Department of the Interior

Departmental Manual

Effective Date: 01/19/2017
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 chapter describes the functions and organizational structure of the Office of the Chief Information Officer (OCIO).

24.2 **Mission**. The OCIO's mission and primary objective is to establish, manage, and oversee a comprehensive information resources management (IRM) program for the Department of the Interior (DOI). A stable, agile, and secure information management and technology (IMT) environment is critical for achieving the Department's mission.

24.3 **Authorities.** The primary authorities for the mission and function of the OCIO are provided in Appendix A.

24.4 **Definitions.** Definitions are provided in Appendix B.

24.5 **Responsibilities**.

A. Chief Information Officer. The Chief Information Officer (CIO) is responsible for oversight and management of all IMT from concept to disposition, including, without limitation, externally hosted, managed, or shared IT services and the delivery of managed or shared services for the use and benefit of the Department, its bureaus and offices and other authorized beneficiaries, or the equivalent thereof. This includes, but is not limited to:

(1) Overseeing the governance, management, and delivery of mission and business IT programs and systems within DOI. Conducting periodic reviews of IT systems, DOI products for IT investments and the operational IT environment. Supporting the DOI mission and program leaders in managing their IT investments through the complete systems lifecycle from inception to retirement, while avoiding unnecessary duplication.

(2) Establishing policies, processes, procedures and guidance for ensuring that DOI missions and programs follow required and sound management practices for IT projects and investments, information system security, privacy, IT development and operations and

employing risk management strategies with the CIO and other relevant stakeholders in IMT decision-making.

(3) Approving the selection, planning, and review of IT and IT-related investments by bureaus/offices, as well as development projects. Approving plans for IT acquisitions.

(4) Establishing appropriate policies, processes and procedures to initiate or terminate IT projects, systems, or investments in the best interest of DOI.

(5) Completing the annual Joint Certification Statement to certify budgetary resources within the DOI's IT portfolio, working in collaboration and coordination with DOI's Deputy Assistant Secretary for Budget, Finance, Performance and Acquisition (DAS-BFPA) and the DOI Director of Budget.

(6) Participating as a principal member of the DOI Acquisition and Procurement Advisory Council (APAC) to oversee significant IMT contracts, working in collaboration and coordination with the DAS-BFPA and the DOI Senior Procurement Executive (SPE).

(7) Certifying that IT investments are adequately implementing incremental (agile) development as defined in Office of Management and Budget capital planning guidance.

(8) Supporting the implementation of policy and guidance on standards and best practices for the management of information in collaboration with mission stakeholders.

(9) Establishing standard position descriptions and DOI-wide critical skill requirements for agency personnel supporting IMT functions across DOI to meet the performance needs of the organization, and ensuring that the positions and personnel at the executive and management levels meet those requirements.

(10) Approving all recruitment and reassignment actions for all IMT positions within DOI and with the best interest of DOI, including bureau/office Associate Chief Information Officers (ACIOs) or other designated positions. (Each bureau must have one full-time ACIO position reporting to the Deputy Director of the bureau and the CIO, unless otherwise agreed to in writing by the CIO.) The CIO approves the selection of all ACIOs and serves as the second line supervisor of the bureau ACIO, unless otherwise agreed to in writing by the CIO. There is one ACIO with responsibility for all offices in the Office of the Secretary.

(11) Jointly establishing a DOI-wide critical element (or elements) with the Deputy Assistant Secretary – Human Capital and Diversity (DAS-HCD) to be included in all bureau ACIO performance evaluations. The CIO works in partnership with the Deputy Bureau Directors to approve the ACIO's annual performance plan, provides input into progress reviews, and approves the final rating.

(12) Jointly conducting with the DAS-HCD a survey of all bureau/office ACIOs, or other titles holding similar responsibilities to publish and maintain a dataset identifying all bureau officials with the title or duties of an ACIO. The dataset includes explicit information on delegated authorities by the CIO.

(13) Jointly establishing with the DAS-HCD a set of competency requirements for IT staff including IT leadership positions, and developing and maintaining a current IT workforce planning process to ensure that DOI 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.

(14) Engaging in all bureau/office strategic management activities as they relate to IMT, including the development, implementation, oversight, and maintenance of DOI business analytics, operational, and alignment (or consolidation) plans through collaborative efforts supported by the Business Integration Office (BIO), the Office of Financial Management (PFM), and the Office of Acquisition and Property Management (PAM).

(15) Participating in the decision processes for all annual and multi-year planning, programming, budgeting, and execution decisions, including the management, governance and oversight of processes related to IMT. This includes participation in the Department's Working Capital Fund (WCF) Consortium as a voting member and providing recommendations directly to the Secretary and Deputy Secretary of the Interior for information technology mandatory issues and services. The CIO identifies and approves information technology requirements for all WCF services.

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

(17) Developing and monitoring Departmental compliance with the policies, reporting, procedures, and guidance in OMB Circular A-130. Acting as an IMT ombudsman, the CIO considers alleged instances of bureau/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.

(18) Facilitating 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.

