CHIEF INFORMATION OFFICERS COUNCIL

HANDBOOK

CIO Handbook

Table of Contents

Executive Summary

As a business executive, the Chief Information Officer (CIO) challenges executive leadership to think strategically about digital disruptions that are forcing business models to change and technology's role in mission delivery. As a technology leader, the CIO enables and rapidly scales the agency's digital business ecosystem while concurrently ensuring digital security. The CIO drives transformation, manages innovation, develops talent, enables the use of data, and takes advantage of evolving technologies.

The Federal Chief Information Officers Handbook is provided for newly designated CIOs, Deputy CIOs, agency heads and other senior leaders during transition to both understand the role of the CIO and the CIO Council.

This handbook aims to give CIOs important information needed to be a technology leader at their respective agency. It is designed to be useful both to an executive with no Federal Government experience and to a seasoned Federal employee familiar with the nuances of the public sector. At its core, the handbook is a collection of resources that illuminate the many facets of the Federal IT landscape and the related issues and opportunities of Federal management.

Document Objectives:

- Educate and inform new and existing CIOs about their roles and responsibilities.
- Highlight laws, policies, tools, and initiatives that can assist CIOs and their staff as they develop or improve their organization's IT portfolio.
- Streamline agency processes and improve reporting to oversight entities.
- Enable improved decision-making by leading and facilitating communication and collaboration within agencies and government wide.

The handbook:

1. Reviews the statutory responsibilities that define the CIO's mandate in eight responsibility areas, the corresponding Laws and Executive Orders, and any applicable implementation guidance issued by the Office of Management and Budget (OMB) and other government-wide organizations;
2. Describes, in detail, the applicable laws relevant to the CIO's role, other authorities, key stakeholders that CIOs should meet in their first month, and key organizations and their role in Federal IT;
3. Outlines government-wide IT policies and initiatives, summarizes the many kinds of reporting activities the CIO must conduct to keep their agency accountable to government-wide authorities, and provides a reporting calendar with the most up-to-date reporting activities available.

The handbook concludes with a list of additional Federal IT resources and where to find them.

As a whole, this handbook is meant to provide CIOs with a foundational understanding of their role. The tools, initiatives, policies, and links to more detailed information make the handbook an effective reference document regardless of the reader's familiarity with Federal IT.

CIO Role at a Glance

The CIO's role at their agency is to enable the organization's mission through the effective use of information resources and information technology. As technology has become increasingly entwined with the daily functions of the Federal Government, the CIO's role has been expanded through several key acts of Congress.

The Clinger Cohen Act of 1996[1] was the first time that federal agency CIO positions were established with designated roles and responsibilities. Clinger Cohen directs federal agencies to focus more on the results achieved through IT investments and streamlined the Federal IT procurement process, detailing how agencies approach the selection and management of IT projects.

The role of the CIO expanded further under the Federal IT Acquisition Reform Act (FITARA),[2] which established the agency CIO as a key strategic partner to the agency head and enabler of agency modernization goals. The CIO provides advice and other assistance to the head of the agency and other senior management personnel to ensure that IT is acquired, and information resources are managed in a manner that achieves the agency's strategic goals.

The CIO has responsibilities in six key areas:

1. IT leadership and accountability – CIOs are responsible and accountable for the effective implementation of IT management responsibilities.
2. IT strategic planning – CIOs are responsible for strategic planning for all IT management functions.
3. IT workforce – CIOs are responsible for assessing agency IT workforce needs and developing strategies and plans for meeting those needs.
4. IT budgeting – CIOs are responsible for the processes for all annual and multi-year IT planning, programming, and budgeting decisions.
5. IT investment management – CIOs are responsible for the processes for managing, evaluating, and assessing how well the agency is managing its IT resources.
6. Information security and privacy – CIOs are responsible for establishing, implementing, and ensuring compliance with an agency-wide information security program.[3]

The CIO also has two additional areas of focus in their agency's architecture and information resources and data.

The aforementioned responsibilities position the CIO to effectively advise the agency head on the strategic planning and management of information technology, including the prioritization of requirements to receive the maximum benefit of scarce resources and when the agency is no longer

---

[1] Clinger-Cohen Act of 1996. https://home.treasury.gov/system/files/236/Clinger-Cohen_Act_of_1996.pdf

[2] Federal Information Technology Acquisition Reform Act (FITARA). https://management.cio.gov/#:~:text=The%20Federal%20Information%20Technology%20Acquisition,IT)%20in%20almost%2020%20years.

[3] GAO-18-93. Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities. August 2018. https://www.gao.gov/assets/700/693668.pdf

getting the best return on investment. These CIO responsibilities also ensure the agency has a skilled workforce that can keep pace with technical advances and mission areas.

Under the Federal Information Security Modernization Act (FISMA),[4] the CIO must designate a senior official in charge of information security. In most cases, that official is the agency's Chief Information Security Officer (CISO) and works closely with the CIO to protect and secure the information resources of the agency.

[4] Federal Information Security Modernization Act of 2014 (FISMA). https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

01

SECTION

CIO RESPONSIBILITIES

1. CIO Responsibilities

1.1 IT Leadership and Accountability

1.1.1 CIO Responsibilities – Laws and Executive Orders

CIOs are responsible and accountable for the effective implementation of IT management responsibilities. This section includes statutory responsibilities of CIOs related to leadership and accountability. The statutory language is *directly pulled* from applicable laws and executive orders. These statutory responsibilities are then implemented through OMB guidance and guidance from other government-wide organizations. This language, along with the language in other sections under the heading "CIO Responsibilities - Laws and Executive Orders," defines the CIO role and gives the CIO their statutory mandate.

General Responsibilities

1. [CIO] of an executive agency is responsible for—providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the priorities established by the head of the executive agency.[5]
2. The [CIO] designated under paragraph (2) shall head an office responsible for ensuring agency compliance with and prompt, efficient, and effective implementation of the information policies and information resources management responsibilities established under this subchapter, including the reduction of information collection burdens on the public. The [CIO] and employees of such office shall be selected with special attention to the professional qualifications required to administer the functions described under this subchapter.[6]
3. The [CIO] of an executive agency is responsible for:
    a. Providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this subtitle, consistent with chapter 35 of title 44 and the priorities established by the head of the executive agency;
    b. Developing, maintaining, and facilitating the implementation of a sound, secure, and integrated information technology architecture for the executive agency; and
    c. Promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency.[7]

---

[5] 44 U.S.C. §3506. US Federal Information Policy. Federal Agency Responsibilities. https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapI-sec3506/context

[6] 44 U.S.C. §3506(a)(3). US Federal Information Policy. Federal Agency Responsibilities. Chief Information Officer. https://www.law.cornell.edu/uscode/text/44/3506

[7] 44 U.S.C. §3506. US Federal Information Policy. Federal Agency Responsibilities. https://www.law.cornell.edu/uscode/text/44/3506

