

GENERAL SERVICES ADMINISTRATION  
Washington, DC 20405

CIO 2101.2  
September 3, 2019

**GSA ORDER**

**SUBJECT: GSA Enterprise Information Technology Management (ITM) Policy**

**1. Purpose.**

a. In accordance with the Federal Information Technology Acquisition Reform Act (FITARA), Pub. L. No. 113-291, this Order outlines the authorities, responsibilities, and policies for management of all General Services Administration (GSA) Information Technology (IT) solutions, resources, and shared services.

b. IT will be managed in accordance with all statutory, regulatory, Office of Management and Budget (OMB), and agency requirements, including but not limited to FITARA. This Information Technology Management (ITM) Policy, along with associated processes, will be administered by the GSA Chief Information Officer (CIO) with support from applicable Services and Staff Offices (SSOs).

**2. Cancellation.** This Order cancels and supersedes CIO 2101.1, GSA Enterprise Information Technology Management (ITM) Policy, dated July 14, 2017; CIO 2102.1, Information Technology (IT) Integration Policy, dated March 9, 2015; and CIO-IL-16-02, Information Technology Shared Services Agreements, dated September 7, 2018.

**3. Revisions.** The following changes have been made to the Order.

a. Applicability and scope have been clarified.

b. Responsibilities have been revised to add governance, interagency-agreements (IAAs), and contract approval responsibilities for the CIO.

c. References have been updated.

d. Appendix A has been updated and renamed to add specific CIO roles.

e. Appendices B and C have been added to provide IT-specific definitions and policy guidance for submitting IT shared services agreements to the CIO for review.

#### 4. Background.

a. In accordance with FITARA, the CIO is required to perform a significant role in agency IT decisions: including annual and multi-year planning, programming, budgeting, execution, reporting, management, governance, and oversight functions. (See [Appendix A](#) for detailed responsibilities from FITARA and other authorities).

b. To establish consistent agency interpretation for the scope of the covered areas, this policy uses the definitions of "information technology" and other terms from [OMB M-15-14](#), Management and Oversight of Federal Information Technology. (See [Appendix B](#) for IT definitions).

#### 5. Applicability.

a. This policy applies to:

(1) All GSA SSOs, including Regional Offices, and all GSA Federal employees and contractors.

(2) The Office of Inspector General (OIG) to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act, and it does not conflict with other OIG policies or the OIG mission;

(3) The Civilian Board of Contract Appeals (CBCA) to the extent that the CBCA determines it is consistent with the CBCA's independent authority under the Contract Disputes Act, and it does not conflict with other CBCA policies or the CBCA mission.

b. This policy applies to all IT resources, solutions, and/or services, and all activities pertaining to IT acquisition planning; IT budget formulation and execution; IT personnel resourcing and workforce development; IT development and enhancement activities; and operation and disposal of IT resources of any size where GSA is responsible for managing, hosting, and/or funding the work. (See [Appendix B](#) for definitions and examples of "IT resources, solutions, and/or services").

#### 6. Responsibilities.

a. The CIO is responsible for:

(1) Promulgating policy addressing IT leadership and accountability, IT strategic planning, IT workforce, IT budgeting, investment management, and information security;

(2) Designating GSA IT officials to serve as liaisons between the GSA lines of business and GSA IT in order to facilitate interactions such as reviewing incoming requests, advising on IT strategies, conducting IT portfolio or budget reviews, conducting project/program reviews, and other IT functions;

(3) Overseeing and managing internal delivery and performance management of IT initiatives, to include but not limited to, IT commodities, IT services, internet or

network-based solutions, telecommunications, and business or core mission systems;

(4) Participating in governance and management processes to review and concur on IT strategies and budgets managed across GSA; and

(5) Reviewing and approving contracts or other agreements for IT resources, IT services, or spending by GSA SSOs, in conjunction with applicable procurement groups, the Chief Acquisition Officer (CAO) and the Chief Financial Officer (CFO). (See [Appendix C](#) for further information on IT shared services agreements).

b. CIO approval must be obtained before entering into any contracts or other agreements for all major IT investments. This approval **cannot** be delegated. Approval for non-major IT investments, as defined in OMB's annual IT capital planning guidance, may be delegated to the Deputy CIO (See [ADM 5450.39D, GSA Delegations of Authority Manual](#)). Non-major IT investments are those that do not require special management attention because of their importance to the mission or function to the Government; high executive visibility; high development, operating or maintenance costs; or unusual funding mechanisms (OMB M-15-14). GSA's Capital Planning and Investment Control ([CPIC](#)) guide has additional GSA-specific guidance.

c. All SSOs are responsible for:

(1) Ensuring appropriate business planning and management of business requirements to guarantee transparency, accountability, and coordination with the CIO, and/or appointed delegate(s), throughout the IT lifecycle;

(2) Collaborating with the CIO, and/or appointed delegate(s), regarding organizational plans or changes that have an impact on the delivery of IT systems or solutions for IT initiatives that are managed outside of GSA IT; and

(3) Implementing standardized processes to ensure that:

(a) Before entering into any contract or other agreement for IT or IT services, the contract or agreement has undergone the required CIO review and obtained the required approval. (See ADM 5450.39D, GSA Delegations of Authority Manual).

(b) Before requesting the allocation or reprogramming of any funds made available for IT programs, systems, solutions, resources, and/or shared services, the request has undergone the required CIO review and obtained the required approval. (See ADM 5450.39D, GSA Delegations of Authority Manual).

7. Policy. This policy ensures compliance with FITARA and other regulations for all planned or existing IT systems, solutions, resources, and shared services, regardless of budget source, size, complexity or significance, in all of its acquisitions or solutions life-cycle phases.

8. References.

- a. [Federal Information Technology Acquisition Reform Act \(FITARA\)](#), Pub. L. 113-291
- b. [Clinger-Cohen Act of 1996](#), (formerly called the Information Technology Management Reform Act of 1996), codified at 40 U.S.C. § 11101, *et seq*
- c. [Federal Information Security Modernization Act \(FISMA\) of 2014](#), Pub. L. 113-283
- d. [GAO-04-394G](#), Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity
- e. [GAO-18-93](#), Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities
- f. [OMB Circular A-11](#), Preparation, Submission, and Execution of the Budget
- g. [OMB Circular A-123](#), Management's Responsibility for Internal Control
- h. [OMB Circular A-130](#), Managing Information as a Strategic Resource
- i. [OMB M-19-03](#), Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program
- j. [OMB M-19-16](#), Centralized Mission Support Capabilities for the Federal Government
- k. [OMB M-19-18](#), Federal Data Strategy - A Framework for Consistency
- l. [OMB M-15-14](#), Management and Oversight of Federal Information Technology
- m. [ADM 5450.39D](#), GSA Delegations of Authority Manual
- n. [Executive Order 13833](#), Enhancing Effectiveness of Agency Chief Information Officers
- o. [Executive Order 13873](#), Securing the Information and Communications Technology and Services Supply Chain

9. Signature.

e-Signed by David Shive  
on 2019-09-03

---

DAVID SHIVE  
Chief Information Officer  
Office of GSA IT