(19) Responding to requests from and collaborating with the OMB Office of E-Government and Information Technology (E-Gov), also known as the Office of the Federal Chief Information Officer (OFCIO), 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 ensuring the security and privacy of IT systems and information.

(20) Leads the coordination and oversight of DOI compliance with the Paperwork Reduction Act. This includes ensuring the appropriate reviews for all DOI information collection requests and obtaining required DOI and OMB approvals for bureau and office information collection activities from the public and external entities.

B. OCIO. The OCIO issues and supports the implementation of policy and guidance on standards and best practices for the management of information in collaboration with mission stakeholders. This includes defining and implementing IRM governance, policies, standards, guidelines, metrics, and processes, IT shared services, and geospatial technology; and is responsible for implementing policies and best practices to drive consistency in DOI's IT environment and eliminate unnecessary duplication in IT systems where possible.

24.6 **Organization.** The OCIO is headed by the CIO. (See Organizational Chart in Appendix C) The CIO reports to the Secretary and receives operational guidance and support from the Assistant Secretary – Policy, Management and Budget (PMB) through the Deputy Assistant Secretary – Technology, Information, and Business Services (DAS-TIBS). The CIO provides vision and leadership in developing and implementing the DOI's IMT programs. The IT underpins DOI's ability to accomplish its mission and the services, activities, and programs provided to the American people. The CIO leads planning and implementation of DOI-wide information systems that support both distributed and centralized business operations, with a focus on achieving efficiencies and optimizing value to our missions through DOI-wide IT operations and shared services. The OCIO facilitates the implementation of a shared services strategy for common IT needs across the Department that can include qualified and interested bureaus as shared services providers. The OCIO includes executive functions such as customer relationships, management, communications, and the following:

A. Senior Associate CIO (SACIO) reports to the CIO and serves as the OCIO's primary liaison to bureau ACIOs for day-to-day interactions between bureau IMT staff and OCIO's major functions. The ACIO supports the CIO in IMT strategy development, facilitates fluid communications between the OCIO and bureaus, and plans and coordinates regular IMT governance meetings with bureau ACIOs and OCIO's core leadership team.

B. DOI Chief Information Security Officer (CISO) reports to the CIO and oversees the Information Assurance Division (IAD). The Division is responsible for IT security and privacy policy, planning, compliance and operations. The division provides a single point of accountability and visibility for cybersecurity, information privacy and security. The Federal Information Security Modernization Act (FISMA) reinforces the direct reporting relationship of the CISO to the CIO. Additionally, the CISO performs the following:

(1) Serves as the principal senior level executive technical advisor and consultant to the CIO regarding formulation and implementation of DOI-wide IA (IT Security and Privacy) policies, standards, procedures and guidance, as well as coordination of all aspects of the IA program that directly support DOI's risk management objectives.

(2) Provides executive leadership in IA policy and guidance; expert advice and consultancy to senior DOI officials; collaborates with bureaus/offices in support of mission/business risk management objectives; and represents DOI to internal and external oversight agencies, organizations, offices and the Congress on matters relating to protecting DOI's information assets.

(3) Facilitates coordination with bureau/office mission and business areas and other OCIO organizations, divisions and offices to help ensure information assurance policies, standards and guidelines are appropriately implemented throughout the agency and that responsible organizations are measuring and monitoring their effectiveness.

(4) Establishes appropriate IA (IT Security and Privacy) education, awareness and training for DOI-wide delivery to required employees and contractors through approved Learning Management System (LMS) service delivery provider(s) and coordinating with DOI's Office of Human Resources in support of their role and responsibility to enforce employees and managers compliance in completing annual mandatory agency training requirements.

(5) Coordinates implementation of the DOI's IT Risk Management Framework, Assessment and Authorization, and associated enterprise-wide continuous monitoring processes, procedures and programs by appropriate organizational elements across the agency to reduce the risk of vulnerabilities and weaknesses that could adversely impact the confidentiality, integrity or availability of sensitive agency information and information systems.

(6) Works with other cabinet level agencies and the senior executive level at those agencies and participates on government-wide advisory boards that draft policy recommendations for IA (IT Security and Privacy).

(7) Oversees DOI's Privacy Officer who approves the selection of all Associate Privacy Officers (APOs) and provides input into the APO's performance plans and evaluations.

(8) Performs management functions to ensure compliance with the requirements of the Federal Information Security Modernization Act (FISMA), including the following:

(a) Performs the CIO's responsibilities under section 3554 of FISMA and heads an office with the mission and resources necessary to ensure DOI compliance with section 3554 of FISMA.

(b) Develops and maintains a DOI-wide information security program as required by subsection (b) of section 3554 of FISMA.

(c) Develops and maintains information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 of FISMA, and section 11331 of title 40.

(d) Trains and oversees personnel with significant responsibilities for information security with respect to such responsibilities; and

(e) Assists senior DOI officials concerning their responsibilities under paragraph 3554 (a) (2) of FISMA, and ensures that:

(i) subordinate security plans are documented for DOI's information systems;

(ii) all of DOI's information systems are appropriately assessed and authorized to operate by the responsible Authorizing Official prior to allowing their use with any sensitive DOI information or within the production networking environment;

(iii) plans and procedures are in place to ensure recovery and continued operation of DOI's information systems in the event of a disruption; and

(iv) contractor systems meet the same security requirements and controls, as required by FISMA;

(9) Approves the selection of all bureau Associate Chief Information Security Officers and provides input into their performance plans and evaluations.