4. The [CIO] of an agency listed in section 901(b) of title 31:
    a. Has information resources management duties as that official's primary duty;
    b. Monitors the performance of information technology programs of the agency, evaluates the performance of those programs on the basis of the applicable performance measurements, and advises the head of the agency regarding whether to continue, modify, or terminate a program or project; and
    c. Annually, as part of the strategic planning and performance evaluation process required (subject to section 1117 of title 31) under section 306 of title 5 and sections 1105(a)(28), 1115–1117, and 9703 (as added by section 5(a) of the Government Performance and Results Act of 1993 (Public Law 103–62, 107 Stat. 289)) of title 31—(A) assesses the requirements established for agency personnel regarding knowledge and skill in information resources management and the adequacy of those requirements for facilitating the achievement of the performance goals established for information resources management; (B) assesses the extent to which the positions and personnel at the executive level of the agency and the positions and personnel at management level of the agency below the executive level meet those requirements; (C) develops strategies and specific plans for hiring, training, and professional development to rectify any deficiency in meeting those requirements; and (D) reports to the head of the agency on the progress made in improving information resources management capability.[8]

Authorities and Reporting Relationships

The CIO of the covered agency approves the appointment of any component CIO in that agency.[9] The CIO of the covered agency reports directly to the agency head, such that the CIO has direct access to the agency head regarding all programs that include IT.[10]

Role

1. To promote the effective, efficient, and secure use of IT to accomplish the agency's mission, the CIO serves as the primary strategic advisor to the agency head concerning the use of IT.[11]

[8] 40 U.S.C. §11315. Responsibility for Acquisitions of Information Technology. Agency Chief Information Officer. https://www.law.cornell.edu/uscode/text/40/11315

[9] 40 U.S.C. §11319(b)(2). Responsibility for Acquisitions of Information Technology. Resources, planning, and portfolio management. https://uscode.house.gov/view.xhtml?req=(title:40%20section:11319%20edition:prelim) & EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers

[10] 44 U.S.C. §3506(a)(2). Federal Information Policy. Federal Agency Responsibilities. https://www.law.cornell.edu/uscode/text/44/3506 & EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers

[11] 40 U.S.C. §11315(b). Agency Chief Information Officer. General Responsibilities. https://www.law.cornell.edu/uscode/text/40/11315 & EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers

2. The CIO has a significant role, including, as appropriate, as lead advisor, in all annual and multiyear planning, programming, budgeting, and execution decisions, as well as in all management, governance, and oversight processes related to IT.[12]

Governance
The CIO shall be a member of any investment or related board of the agency with purview over IT, or any board responsible for setting agency-wide IT standards.[13]

1.1.2. Agency IT Authorities – Laws and Executive Orders

This section consists of IT authorities assigned to agencies in laws and executive orders which directly or indirectly task the CIO with duties or responsibilities pertaining to IT leadership and accountability. The statutory language is *directly pulled* from the applicable laws and executive orders. In most cases, the heads of agencies delegate all IT management responsibilities to the CIO, but some functions are explicitly assigned to more than one person (e.g. the CIO in consultation with the Chief Financial Officer (CFO)). See individual agency policies to determine how instances of dual responsibility are implemented and executed, and what tasks (if any) are required of the agency head but not delegated to the CIO.

Role
The head of each agency shall be responsible for:

1. Carrying out the agency's information resources management activities to improve agency productivity, efficiency, and effectiveness; and complying with the requirements of this subchapter and related policies established by the Director.
2. Except as provided under subparagraph (B), the head of each agency shall designate a [CIO] who shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter.[14]

In consultation with the [CIO] designated under paragraph (2) and the agency [CFO] (or comparable official), each agency program official shall define program information needs and develop strategies, systems, and capabilities to meet those needs.[15]

---

[12] 40 U.S.C. §11319(b)(1)(A). Responsibility for Acquisitions of Information Technology. Resources, planning, and portfolio management. Additional Authorities for Chief Information Officers. https://uscode.house.gov/view.xhtml?req=(title:40%20section:11319%20edition:prelim) & EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers

[13] EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers

[14] 44 U.S.C. §3506. US Federal Information Policy. Federal Agency Responsibilities. Information Resources Management. https://www.law.cornell.edu/uscode/text/44/3506

[15] Ibid.

Establish a process within the office headed by the [CIO] designated under subsection (a), that is sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be approved under this subchapter, to—review each collection of information before submission to the Director for review under this subchapter.[16]

Policy
It is the policy of the executive branch to:

- Empower agency CIOs to ensure that agency IT systems are secure, efficient, accessible, and effective, and that such systems enable agencies to accomplish their missions;
- Modernize IT infrastructure within the executive branch and meaningfully improve the delivery of digital services; and
- Improve the management, acquisition, and oversight of Federal IT.[17]

Agency-Wide IT Consolidation
The head of each covered agency shall take all necessary and appropriate action to:

- Eliminate unnecessary IT management functions;
- Merge or reorganize agency IT functions to promote agency-wide consolidation of the agency's IT infrastructure, taking into account any recommendations of the relevant agency CIO; and
- Increase use of industry best practices, such as the shared use of IT solutions within agencies and across the executive branch.[18]

Strengthening Cybersecurity
The head of each covered agency shall take all necessary and appropriate action to ensure that:

- The CIO, as the principal advisor to the agency head for the management of IT resources, works closely with an integrated team of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources to implement appropriate risk management measures; and
- The agency prioritizes procurement of shared IT services, including modern email and other cloud-based services, where possible and to the extent permitted by law.[19]

---

[16] Ibid.
[17] EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers
[18] EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers & EO 13781. Comprehensive Plan for Reorganizing the Executive Branch. March 2017. https://www.federalregister.gov/documents/2017/03/16/2017-05399/comprehensive-plan-for-reorganizing-the-executive-branch
[19] EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers & EO 13800. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. May 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

Knowledge and Skills Standards for IT Personnel

- The CIO assesses and advises the agency head regarding knowledge and skill standards established for agency IT personnel;
- Ensures that the established knowledge and skill standards are included in the performance standards and reflected in the performance evaluations of all component CIOs and that the CIO is responsible for that portion of the evaluation; and
- Ensures all component CIOs apply those standards within their own components.[20]

CIO Hiring Authorities

As directed in EO 13833, OPM and the Chief Human Capital Officer Council published guidance delegating to the head of each covered agency authority to determine whether there is a severe shortage of candidates, or that a critical hiring need exists, for IT positions at the agency.[21] This direct hire authority (DHA) expands agencies' ability to maximize DHA for meeting critical IT hiring challenges beyond the Government-wide DHA for IT, which is limited to IT positions related to information security.

Governance

Wherever appropriate and consistent with applicable law, the head of each covered agency shall ensure that the CIO shall be a member of any investment or related board of the agency with purview over IT, or any board responsible for setting agency-wide IT standards. The head of each covered agency shall also, as appropriate and consistent with applicable law, direct the CIO to chair any such board. To the extent any such board operates through member votes, the head of each covered agency shall also, as appropriate and consistent with applicable law, direct the CIO to fulfill the role of voting member.[22]

1.1.3 CIO Responsibilities – OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or otherwise clarifies the responsibilities of agency CIOs with regards to IT leadership and accountability. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on the Office of Inspector General (OIG) and the Government Accountability Office (GAO) to review how compliance with policies is measured.

