidance and support from the Assistant Secretary – Policy, Management (PMB) through the Deputy Assistant – Technology, Information, and Business Services (DAS – TIBS).

A. The CIO provides vision and leadership in the development and implementation of DOI's IRM strategic plan and IT programs. The CIO leads the Department in planning and implementing enterprise information systems to support both distributed and centralized business operations and to achieve more effective and cost beneficial enterprise-wide IT operations. The OCIO is aligned to provide coverage, minimize redundancies, streamline information technology, and enhance customer service, while lowering DOI's IT costs. The OCIO leads the shared services strategy for common IT needs across DOI working in collaboration with bureaus and offices.

B. The CIO provides oversight and governance for DOI in planning and implementing enterprise information systems to support both distributed and centralized business operations, as well as achievement of effective enterprise-wide IT operations. The CIO carries out these functions with the assistance and collaboration of bureaus and offices and partnering with offices under the Assistant Secretary – Policy, Management and Budget.

C. The CIO is assisted by a Deputy CIO responsible for managing the OCIO's daily operations. The OCIO accomplishes its objectives through the following divisions.

(1) Information Assurance Division (IAD). The IAD reports directly to the CIO. The Division is headed by the Chief Information Security Officer (CISO) who is responsible for IT security policy and operations, privacy, risk management, and IT security operations. As a direct report to the CIO, a single point of accountability and visibility is provided in a critical area. The Federal Information Security Management Act (FISMA) reinforces the direct reporting relationship of the CISO to the CIO.

(2) Business Operations Division (BOD). The BOD is responsible for budget coordination with the Office of Budget including formulation, presentation, and execution. The Division coordinates with service providers for Human Resources, Acquisition, and Financial Management within the Interior Business Center. The Division also provides administrative

support services to the OCIO divisions and assists the CIO in developing IT policies and directives.

(3) Planning and Performance Management Division (PPMD). The PPMD is responsible for IRM strategic planning and execution, enterprise architecture, IT capital planning and investment control, portfolio management, IT project management, IRM community workforce planning, IT governance, policy, and management. In addition, PPMD oversees internal controls for IT systems, quality assurance, verification and validation, program assessment, audit liaison, and IT performance management, including the preparation of annual assurance statements.

(4) Information and Technology Management Division (ITMD). The ITMD is responsible for technology innovation, geospatial programs, enterprise data management, solutions architecture and design, information and records management, accessibility and shared service program development and management. This includes commodity IT service brokering and the management of the Departmental IT service catalog.

(5) IT Service Delivery Division (ITSDD). The ITSDD is responsible for Department-wide IT services including telecommunications, customer support, hosting and end user services. The Division manages the Department's telecommunications backbone and wide-area network, enterprise directory services, and is responsible for the Department-wide cloud-based email and collaboration system that supports over 70,000 end users. The Division also provides intra- and interagency shared services in these areas.

Office of the Chief Information Officer