C. Deputy CIO. The Deputy CIO (DCIO) reports to the CIO and is responsible for the day-to-day operations of the OCIO. The DCIO oversees the following divisions, each headed by a Division Chief:

(1) Business Operations Division (BOD). Responsible for planning and executing the administrative functions of the OCIO, including budget formulation, budget execution, OCIO IT acquisitions planning and management, OCIO personnel management and oversight, as well as general office management and administration. The division coordinates its activities with other key service providers including the DOI Office of Budget and the Interior Business Center (IBC) for primary support in finance, acquisitions, and human resources. The division supports the CIO in ensuring that DOI IT policies and directives are communicated and distributed throughout DOI.

(2) Planning and Performance Management Division (PPMD). Responsible for IRM strategic planning, enterprise architecture, capital planning and investment control (CPIC), IT investment management and oversight, IT project management and IT workforce planning. The division leads DOI's IT investment and portfolio management program and supports the CIO with IT governance and policy. In addition, this division leads the OCIO's

oversight role for internal controls for IT systems, quality assurance, verification and validation, program assessment, audit liaison, and IT performance management.

(3) Information and Technology Management Division (ITMD). Responsible for technology innovation, and the design and development of new IT solutions in demand by DOI's missions and programs. The division houses the DOI's Chief Technology Officer (CTO) and Geospatial Information Officer (GIO) to drive the adoption of new technologies, while promoting standards, and facilitating DOI Geospatial programs. The division leads the DOI's information management and enterprise data management programs, including electronic records, document management, accessibility, solutions architecture and design, IMT vendor management and shared service program management. The division is responsible for DOI's data center optimization and cloud computing programs.

(4) IT Service Delivery Division (ITSDD). Provides services including customer support, telecommunications, hosting and end user services. The division manages DOI's telecommunications backbone and wide area network, enterprise directory services, and is responsible for the DOI-wide cloud-based email and collaboration system that supports over 70,000 end users. It is the inter-agency shared service provider for customer support and IT infrastructure for the IBC's over 300,000 external customers in the human resources, financial management and acquisition lines of business.

D. Information Management and Technology Leadership Team. The Information Management and Technology Leadership Team (IMTLT) is a central component of DOI's IMT governance structure. The IMTLT leads DOI's IMT vision and provides strategic direction. The CIO leads the team comprised of all division heads in the Office of the CIO and the bureau and Office of the Secretary ACIOs who have a direct line of performance accountability to the CIO.

Appendix A

Authorities

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 Federal Information Security Modernization Act (FISMA) of 2014 [44 USC 101].

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

E. The E-Government Act (E-GOV) of 2002 [PL 107-347, 44 USC 36].

F. The Privacy Act of 1974, as amended [5 USC 552a].

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

H. The Federal Records Act, as amended [44 USC].

I. The Freedom of Information Act, as amended [PL 104-232, 5 USC 552].

J. The Intelligence Reform and Terrorism Prevention Act [PL 108–458, 50 USC 401].

K. Section 508 of the Rehabilitation Act of 1973, as amended [PL 105-220, 29 U.S.C. 794d].

L. The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," and Circular A-16, "Coordination of Geographic Information and Related Spatial Data Activities."

M. The Office of Management and Budget (OMB) Memorandum 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," and M-15-14, "Management and Oversight of Federal Information Technology."

Appendix B

Definitions

A. Enterprise-Level Contract. The term Enterprise-Level Contract includes any procurement contract that can be used by and/or affects more than one bureau, including both optional and mandatory use contracts. It includes, but is not limited to contracts where bureaus place their own orders, contracts where all orders are placed by a single acquisition office, and contracts where no orders are placed but the contract benefits multiple bureaus, regardless of contract type.

B. Information Management. The collection and management of information from one or more sources and distribution of that information to one or more audiences. This may involve persons who have a stake in, or a right to that information. Management means the organization of and control over information activities, planning, structure, organization, controlling, processing, evaluating, and reporting in order to meet mission objectives and to enable organizations to function in the delivery of information.

C. Information Technology (IT). The IT includes, but is not limited to any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where such services or equipment are “used by an agency” if used by the agency directly, or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product. The term "information technology" 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 provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment. This definition is based on the definition of IT in the Clinger-Cohen Act of 1996.

D. Information Technology Resources. The IT Resources includes all agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of IT, acquisitions or interagency agreements that include IT and the services or equipment provided by such acquisitions or interagency agreements. IT resources do not include grants to third parties, cooperative agreements, or Public Law 93-638 contracts, which establish or support IT not operated directly by the Federal Government.

E. Information Management and Technology (IMT). The IMT includes the collective definitions articulated in B, C, and D above.

Appendix C

Department of the Interior

Office of the Chief Information Officer