Empowering Agency CIOs

IT solutions are most effective when they result from a strong partnership between program and mission officials and empowered CIOs. Program and mission officials are responsible for understanding customer needs and establishing business requirements. Agency CIOs must support mission programs by providing secure and effective commodity IT and business systems that take enterprise needs into account. Consistent with OMB Memorandum M-11-29, CIOs must be empowered by the agency head to drive operating efficiencies by having authority over IT governance, commodity IT systems, information

[20] OPM. Announcing Government-wide Direct Hire Appointing Authorities. 10/11/2018. https://www.sfs.opm.gov/Documents/GovHireAppointingAuthorityMemo.pdf

[21] OPM. Delegation of Direct-Hire Appointing Authority for IT Positions. 4/5/2019. https://www.chcoc.gov/content/delegation-direct-hire-appointing-authority-it-positions

[22] EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers

security, and IT program management oversight. Agencies without an empowered CIO regularly lack a complete and accurate inventory of IT assets and services (including mission systems) across the enterprise. This lack of visibility reduces agencies' capacity to consolidate redundant applications, promote modular development, use enterprise license agreements, and migrate to a service orientation.[23]

Reporting Relationships
The CIO reports to the agency head (or deputy/[Chief Operating Officer (COO)]). As required by the Clinger Cohen Act and left in place by The Federal IT Acquisition and Reform Act (FITARA), the CIO "shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter."[24]

IT Investment Governance
FITARA creates clear responsibilities for agency CIOs related to IT investments and planning, as well as requiring that agency CIOs be involved in the IT acquisition process. OMB's FITARA implementation guidance established a "common baseline" for roles, responsibilities, and authorities of the agency CIO and the roles of other applicable Senior Agency Officials in managing IT as a strategic resource. Accordingly, agency heads must ensure that CIOs and Senior Agency Officials, including Chief Acquisition Officers (CAOs), are positioned with the responsibility and authority necessary to implement the requirements of this policy.

1.1.4 Agency IT Authorities – OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or clarifies IT authorities assigned to agencies. This language directly or indirectly tasks the CIO with duties or responsibilities pertaining to IT leadership and accountability. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with policies is measured.

Governance
In support of agency missions and business needs, and in coordination with program managers, agencies shall:

1. Define, implement, and maintain processes, standards, and policies applied to all information resources at the agency, in accordance with OMB guidance;
2. Require that the CIO, in coordination with appropriate governance boards, defines processes and policies in sufficient detail to address information resources appropriately. At a minimum, these processes and policies shall require that:

    a. Investments and projects in development are evaluated to determine the applicability of agile development;

[23] OMB M-13-09. Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management. March 2013. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-09.pdf
[24] OMB M-15-14. Management and Oversight of Federal Information Technology. June 2015. https://www.fai.gov/sites/default/files/2015-06-10-OMB-Memo-FITARA.pdf, 44 U.S.C. §3506. US Federal Information Policy. Federal Agency Responsibilities. https://www.law.cornell.edu/uscode/text/44/3506

b. Open data standards are used to the maximum extent possible when implementing IT systems;
c. Appropriate measurements are used to evaluate the cost, schedule, and overall performance variances of IT projects across the portfolio leveraging processes such as IT investment management, enterprise architecture, and other agency IT or performance management processes;[25]
d. There are agency-wide policies and procedures for conducting IT investment reviews, operational analyses, or other applicable performance reviews to evaluate IT resources, including projects in development and ongoing activities;
e. Data and information needs are met through agency-wide data governance policies that clearly establish the roles, responsibilities, and processes by which agency personnel manage information as an asset and the relationships among technology, data, agency programs, strategies, legal and regulatory requirements, and business objectives; and
f. Unsupported information systems and system components are phased out as rapidly as possible, and planning and budgeting activities for all IT systems and services incorporate migration planning and resourcing to accomplish this requirement;

3. Ensure that the CIO is a member of governance boards that inform decisions regarding IT resources to provide for early matching of appropriate information resources with program objectives. The CIO may designate, in consultation with other senior agency officials, other agency officials to act as their representative to fulfill aspects of this responsibility so long as the CIO retains accountability;
4. Require that information security and privacy be fully integrated into the system development process;
5. Conduct TechStat reviews, led by the CIO, or use other applicable performance measurements to evaluate the use of agency information resources. The CIO may recommend to the agency head the modification, pause, or termination of any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation, within the terms of the relevant contracts and applicable regulations;
6. Establish and maintain a process for the CIO to regularly engage with program managers to evaluate IT resources supporting each agency strategic objective. It shall be the CIO and program managers' shared responsibility to ensure that legacy and ongoing IT investments are appropriately delivering customer value and meeting the business objectives of the agency and the programs that support the agency; and
7. Measure performance in accordance with the GPRA Modernization Act and OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*.[26]

Risk Management

Risk Identification

OMB Circular No. A-123 requires agencies to identify and assess risk as part of the agency's risk profile. A critical component of developing the risk profile is the determination by management

[25] Federal Acquisition Streamlining Act of 1994. https://www.congress.gov/bill/103rd-congress/senate-bill/1587/text

[26] OMB Circular A-130. Managing Information as a Strategic Resource. Policy. July 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

of those risks in which the application of formal internal control activities is the appropriate risk response.[27]

Materiality
Management has responsibility in determining risk to achieving reporting objectives and aligning the level of control activities to provide reasonable assurances over reporting.[28]

Governance
The responsibilities of managing risks are shared throughout the Agency from the highest levels of executive leadership to the service delivery staff executing Federal programs.[29]

Risk Management Council
To provide governance for the risk management function, agencies may use a Risk Management Council (RMC) to oversee the establishment of the Agency's risk profile, regular assessment of risk, and development of appropriate risk response. RMC structures will vary by Agency, and in some cases may be integrated with existing management structures. An effective RMC will include senior officials for program operations and mission-support functions to help ensure those risks are identified which have the most significant impact on the mission outcomes of the Agency. Should agencies choose to use an RMC, the RMC should be chaired by the Agency [COO] or a senior official with responsibility for the enterprise. In cabinet-level Agencies this is the Deputy Secretary.[30]

Risk Profile
Agencies must maintain a risk profile. The primary purpose of a risk profile is to provide a thoughtful analysis of the risks an Agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. The risk profile must consider risks from a portfolio perspective and be approved by an Agency's RMC or equivalent.[31]

Appropriate Content and Format
Agencies have discretion in terms of the appropriate content and format for their risk profiles; however, in general risk profiles should include the following seven components:[32]

1. Identification of Objectives
2. Identification of Risk
3. Inherent Risk Assessment
4. Current Risk Response
5. Residual Risk Assessment
6. Proposed Risk Response

---

[27] OMB M-18-16. Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk M-18-16. June 2018. https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-16.pdf
[28] Ibid.
[29] OMB M-16-17. Circular A-123. Management's Responsibility for Enterprise Risk Management and Internal Control. July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf
[30] Ibid.
[31] Ibid.
[32] Ibid.

