

Department of the Interior
Departmental Manual

Effective Date: 01/19/2017

Series: Delegation

Part 212: Policy, Management and Budget

Chapter 24: Chief Information Officer

Originating Office: Office of the Chief Information Officer

212 DM 24

24.1 General. This chapter provides the delegation of authority for the Department's Chief Information Officer (CIO). The title and designation "CIO" is given to only one individual within the Department of the Interior (DOI).

24.2 Authority Delegated to the Chief Information Officer (CIO). Authority is delegated to the CIO to carry out the functions of the position as required by all applicable laws, regulations, and policies. This authority includes the following:

A. Authority to carry out and exercise the program and management functions described in 112 DM 24, 375 DM 1, and the administrative authorities delegated in 212 DM 1 subject to the limitations described therein.

B. Authority to implement and verify compliance with requirements of the 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)], the Clinger-Cohen Act of 1996, the Federal Information Security Modernization Act (FISMA), the Privacy Act, and all other applicable information management and technology (IMT) laws, regulations, and policies. This authority includes:

(1) Providing oversight and management of Information Management and Technology (IMT) resources (as that term is defined in 112 DM 24) infrastructure and service delivery. This includes oversight and management of all IMT 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 further includes all IT infrastructure, telecommunications and radio assets, as well as services and systems necessary to sustain the geospatial activities of the Department.

(2) Issuing and supporting the implementation of policy and guidance on standards and best practices for managing information in collaboration with mission stakeholders.

01/19/2017 #4075

Replaces 07/23/2001 #3372

(3) Carrying out the provisions of the Office of Management Budget (OMB) Circular A-130, "Management of Federal Information Resources," OMB Circular A-11, Memorandum M-09-02, "Information Technology Management Structure and Governance Framework", M-11-29, "Chief Information Officer Authorities," M-12-10, "Implementing PortfolioStat," and M-13-13, "Open Data Policy-Managing Information as an Asset" which designates responsibility and accountability to the agency CIO within each Federal agency to effectively manage all IT resources, and M-15-14, "Management and Oversight of Federal Information Technology", and other federal policies, regulations and guidelines pertaining to information management and technology for Executive Branch agencies.

(4) Performing the responsibilities of the Senior Agency Official for Privacy under the provisions of the Privacy Act of 1974, 5 U.S.C. 552a, Section 208 of the E-Government Act of 2002, OMB circulars, and related privacy laws, regulations, and policies. As the Senior Agency Official for Privacy, the CIO has authority and oversight of DOI-wide privacy compliance activities including formulation, promulgation and implementation of privacy policies, procedures, and training; management and administrative functions described in DOI Privacy Act regulations at 43 CFR part 2, Subpart K, and 383 DM 1-13, including budget, staffing, reporting and other program functions; establishing privacy requirements in the risk management framework and ensuring privacy reporting requirements are met in accordance with Federal laws and policies; and serving as the senior official for privacy and civil liberties matters related to the Department's law enforcement and information sharing environment activities.

(5) Carrying out the provisions of the Federal Records Act as amended [44 USC] and OMB Memorandum M-12-18, "Managing Government Records Directive". This includes the authority to develop and implement Federal Records Act policies and procedures. The CIO is DOI's Senior Agency Official for Records.

(6) Approving recruitment and reassignment actions for all IMT positions within the Department. Approving the selection of all bureau Associate Chief Information Officers (ACIO). In consultation with the Deputy Assistant Secretary – Human Capital and Diversity, establishing a baseline position description for all ACIOs and Department-wide critical elements for the ACIO position (Senior Level or GS-15 positions; or agency-specific performance requirements for Senior Executive Service positions). In partnership with bureau Deputy Directors, providing input and approving bureau ACIO annual performance plans, providing input into progress and final performance appraisals, and approving final performance ratings.

(7) Serving as the final authority in managing DOI's IMT portfolio and establishing appropriate policies and procedures to initiate or terminate any IMT project as the CIO deems necessary and in the best interest of DOI. The CIO has a significant role in planning, programming, budget formulation, and execution decisions for IMT across the Department.

(8) Annually certifying DOI's IMT portfolio and approving the budget request for all IMT spending across DOI. (The CIO and the Director, Office of Budget, must complete an annual Joint Certification Statement to certify the Department's IT portfolio based on the recommendations of bureau ACIOs and budget officers.)

(9) Overseeing all IMT acquisitions. (The CIO and the Senior Procurement Executive develop and implement policies and procedures as necessary to ensure that the CIO has full visibility into the Department's IMT purchases, including enterprise-level contracts.)

(10) Carrying out the provisions of the OMB Circular A-16, "Coordination of Geographic Information and Related spatial Data Activities."

(11) Carrying out the provisions of the Intelligence Reform and Terrorism Prevention Act [PL 108-458, 50 USC 401].

(12) Carrying out the duties of DOI's Chief FOIA Officer as required under the provisions of the Freedom of Information Act (FOIA), as amended, 5 U.S.C. 552 (k).

(13) Issuing DOI-wide policy and guidance affecting IT management programs.

(14) Overseeing, coordinating, and reviewing IT security and privacy components of emergency management budgets for bureaus/offices in coordination and collaboration with the Office of Emergency Management.

(15) Coordinating, evaluating, and implementing DOI's response to Homeland Security Presidential Directives and other law enforcement, homeland security, and emergency mandates and Executive Orders as they relate to IMT.

(16) 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/office information collection activities from the public and external entities.

(17) Making decisions about all DOI IT resources when a determination is made by a properly authorized official that a national emergency or incident impacting more than one bureau, a non-DOI customer, or partner organization, is occurring or about to occur. Report incidents designated as "major" to Congress within seven (7) days. (A national emergency is defined as a situation that could result in, or has resulted in, a Presidential Declaration of a National Emergency. An incident is defined as an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The OMB provides agencies with the definition and framework for assessing whether an incident is "major".)

24.3 Authority Delegated to the Chief Information Security Officer (CISO). Authority is delegated to the CISO to carry out Information Assurance (IA) functions and programs in DOI (includes all bureaus/offices) in accordance with section 3554(a)(3)(A) of the Federal Information Security Modernization Act of 2014 (FISMA). This authority includes the design,

architecture, development, engineering, implementation, management, operations and maintenance of IA functions and programs and associated resources (i.e., budgetary and staffing), all of which are under the purview (i.e., range of operation, authority, control, concern, vision, insight, understanding, and responsibility) of the CISO. All of the authority of the CISO may be redelegated.

24.2 Limitations. All authorities delegated in this chapter are subject to the limitations contained in 200 DM 1.

24.3 Authority to Redelegate.

A. Except where re-delegation is prohibited by statute, Executive Order, or limitations established by other competent authority, the authorities delegated in this Chapter may be redelegated. All redelegations of authority must be made in writing by the CIO.

B. Consistent with FITARA, the CIO may delegate allowable authorities over IMT in writing to individuals within the Department, provided that those individuals have direct performance accountability to the CIO.

(1) The CIO may withdraw delegations as deemed necessary.

(2) The CIO may not delegate the responsibility to approve all major IMT investments or to approve the selection of Associate Chief Information Officers (ACIO).

C. The ACIO may delegate aspects of her/his authority over IMT in writing to individuals within the bureau, provided the individuals have adequate lines of accountability to the ACIO.