



THE SECRETARY OF THE INTERIOR
WASHINGTON

ORDER NO. 3340

Subject: Strengthening and Securing Information Management and Technology at the
Department of the Interior

Sec. 1 Purpose. The Department of the Interior's (Department) mission covers a broad range of activities, including land and water conservation, responsible use and development of our Nation's natural resources, upholding trust and treaty obligations to American Indians and Alaska Natives, and furthering the understanding of natural systems through science. Information Technology (IT) is essential to the Department's ability to accomplish its diverse mission and the services, activities, and programs that it provides to the American people. Bureaus and offices use IT to achieve their missions, facilitate efficient, effective work by employees, and provide a wide range of services to the public. Department employees depend on IT tools to carry out their everyday work, and these tools continue to evolve rapidly.

The Department's mission-critical IT systems continue to age, presenting challenges to the adoption of modern, innovative approaches to doing business. Outdated IT systems increase security risks and vulnerabilities in an environment where threats to Federal IT systems are more significant every year. Safeguarding the Department's IT systems is essential to reliably carrying out mission-essential functions of the United States Government and to delivering uninterrupted services to the public. This Secretarial Order sets forth improved functions, authorities, policies, and strategies for securing the Department's IT and for making investments to maximize benefits and avoid unnecessary or duplicative IT spending. This Order directs the necessary management changes in IT to establish strong accountability for IT across the Department and to comply with requirements under the Federal Information Technology Acquisition Reform Act (FITARA) of 2014 and the Federal Information Security Modernization Act (FISMA) of 2014.

Sec. 2 Background. In an effort to eliminate duplicative and wasteful spending, over the past 20 years, Congress passed several laws, and the Office of Management and Budget (OMB) issued associated policies to direct how the Government manages its IT resources. Congress enacted the Clinger-Cohen Act in February 1996 to improve the way Federal agencies acquire and manage information and related resources, such as personnel, equipment, funds, and IT. The law required each agency head to establish clear accountability for IT management activities by appointing an agency Chief Information Officer (CIO) with the visibility and management responsibilities needed to carry out the provisions of the Act. The CIO plays a critical leadership role in driving reforms to help control system development risks, better manage IT spending, and achieve measurable improvements in agency performance. The Clinger-Cohen Act assigns the Director of OMB responsibility for improving the acquisition, use, retirement, and disposal of IT assets by the Federal Government to improve the productivity, efficiency, and effectiveness of Federal programs. This includes the dissemination of public information and the reduction of

information collection burdens on the public. Following the enactment of the Clinger-Cohen Act, the OMB issued a series of memoranda and, ultimately, OMB Circular (A-130) about the management of Federal Information Resources. In 2002, Congress passed the E-Government Act of 2002 that reiterated the CIO's responsibilities for agency IT management and information security at their respective agencies.

In December 2014, Congress enacted FITARA. The FITARA imposes new legal requirements that enhance Department-level CIO authorities across a broad scope of IT-related activities, including: (1) planning, programming, budget formulation, and execution; (2) management, governance, and oversight processes related to IT; (3) contracts or agreements for IT or IT services; (4) decisionmaking for major IT investments; and, (5) appointment of any bureau/office CIO or equivalent. In June 2015, OMB provided implementation guidance for FITARA and related IT management practices (OMB Circular M-15-14).

The Department spends over \$1 billion annually on IT investments with more than 85 percent devoted to steady state systems, many of which are antiquated and in need of modernization. In a 2008 Office of Inspector General (OIG) report entitled, "Compilation of Information Technology Challenges at DOI – A Blueprint for Change," the OIG asserted: "The Department's management of IT is ineffective, costly, wasteful and lacks accountability." This report and more recent OIG reports from 2015 cite IT security vulnerabilities in the Department's IT systems that expose the Department to infiltration by unauthorized entities. Recent cybersecurity incidents and reports from the OIG on IT security vulnerabilities prompted the Department to thoroughly review how the Department and its bureaus manage and operate IT systems and undertake remediation where needed.

Decentralized management of IT resources presents serious challenges, including inefficient and duplicative IT spending, poor interoperability and integration among mission IT systems, and limited visibility and understanding of the full IT environment at the Department and bureau levels; this presents significant cybersecurity risks. The Department's Office of the Chief Information Officer (OCIO) provides leadership, oversight, and policy guidance for the Department's bureaus and offices in all areas of information resource management. The OCIO also operates many Department-wide IT systems, such as the email system, and supports the Department's delivery of shared services for other Federal agencies, such as payroll. Bureaus are responsible for their respective mission systems and underlying IT infrastructure; for most of the Department's largest bureaus, IT is further decentralized to program managers in the field with limited, if any, central authority or accountability within the bureau. The Department's implementation of FITARA will rectify these challenges by establishing new, formal lines of authority and accountability for IT and information resources management between the CIO and bureau IT leaders, and by requiring bureaus to centralize accountability under a single IT leader.