7. Proposed Action Category

Risk Identification

The identification of risk is a continuous and ongoing process. Once initial risks are identified, it is important to re-examine risks on a regular basis to identify new risks or changes to existing risks.[33]

Risk Response

As part of developing the risk profile, management must determine those risks for which the appropriate response includes implementation of formal internal control activities as described in Section III of this guidance and which conform to the standards published by GAO in the Green Book. Identification of the existing management process that will be used to implement and monitor proposed actions. Those proposed actions that will be discussed with OMB as part of the annual Strategic Review must be identified,[34] as well as proposed actions to be considered during formulation of the President's Budget.[35]

Annual Reviews

After initial implementation, the agency's risk profile must be discussed each year with OMB as a component of the summary of findings from the Agency strategic review and FedSTAT.[36]

Risk Governance and Internal Control

Agencies must have a Senior Management Council (SMC) to assess and monitor deficiencies in internal control. This SMC may be a subset of the Risk Management Council; however, agencies have discretion in determining the appropriate structure. A Senior Management Council may include the [CFO], [Chief Human Capital Officer (CHCO)], [CIO], [CISO], [CAO], Senior Agency Official for Privacy, Designated Agency Ethics Official, and Performance Improvement Officer and the managers of other program offices, must be involved in identifying and ensuring correction of systemic material weaknesses relating to their respective programs.[37]

Internal Control Sources of Information

The Agency's assessment of internal control may be documented using a variety of information sources to include:[38]

- Management reviews and annual evaluations and reports related to information technology, information security, and information resources pursuant to the Federal Information Security Modernization Act of 2014 and OMB Circular No. A-130, Responsibilities for Protecting Federal Information Resources;

---

[33] Ibid.

[34] OMB Circular A-11. Section 270, Performance and Strategic Reviews. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/a11_current_year/s270.pdf

[35] OMB M-16-17. Circular A-123. Management's Responsibility for Enterprise Risk Management and Internal Control. July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

[36] OMB Circular A-11. Section 270, Performance and Strategic Reviews. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/a11_current_year/s270.pdf

[37] OMB M-16-17. Circular A-123. Management's Responsibility for Enterprise Risk Management and Internal Control. July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

[38] Ibid.

- Outputs of governance mechanisms for information technology resources published by the Agency, pursuant to the "CIO Authorities" described in the Federal Information Technology Acquisition Reform Act (FITARA).

Enterprise Risk Management (ERM) Requirements

All executive agencies are required by OMB Circular No. A-123 to integrate ERM processes and internal controls and are required to include consideration of internal controls over reporting [ICOR] in their annual assurance statement. This update aligns ICOR with existing OMB Circular No. A123 ERM efforts. This framework for internal controls over reporting may be phased in over several years as the agency's ERM process matures. As an agency's ERM process matures, the agency risk profile may begin to identify and link some enterprise risks with formal internal controls. As this integration occurs, management must include consideration of these controls in the OMB Circular No. A-123 assurance process.[39]

COVID-19 and Mission Delivery

In response to the national emergency for COVID-19, agencies are directed to use the breadth of available technology capabilities to fulfill service gaps and deliver mission outcomes. The [Harnessing Technology to Support Mission Continuity] "frequently asked questions" are intended to provide additional guidance and further assist the IT workforce as it addresses impacts due to COVID-19. Additional technology related questions should be directed to the Office of the Federal CIO at OFCIO@omb.eop.gov. OMB will continue to provide updates and additional information as needed to support the resiliency of agency missions.[40]

Program Management

Program Management Improvement Accountability Act (PMIAA) Implementing Strategy 1 - Coordinated Governance: Overview of Organizational Changes

The PMIAA [established] a new governance structure and function at agencies for advancing the practice of [program/project management (P/PM)] across the Federal Government. This section provides guidance to agencies by describing how agency COOs should integrate P/PM as a component of the agencies' broader management capabilities, providing the role and responsibilities of the PMIO, and defining the functions and composition of the PMPC.

Roles and Functions of the Program Management Improvement Officer (PMIO)

Improvements in program management should lead to improved program performance and effectiveness that advance progress towards the achievement of agency strategic goals and objectives. In order to enhance and coordinate the practice and application of program management at agencies, PMIOs will:[41]

- Collaborate with and support CIOs to ensure IT programs and projects have trained and qualified program and project managers with the appropriate qualifications per the

[39] OMB M-18-16. Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk M-18-16. June 2018. https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-16.pdf

[40] OMB M-20-19. Harnessing Technology to Support Mission Continuity. March 2020. https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-19.pdf

[41] OMB M-18-19. Improving the Management of Federal Programs and Projects through Implementing the Program Management Improvement Accountability Act (PMIAA). Appendix 2. June 2018. https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-19.pdf

approved Federal IT PM Guidance Matrix and to enforce FITARA, OMB Memorandum M-04-19, and OMB Memorandum M-10-27 policy for IT programs.

Implementing Acquisition Portfolio Reviews: Acquisition Program Management
Several laws, regulations, and policies have provided direction for acquisition program management, including provisions in the Federal Acquisition Streamlining Act (FASA), the Clinger-Cohen Act, OMB's Capital Programming Guide, and Part 34 of the Federal Acquisition Regulation (FAR). Agencies have developed detailed policies and procedures to implement these requirements, but too often, this guidance has not been reflected adequately in agency governance structures and protocols.

Identifying IT Programs vs. Non-IT Programs
Reviews of major acquisitions supporting IT programs shall build on portfolio reviews conducted pursuant to FITARA, 44 U.S.C. § 11319. Programs shall be considered IT programs if the investment scope is primarily information technology as defined in FAR Subpart 2.1. Programs with embedded systems or small IT components shall be considered non-IT, but collaboration with CIOs is expected for any significant components of the investment that involve IT.[42]

Portfolio Management

Integrated Data Collection (IDC)
[OMB established] an Integrated Data Collection channel for agencies to report structured information. Agencies will use this channel to report agency progress in meeting IT strategic goals, objectives and metrics as well as cost savings and avoidances resulting from IT management actions. This data includes information previously reported by agencies as well as data which agencies [should have reported] by May 15, 2013 and then update every three months thereafter. Subsequent updates will be on the last day of August, November, and February of subsequent fiscal years. Appendix B provides more detail on this Integrated Data Collection and a link to reporting instructions and guidance for the May 15, 2013 deadline. This Integrated Data Collection will draw on information previously reported under PortfolioStat, the FDCCI, the Federal Digital Government Strategy, quarterly Federal Information Security Management Act metrics, the Federal IT Dashboard, and selected human resource, financial management, and procurement information requested by OMB.[43]

PortfolioStat Sessions
In support of this review process, Agency [COO], on an annual basis, shall be required to lead an agency-wide IT portfolio review within their respective organization (PortfolioStat). A PortfolioStat session is a face-to-face, evidence-based review (e.g., including data on commodity IT investments, potential duplications, investments that do not appear to be well aligned to agency missions or business functions, etc.) of an agency's IT portfolio.

[42] Ibid, Appendix 5.
[43] OMB M-13-09. Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management. March 2013. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-09.pdf

CIOs, CFOs, and CAOs must support the PortfolioStat process by providing the necessary data and analysis, attending the PortfolioStat meeting, and support all decisions made through the process. This is necessary so that the portfolio-wide review results in concrete actions to maximize the investment in mission and support IT, consolidate the acquisition and management of commodity IT, reduce duplication, and eliminate waste.

To support this process, OMB is requiring that each agency take the following actions:[44]

- Designate Lead for Initiative
- Complete a High-Level IT Portfolio Survey
- Establish a Commodity IT Investment Baseline
- Submit a Draft Plan to Consolidate Commodity IT
- Hold PortfolioStat Session
- Submit a Final Plan to Consolidate Commodity IT
- Migrate at Least Two Duplicative Commodities IT Services
- Document Lessons Learned

Agency PortfolioStat Conduct

PortfolioStat is a data-driven tool that agencies use to assess the current maturity of their IT portfolio management processes and select PortfolioStat action items to strengthen their IT portfolio. Covered agencies shall hold PortfolioStat sessions on a quarterly basis with OMB, the agency CIO, and other attendees.[45]

Data Management

Code Inventories and Discovery Inventories

Code Inventories and Discovery Inventories are a means of discovering information such as the functionality and location of potentially reusable or releasable custom-developed code. Within 120 days of the publication date of [the Federal Source Code Policy], each agency [should have updated]—and thereafter keep up to date—its inventory of agency information resources to include an enterprise code inventory that lists custom-developed code for or by the agency after the publication of this policy. Each agency's inventory will be reflected on Code.gov. The inventory will indicate whether the code is available for Federal reuse, is available publicly as OSS, or cannot be made available due to a specific exception listed in this policy. Agencies shall fill out this information based on a metadata schema that OMB will provide on Code.gov.[46]

Open Source Software Policy

---

[44] OMB M-12-10. Implementing PortfolioStat. March 2012. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2012/m-12-10_1.pdf

[45] These sessions were previously annual and required the attendance of the agency deputy secretary, see OMB M-12-10. March 2012. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2012/m-12-10_1.pdf, OMB M-13-09. March 2013. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-09.pdf, OMB M-14-08. June 2015. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2014/m-14-08.pdf

[46] OMB M-16-21. Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. August 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

As appropriate, Senior Agency Officials should also work with the agency's public affairs staff, open government staff, web manager or digital strategist, program owners, and other leadership to properly identify, publish, and collaborate with communities on their Open Source Software (OSS) projects.[47] Each agency's CIO—in consultation with the agency's CAO—shall develop an agency-wide policy that addresses the requirements of this document. For example, the policy should address how the agency will ensure that an appropriate alternatives analysis has been conducted before considering the acquisition of an existing commercial solution or a custom-developed solution. In accordance with OMB guidance, these policies will be posted publicly. Moreover, within 90 days of the publication date of this policy, each agency's CIO office [should have corrected or amended] any policies that are inconsistent with the requirements of this document, including the correction of policies that automatically treat OSS as noncommercial software.[48]

Open Data Policy

The Clinger-Cohen Act of 1996 assigns agency CIOs statutory responsibility for promoting the effective and efficient design and operation of all major Information Resources Management (IRM) processes within their agency. Accordingly, agency heads must ensure that CIOs are positioned with the responsibility and authority to implement the requirements of the Open Data Policy Memorandum in coordination with the agency's [CAO], [CFO], Chief Technology Officer, Senior Agency Official for Geospatial Information, Senior Agency Official for Privacy (SAOP), [CISO], [Senior Agency Official for Records Management (SAORM)], and Chief Freedom of Information Act (FOIA) Officer. The CIO should also work with the agency's public affairs staff, open government staff, web manager or digital strategist, program owners and other leadership, as applicable.[49]

[47] Ibid.

[48] Ibid.

[49] OMB M-13-13. Open Data Policy-Managing Information as an Asset. May 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf

1.2 IT Strategic Planning

1.2.1 CIO Responsibilities - Laws and Executive Orders

CIOs are responsible for strategic planning for all IT management functions. This section lists the statutory responsibilities of CIOs related to strategic planning. The statutory language is *directly pulled* from applicable laws and executive orders. These statutory responsibilities are then implemented through OMB guidance and guidance from other government-wide organizations. This language, along with the language in other sections under the heading "CIO Responsibilities - Laws and Executive Orders," defines the CIO role and gives the CIO their statutory mandate.

General Responsibilities

Planning, programming, budgeting, and execution authorities for CIOs:

1. The head of each covered agency other than the Department of Defense shall ensure that the [CIO] of the agency has a significant role in:
    a. The decision processes for all annual and multi-year planning, programming, budgeting, and execution decisions, related reporting requirements, and reports related to information technology; and
    b. The management, governance, and oversight processes related to information technology.[50]

Chief Information Officer (CIO)

The CIO of an agency listed in section 901(b) of title 31… annually, as part of the strategic planning and performance evaluation process required (subject to section 1117 of title 31) under section 306 of title 5 and sections 1105(a)(28), 1115–1117, and 9703 (as added by section 5(a) of the Government Performance and Results Act of 1993 (Public Law 103–62, 107 Stat. 289)) of title 31—(C) develops strategies and specific plans for hiring, training, and professional development to rectify any deficiency in meeting those requirements; and (D) reports to the head of the agency on the progress made in improving information resources management capability.[51]

1.2.2 CIO Responsibilities - OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or otherwise clarifies the responsibilities of agency CIOs with regards to strategic planning. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with these documents is measured.

Streamlining of Agency Reporting

To improve the outcomes of PortfolioStat and to advance agency IT portfolio management, OMB is consolidating previously collected IT plans, reports and data calls into four primary collection channels:

[50] 40 U.S.C. §11319. Responsibility for Acquisitions of Information Technology. Resources, Planning, and Portfolio Management. https://uscode.house.gov/view.xhtml?req=(title:40%20section:11319%20edition:prelim)

[51] 40 U.S.C. §11315. Agency Chief Information Officer. https://www.law.cornell.edu/uscode/text/40/11315

Information Resources Management (IRM) Strategic Plans, Capital Planning and Investment Control (CPIC), Enterprise Roadmap and Integrated Data Collection.

Information Resources Management (IRM) Strategic Plans

According to Circular A-130, "Information Resources Management (IRM) Strategic Plans should support the agency Strategic Plan required in OMB Circular A-11, and provide a description of how information resources management activities help accomplish agency missions, and ensure that information resource management decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions."[52] In addition to requirements established in OMB Circular A-130, IRM Strategic Plans must now be signed by the Agency COO. At "each agency the deputy head of agency, or equivalent, shall be the [COO] and as needed the head of the agency may make adjustments to the strategic plan to reflect significant changes in the environment in which the agency is operating with appropriate notification of Congress."[53]

[Agencies are] required to address the specific requirements that are defined in Appendix A of OMB Memorandum M-13-09.[54]

Capital Planning and Investment Control (CPIC)

CPIC is a structured approach to managing IT investments. CPIC ensures that IT investments align with the agency's mission, strategic goals, and objectives, and support business needs, while minimizing risks and maximizing returns throughout the investment's life cycle. CPIC relies on systematic selection, control, and continual evaluation processes to ensure that the investment's objectives are met effectively.

Investments in IT can dramatically enhance organizational performance. When carefully managed, IT becomes a critical enabler to improve business processes, makes information widely available, and reduces the cost of providing essential Government services. As IT rapidly evolves, the challenge of realizing its potential benefits also becomes much greater.

Congress and OMB have clearly stated that each executive agency must actively manage its IT program to provide assurances that technology expenditures are necessary and shall result in demonstrated improvements in mission effectiveness and customer service. The Clinger-Cohen Act (CCA) of 1996, Public Law 104 – 106, legislatively mandates that IT investments be prudently managed.