The Department's FITARA Implementation Plan (Implementation Plan), which meets the requirements of OMB Circular M-15-14, describes how the Department intends to meet OMB's common baseline for FITARA implementation across the Executive Branch. One of the most fundamental strategies of the Implementation Plan is to consolidate authority for information management and technology (IMT) within the bureaus under a single position that has a direct

reporting line to the CIO. Notwithstanding improvements made in recent years to IMT functions, most of the Department's bureaus lack a central authority for this, creating a duplicative, highly-distributive, costly, and risky IT environment for the Department at large. Under this Order, bureau heads will implement policies and procedures as necessary to ensure that their top-level IT leader has full visibility, accountability, and control over IMT within the bureau. Each bureau must prepare a plan that describes how they will achieve this; the CIO must formally approve each bureau plan. The top-level IT leader for the bureau would remain an employee of the bureau, but would have a dual reporting line to the CIO and a senior career bureau leader, generally the Deputy Bureau Director. Overall, the Implementation Plan outlines key actions that the Department will undertake to meet OMB's FITARA common baseline requirements in governance, budget formulation and execution, acquisition, organization, and workforce. This Order ensures implementation of that Plan.

Sec. 3 Authorities. This Order is issued in accordance with the authority of FITARA, OMB Memorandum M-15-14, the Clinger-Cohen Act of 1996, OMB Circular A-130, FISMA, the Privacy Act, E-Government Act, Paperwork Reduction Act, and OMB Memorandum M-09-02.

Sec. 4 Definitions.

- a. Bureau. A major organizational unit carrying out specific operating programs, and, as necessary, maintaining field operating units. Such organizational units may have one of the following designations: bureau, office, service, administration, or other designations established by law.
- b. Department and Departmental. The Department of the Interior in general or as a whole. These designations may be used to refer only to the entire Department.
- c. 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.
- d. Information Management. The term Information Management refers to 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.
- e. Information Technology. 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.

f. Information Technology Resources. 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.

g. Information Management and Technology. IMT includes the collective definitions articulated in d, e, and f above.

h. Secretarial Offices. Offices reporting to the Secretary, Deputy Secretary, Solicitor, Inspector General, or an Assistant Secretary.

i. Subordinate Organization. Refers to organizational components of any size within a headquarters or field office (state, region, field office, science centers).

Sec. 5 Policy. It is a critical priority of the Department and its bureaus and offices to strengthen IT management by safeguarding mission IT; strengthen the acquisition and management of IT investment to eliminate duplication and waste; and, provide strong oversight of IT assets.

a. Accountability for Department-wide IMT.

(i) The Department will have only one individual with the title and designation “Chief Information Officer” (CIO). Any person with the title “Deputy Chief Information Officer” (DCIO) must work in the OCIO and report directly to the CIO. No bureau or subordinate organization may designate a person with the title “Chief Information Officer” or “Deputy Chief Information Officer.”

(ii) The CIO reports to the Secretary and receives administrative support from the Assistant Secretary - Policy, Management and Budget, through the Deputy Assistant Secretary - Technology, Information, and Business Services (DAS - TIBS). The CIO also

receives management guidance from the Deputy Secretary who serves as the Department's Chief Operating Officer.

(iii) The CIO is responsible for the 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 other authorized beneficiaries or the equivalent thereof.

(iv) Consistent with FITARA, the CIO may delegate aspects of her/his authority over IMT in writing to individuals within the Department, provided that those individuals have adequate lines of accountability to the CIO.

(v) The CIO approves all recruitment and reassignment actions for all IMT positions within the Department. The CIO may delegate this authority to individuals who have adequate lines of accountability to the CIO.

(vi) The CIO is the final authority in managing the Department's IT portfolio. The CIO establishes appropriate policies and procedures to initiate or terminate any IT project as the CIO deems necessary and in the best interest of the Department.

(vii) The Department will have only one individual with the title and designation "Chief Information Security Officer" (CISO) and one individual with the title "Privacy Officer." No bureau or subordinate organization may designate any other person with the title "Chief Information Security Officer" or "Privacy Officer." The CISO and Privacy Officer report to the CIO.

b. Accountability between the CIO and Bureaus.