[Agency investment estimates] should reflect the Administration's commitment to Information Technology (IT) investments that directly support agency missions as identified in the agency's Information Resources Management (IRM) Strategic Plan, specified in OMB Circular A-130, which should fully describe all IT resources at the agency, be prepared in a manner consistent with the CIO role and CIO review described on page 11 of OMB memorandum M-15-14

---

[52] OMB Circular A-130. Managing Information as a Strategic Resource. Policy. July 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[53] Public Law 107-296. GPRA Modernization Act of 2010. Agency Strategic Plans. https://www.govinfo.gov/content/pkg/BILLS-111hr2142enr/pdf/BILLS-111hr2142enr.pdf

[54] OMB M-13-09. Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management. March 2013. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-09.pdf

Management and Oversight of Federal Information Technology,[55] including the certification statements described in section 51.3, and be consistent with the Federal IT Acquisition Reform Act (FITARA) and other relevant laws as described by instructions in sections 51.19 and 55.[56]

Enterprise Roadmap
In alignment with the IRM Strategic Plan, the Enterprise Roadmap documents an agency's current and future views of its business and technology environment from an architecture perspective. It does so by reflecting the implementation of new or updated business capabilities and enabling technologies that support the agency's strategic goals and initiatives. It also contains a transition plan to show the sequence of actions needed to implement the IRM Strategic plan. Moreover, it focuses on increasing shared approaches to IT service delivery across mission, support, and commodity areas.

See also Appendix A, Additional Information Resources Management (IRM) Strategic Plan and Enterprise Roadmap Reporting Requirements.[57]

Integrated Data Collection (IDC)
[OMB established] an Integrated Data Collection channel for agencies to report structured information. Agencies will use this channel to report agency progress in meeting IT strategic goals, objectives and metrics as well as cost savings and avoidances resulting from IT management actions. This data includes information previously reported by agencies as well as data which agencies [should have reported] by May 15, 2013 and then update every three months thereafter. Subsequent updates will be on the last day of August, November, and February of subsequent fiscal years. Appendix B provides more detail on this Integrated Data Collection and a link to reporting instructions and guidance for the May 15, 2013 deadline. This Integrated Data Collection will draw on information previously reported under PortfolioStat, the FDCCI, the Federal Digital Government Strategy, quarterly Federal Information Security Management Act metrics, the Federal IT Dashboard, and selected human resource, financial management, and procurement information requested by OMB.[58]

Open Data Policy Requirements
Agencies management of information resources must begin at the earliest stages of the planning process, well before information is collected or created. Early strategic planning will allow the Federal Government to design systems and develop processes that unlock the full value of the information and provide a foundation from which agencies can continue to manage information throughout its life cycle.

Build Information Systems to Support Interoperability and Information Accessibility
Through their acquisition and technology management processes, agencies must build or modernize information systems in a way that maximizes interoperability and information accessibility, to the extent practicable and permitted by law. Agencies must exercise forethought when architecting, building, or substantially modifying an information system to facilitate public distribution, where appropriate. In

[55] Management and Oversight of Federal Information Technology. https://management.cio.gov/
[56] OMB Circular A-11. Preparing, Submitting and Executing the Budget. July 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf
[57] Ibid.
[58] OMB M-13-09. Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management. March 2013. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-09.pdf

addition, the agency's CIO must validate that the following minimum requirements have been incorporated into acquisition planning documents and technical design for all new information systems and those preparing for modernization, as appropriate:

- The system design must be scalable, flexible, and facilitate extraction of data in multiple formats and for a range of uses as internal and external needs change, including potential uses not accounted for in the original design. In general, this will involve the use of standards and specifications in the system design that promote industry best practices for information sharing, and separation of data from the application layer to maximize data reuse opportunities and incorporation of future application or technology capabilities, in consultation with the best practices found in Project Open Data.[59]
- The 21st Century Integrated Digital Experience Act (IDEA)[60] aims to improve the digital experience for government customers and reinforces existing requirements for federal public websites. Specifically, the Act requires all executive branch agencies to
    a. Modernize their websites,
    b. Digitize services and forms,
    c. Accelerate use of e-signatures,
    d. Improve customer experience,
    e. Standardize and transition to centralized shared services, and
    f. Comply with website standards using the U.S Web Design Systems[61].

1.2.3 Agency IT Authorities - Laws and Executive Orders

This section consists of IT authorities assigned to agencies in laws and executive orders which directly or indirectly task the CIO with duties or responsibilities pertaining to IT strategic planning. The statutory language is *directly pulled* from the applicable laws and executive orders. In most cases, the heads of agencies delegate all IT management responsibilities to the CIO, but some functions are explicitly assigned to more than one person (e.g. the CIO in consultation with the CFO). See individual agency policies to determine how instances of dual responsibility are implemented and executed, and what tasks (if any) are required of the agency head but not delegated to the CIO.

Agency Strategic Plans
Not later than the first Monday in February of any year, following the year in which the term of the President commences under section 101 of title 3, the head of each agency shall make available on the public website of the agency a strategic plan and notify the President and Congress of its availability.[62]

Such plan shall contain:

1. A comprehensive mission statement covering the major functions and operations of the agency;

[59] OMB M-13-13. Open Data Policy-Managing Information as an Asset. May 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf
[60] H.R.5759 - 21st Century Integrated Digital Experience Act. https://www.congress.gov/bill/115th-congress/house-bill/5759/text
[61] GSA. U.S. Web Design System (USWDS). https://designsystem.digital.gov/
[62] 5 U.S.C. §306. Agency Strategic Plans. https://www.govinfo.gov/app/details/USCODE-2014-title5/USCODE-2014-title5-partI-chap3-sec306

2. General goals and objectives, including outcome-oriented goals, for the major functions and operations of the agency;
3. A description of how any goals and objectives contribute to the Federal Government priority goals required by section 1120(a) of title 31;
4. A description of how the goals and objectives are to be achieved, including:
    a. A description of the operational processes, skills and technology, and the human, capital, information, and other resources required to achieve those goals and objectives; and
    b. A description of how the agency is working with other agencies to achieve its goals and objectives as well as relevant Federal Government priority goals.

1.2.4 Agency IT Authorities - OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or clarifies IT authorities assigned to agencies. This language directly or indirectly tasks the CIO with duties or responsibilities pertaining to IT strategic planning. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with policies is measured.

Strategic Planning
In support of agency missions and business needs, and as part of the agency's overall strategic and performance planning processes, agencies shall develop and maintain an Information Resources Management (IRM) Strategic Plan that describes the agency's technology and information resources goals, including but not limited to, the processes described in this Circular. The IRM Strategic Plan must support the goals of the Agency Strategic Plan required by the Government Performance and Results Modernization Act of 2010.[63]

> **Enterprise Architecture (EA)**
> Agency shall develop an enterprise architecture (EA) that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture. The agency's EA shall align to their IRM Strategic Plan. The EA should incorporate agency plans for significant upgrades, replacements, and disposition of information systems when the systems can no longer effectively support missions or business functions.[64]
>
> **Identification of Objectives**
> Risk must be analyzed in relation to achievement of the strategic objectives established in the Agency strategic plan (See OMB Circular No. A-11, Section 230), as well as risk in relation to appropriate operational objectives. Specific objectives must be identified and documented to facilitate identification of risks to strategic, operations, reporting, and compliance.[65]

[63] Circular A-130. Managing Information as a Strategic Resource. July 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[64] Ibid, Inventories.
[65] Circular A-123. Management's Responsibility for Enterprise Risk Management and Internal Control. July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

Strategic Planning Purpose

An agency's strategic goals and objectives should be used to align resources and guide decision-making to accomplish priorities to improve outcomes. It should inform agency decision-making about the need for major new acquisitions, information technology, strategic human capital planning, evaluations, and other evidence-building and evidence-capacity building investments. Strategic Plans can also help agencies invite ideas and stimulate innovation to advance agency goals. The Strategic Plan should support planning across organizational operating units and describe how agency components are working toward common results. Agencies should plan to address the content as established in section 210 when establishing a new or updated Agency Strategic Plan, and should use findings from strategic reviews as well as the development of enterprise risk management profiles and their analysis of risks to help the agency identify the most effective long-term strategies. Additionally, the [Foundations for Evidence-Based Policy Making Act] requires the agency's Strategic Plan include a separate section on evidence-building, referred to as the Learning Agenda as well as a Capacity Assessment. See section 290 for additional guidance describing the relationship of agency Learning Agendas to the Agency Strategic Plan.[66]

Information Resources Management (IRM) Strategic Plans

Agencies are required to submit Information Resources Management (IRM) Strategic Plans which should fully align with the current Agency Strategic Plan and shall be reviewed annually alongside the Annual Performance Plan Reviews, required by the GPRA Modernization Act, to determine if there are any performance gaps or changes to mission needs, priorities, or goals. IRM Strategic Plans should be updated to align with Agency Strategic Plans as specified in A-11 section 230.4. Agencies should identify where they are making investments and performing activities in support of 44 U.S.C. 3506. At a minimum, agencies should include Open Data Plans to demonstrate how they are supporting priority data improvements that support agency goals and missions. Open Data Plans support agency compliance with the statutory requirements described in 44 U.S.C. 3506 per the Foundations for Evidence-Based Policymaking Act of 2018 (Public Law 115-435). Pursuant to 44 U.S.C. 3506, agencies are required to describe how information resources management activities help accomplish agency missions; this includes but is not limited to developing an open data plan that is updated annually and made publicly available on the website of the agency.[67]

Policy Requirements

Agencies management of information resources must begin at the earliest stages of the planning process, well before information is collected or created. Early strategic planning will allow the Federal Government to design systems and develop processes that unlock the full value of the information and provide a foundation from which agencies can continue to manage information throughout its life cycle.

Collect or create information in a way that supports downstream information processing and dissemination activities. Consistent with OMB Circular A-130, agencies must consider, at each

[66] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Agency Strategic Planning. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[67] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Information Technology investments. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

stage of the information life cycle, the effects of decisions and actions on other stages of the life cycle. Accordingly, to the extent permitted by law, agencies must design new information collection and creation efforts so that the information collected or created supports downstream interoperability between information systems and dissemination of information to the public, as appropriate, without the need for costly retrofitting.

Build Information Systems to Support Interoperability and Information Accessibility
Through their acquisition and technology management processes, agencies must build or modernize information systems in a way that maximizes interoperability and information accessibility, to the extent practicable and permitted by law. [68]

[Data Center Optimization Initiative] Strategic Plans
In accordance with FITARA, each agency head shall annually publish a [Data Center Optimization Initiative (DCOI) Strategic Plan] to describe the agency's consolidation and optimization strategy until [the date the policy sunsets].[69] The National Defense Authorization Act of 2020 extended these requirements through October 1, 2022.[70] The DCOI Strategic Plan and milestones described below replace existing requirements for data center consolidation plans.

Agencies' DCOI Strategic Plans must include, at a minimum, the following:

1. Planned and achieved performance levels for each optimization metric, by year;
2. Planned and achieved closures, by year;
3. An explanation for any optimization metrics and closures for which the agency did not meet the planned level in a previous Strategic Plan;
4. Year-by-year calculations of target and actual agency-wide spending and cost savings on data centers through the sunset of this policy, including:
   A description of any initial costs for data center consolidation and optimization; and
   Life cycle cost savings and other improvements (including those beyond the sunset of this policy, if applicable).
5. Historical costs, cost savings, and cost avoidances due to data center consolidation and optimization; and
6. A statement from the agency CIO stating whether the agency has complied with all reporting requirements in this memorandum and the data center requirements of FITARA. If the agency has not complied with all reporting requirements, the agency must provide a statement describing the reasons for not complying.

[68] OMB M-13-13. Open Data Policy-Managing Information as an Asset. May 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf
[69] OMB M-19-19. Update to Data Center Optimization Initiative. June 2019. https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-19-Data-Centers.pdf
[70] Public Law 116-192. National Defense Authorization Act for Fiscal Year 2020. https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf

1.3 IT Workforce

1.3.1 CIO Responsibilities - Laws and Executive Orders

CIOs are responsible for assessing agency IT workforce needs and developing strategies and plans for meeting those needs. This section lists the statutory responsibilities of CIOs related to the IT workforce. The statutory language is *directly pulled* from applicable laws and executive orders. These statutory responsibilities are then implemented through OMB guidance and guidance from other government-wide organizations. This language, along with the language in other sections under the heading "CIO Responsibilities - Laws and Executive Orders," defines the CIO role and gives the CIO their statutory mandate.

Personnel-Related Authority
Notwithstanding any other provision of law, for each covered agency... the [CIO] of the covered agency shall approve the appointment of any other employee with the title of [CIO], or who functions in the capacity of a [CIO], for any component organization within the covered agency.[71]

The [CIO] of an agency (A) assesses the requirements established for agency personnel regarding knowledge and skill in information resources management and the adequacy of those requirements for facilitating the achievement of the performance goals established for information resources management; (B) assesses the extent to which the positions and personnel at the executive level of the agency and the positions and personnel at management level of the agency below the executive level meet those requirements.[72]

The head of each agency shall designate a [CIO] who shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter.[73]

Knowledge and Skills for IT Personnel
The CIO assesses and advises the agency head regarding knowledge and skill standards established for agency IT personnel.[74]

[71] 40 U.S.C. §319(b)(2). Additional easement authority. https://www.govinfo.gov/app/details/USCODE-1997-title40/USCODE-1997-title40-chap4-sec319/context
[72] 40 U.S.C. §11315. Responsibility for Acquisitions of Information Technology. Agency Chief Information Officer. https://www.law.cornell.edu/uscode/text/40/11315
[73] 44 U.S.C. §3506. US Federal Information Policy. Federal Agency Responsibilities. https://www.law.cornell.edu/uscode/text/44/3506
[74] 40 U.S.C. §11315(c)(3). Agency Chief Information Officer. Duties and Qualifications. https://www.law.cornell.edu/uscode/text/40/11315 & EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers

1.3.2 CIO Responsibilities - OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or otherwise clarifies the responsibilities of agency CIOs with regards to the IT workforce. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with policies is measured.