(i) Each bureau will have one full-time Associate Chief Information Officer (ACIO) position reporting to the Deputy Director of the bureau and the CIO, unless otherwise authorized in writing by the CIO. The ACIO may also hold the title of Director of Information Resources Management for the bureau. The CIO will approve the selection of all ACIOs. [The ACIO position replaces all existing positions currently titled "Assistant Director for Information Resources (ADIRs)"]. There will be one ACIO with responsibility for all Secretarial Offices. (The Secretarial Offices are not authorized to establish an ACIO position, unless otherwise authorized in writing by the CIO.)

(ii) The CIO, in consultation with the Deputy Assistant Secretary - Human Capital and Diversity (DAS - HC&D), will establish a position description as a baseline 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). The CIO will approve the ACIO's annual performance plan, provide input into progress reviews, and approve the final rating.

(iii) Each bureau will have one Associate Chief Information Security Officer (ACISO) position and one Associate Privacy Officer (APO) reporting to the bureau ACIO,

unless otherwise authorized in writing by the CIO. The Secretarial Offices are not authorized to establish an ACISO or APO position, unless otherwise authorized in writing by the CIO. The Department's CISO will approve the selection of all ACISOs, and the Department Privacy Officer will approve the selection of all APOs.

(iv) The CIO, in consultation with the DAS - HCD, will establish a position description as a baseline for all ACISOs and APOs and Department-wide critical elements for the ACISO and APO positions. The CISO will approve the ACISO's annual performance plan, and the Privacy Officer will approve the APO's annual performance plan. The CISO/Privacy Officer will provide input into progress reviews and will approve the final rating.

c. Accountability for IMT within Bureaus.

(i) The ACIO is responsible for oversight and management of all IMT in her/his bureau. The ACIO may delegate aspects of her/his authority over IMT in writing to individuals within the bureau, provided that those individuals have adequate lines of accountability to the ACIO.

(ii) Bureau heads will implement policies and procedures as necessary to ensure that the ACIO has full visibility, accountability, and control over IMT within the bureau. Bureau heads will submit a plan to the CIO that is consistent with the Implementation Plan, which describes the specific, planned actions for achieving this outcome.

d. Planning and Budgeting for IMT.

(i) The CIO has a significant role in planning, programming, budget formulation, and execution decisions for IMT across the Department. The CIO and the Deputy Assistant Secretary - Budget, Finance, Performance and Acquisition (DAS - BFPA) will develop policies and procedures, as necessary, to implement the CIO's role in the planning and budget processes.

(ii) The CIO and the DAS - BFPA will complete an annual Joint Certification Statement to certify the Department's IT portfolio based on the recommendations of bureau ACIOs and budget officers. This certification will ensure that the CIO reviews and approves the budget request for all IMT spending across the Department.

(iii) Each bureau ACIO will participate in the planning, programming, budget formulation, and execution decisions for IMT within their organization, including all subordinate organizations. Bureau heads will issue policies and procedures, as necessary, to implement the ACIO's role in the planning and budget processes. Bureau policies and procedures shall be consistent with the Implementation Plan.

e. Optimizing IMT Acquisitions.

(i) The CIO and the Senior Procurement Executive will 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. These policies and procedures will be consistent with the Implementation Plan.

Sec. 7 Delegation of Authority. Authority is delegated to the CIO to implement and verify compliance with requirements of FITARA, the Clinger-Cohen Act, FISMA, other applicable Federal IMT laws and policies, and this Order.

Sec. 8 Implementation Responsibilities.

a. CIO. The CIO and the Assistant Secretary - Policy, Management and Budget (AS - PMB) are responsible for implementing the requirements of this Order.


b. FITARA Implementation Team (FIT). The FIT is comprised of the CIO; Chief of Staff to the AS - PMB; DAS - BFPA; DAS - HCD; DAS - TIBS; and the Deputy Solicitor - General Law. The CIO and the FIT will collaborate throughout implementation with the appropriate stakeholders.

c. Heads of Bureaus.

(i) Heads of bureaus are responsible for ensuring full implementation of this Order within their respective bureau.

(ii) Bureaus must revise their Departmental Manual functional descriptions to reflect the requirements in this Order with concurrence of the CIO no later than 90 days after the date of this Order.

Sec. 9 Expiration Date. This Order is effective immediately. It will remain in effect until its provisions are converted to the Departmental Manual, or until it is amended, superseded, or revoked, whichever occurs first. Upon completion of the foregoing, the provisions of this Order will terminate.


Secretary of the Interior

Date:

AUG 15 2016