CIO Approves [Component/Bureau] CIOs
The CIO shall be involved in the recruitment and shall approve the selection of any new bureau CIO (includes bureau leadership with CIO duties but not title-see definitions). The title and responsibilities of current bureau CIOs may be designated or transferred to other agency personnel by the agency head or his or her designee as appropriate, and such decisions may take into consideration recommendations from the agency CIO.[75]

Bureau IT Leadership Directory
The CIO and [CHCO] will conduct a survey of all bureau CIOs; and CIO and CHCO will jointly publish a dataset identifying all bureau officials with title of CIO or duties of a CIO. This [should have] been posted as a public dataset based on instructions in the IDC by August 15, 2015 and kept up to date thereafter. The report will identify for each:

- Employment type (e.g., GS, SES, SL, ST, etc.)
- Type of appointment (e.g., career, appointed, etc.)
- Other responsibilities (e.g., full-time CIO or combination CIO/CFO). Evaluation "rating official" (e.g., bureau head, other official)
- Evaluation "reviewing official" (if used)

Whether [agency] CIO identifies this bureau CIO as a "key bureau CIO" and thus requires the [agency] CIO to provide the rating official input into the agency-wide critical element(s) described in IT Workforce.

IT Workforce
The CIO and CHCO will develop a set of competency requirements for IT staff, including IT leadership positions, and develop and maintain a current workforce planning process to ensure the department/agency can:

- Anticipate and respond to changing mission requirements;
- Maintain workforce skills in a rapidly developing IT environment; and
- Recruit and retain the IT talent needed to accomplish the mission.

1.3.3 Agency IT Authorities - Laws and Executive Orders

This section consists of IT authorities assigned to agencies in laws and executive orders which directly or indirectly task the CIO with duties or responsibilities pertaining to the IT workforce. The statutory

[75] OMB M-15-14. Management and Oversight of Federal Information Technology. June 2015. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf

language is *directly pulled* from the applicable laws and executive orders. In most cases, the heads of agencies delegate all IT management responsibilities to the CIO, but some functions are explicitly assigned to more than one person (e.g. the CIO in consultation with the CFO). See individual agency policies to determine how instances of dual responsibility are implemented and executed, and what tasks (if any) are required of the agency head but not delegated to the CIO.

Knowledge and Skill Standards for IT Personnel
The head of each covered agency shall take all necessary and appropriate action to ensure that:[76]

1. The CIO assesses and advises the agency head regarding knowledge and skill standards established for agency IT personnel;
2. The established knowledge and skill standards are included in the performance standards and reflected in the performance evaluations of all component CIOs, and that the CIO is responsible for that portion of the evaluation; and
3. All component CIOs apply those standards within their own components.

1.3.4 Agency IT Authorities - OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or clarifies IT authorities assigned to agencies. This language directly or indirectly tasks the CIO with duties or responsibilities pertaining to the IT workforce. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and the GAO to review how compliance with policies is measured.

Leadership and Workforce
Agency Shall:

1. Require that the [CHCO], CIO, CAO, and SAOP develop a set of competency requirements for information resources staff, including program managers, information security, privacy, and IT leadership positions, and develop and maintain a current workforce planning process to ensure that 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.[77]

[76] EO 13833. Enhancing the Effectiveness of Agency Chief Information Officers. May 2018. https://www.federalregister.gov/documents/2018/05/18/2018-10855/enhancing-the-effectiveness-of-agency-chief-information-officers
[77] OMB Circular A-130. Managing Information as a Strategic Resource. Page 10. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

1.4 IT Budgeting

1.4.1 CIO Responsibilities - Laws and Executive Orders

CIOs are responsible for the processes for all annual and multi-year IT planning, programming, and budgeting decisions. This section lists the statutory responsibilities of CIOs related to budgeting. The statutory language is *directly pulled* from applicable laws and executive orders. These statutory responsibilities are then implemented through OMB guidance and guidance from other government-wide organizations. This language, along with the language in other sections under the heading "CIO Responsibilities – Laws and Executive Orders," defines the CIO role and gives the CIO their statutory mandate.

General Responsibilities
The head of each covered agency… shall ensure that the [CIO] of the agency has a significant role in (i) the decision processes for all annual and multiyear planning, programming budgeting, and execution decisions."[78]

Budget Formulation
The Director of [OMB] shall require in the annual information technology capital planning guidance of the [OMB] the following: (i) That the [CIO] of each covered agency... approve the information technology budget request of the covered agency.[79]

1.4.2 CIO Responsibilities – OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or otherwise clarifies the responsibilities of agency CIOs with regards to IT budgeting. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with these documents is measured.

Visibility of IT Resource Plans/Decisions to CIO
The [CFO] and CIO jointly shall define the level of detail with which IT resource levels are described distinctly from other resources throughout the planning, programming, and budgeting stages. This should serve as the primary input into the IT capital planning and investment control documents submitted with the budget (formerly Exhibits 53 and 300).[80]

CIO Role in Pre-Budget Submission for Programs that Include IT and Overall Portfolio
The agency head shall ensure the agency-wide budget development process includes the CFO, [CAO], and CIO in the planning, programming, and budgeting stages for programs that include IT resources (not just programs that are primarily IT oriented). The agency head, in consultation with the CFO, CIO, and

[78] 40 U.S.C. §11319(b)(1)(A). Responsibility for Acquisitions of Information Technology. Resources, planning, and portfolio management. Additional Authorities for Chief Information Officers. https://uscode.house.gov/view.xhtml?req=(title:40%20section:11319%20edition:prelim)
[79] Ibid, Budget Formulation.
[80] OMB M-15-14. Management and Oversight of Federal Information Technology. June 2015. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf

program leadership, shall define the processes by that program leadership works with the CIO to plan an overall portfolio of IT resources that achieve program and business objectives and to develop sound estimates of the necessary IT resources for accomplishing those objectives.[81]

CIO Role in Planning Program Management
The CIO shall be included in the internal planning processes for how the agency uses IT resources to achieve its objectives. The CIO shall approve the IT components of any plans, through a process defined by the agency head that balances IT investments with other uses of agency funding. This includes CIO involvement with planning for IT resources at all points in their lifecycle, including operations and disposition or migration.[82]

CIO Review/Approve Major IT Investment Budget Request
Agency budget justification materials in their initial budget submission to OMB shall include a statement that affirms:

- The CIO has reviewed and approves the major IT investments portion of this budget request; the CFO and CIO jointly affirm that the CIO had a significant role in reviewing planned IT support for major program objectives and significant increases and decreases in IT resources; and
- The IT Portfolio (formerly Exhibit 53) includes appropriate estimates of all IT resources included in the budget request.[83]

Capital Planning and Investment Control (CPIC)
CPIC is a structured approach to managing IT investments. CPIC ensures that IT investments align with the agency's mission, strategic goals, and objectives, and support business needs, while minimizing risks and maximizing returns throughout the investment's life cycle. CPIC relies on systematic selection, control, and continual evaluation processes to ensure that the investment's objectives are met effectively.

Investments in IT can dramatically enhance organizational performance. When carefully managed, IT becomes a critical enabler to improve business processes, makes information widely available, and reduces the cost of providing essential Government services. As IT rapidly evolves, the challenge of realizing its potential benefits also becomes much greater.

Congress and OMB have clearly stated that each executive agency must actively manage its IT program to provide assurances that technology expenditures are necessary and shall result in demonstrated improvements in mission effectiveness and customer service. The Clinger-Cohen Act (CCA) of 1996, Public Law 104 – 106, legislatively mandates that IT investments be prudently managed.

[Agency investment estimates] should reflect the Administration's commitment to information technology (IT) investments that directly support agency missions as identified in the agency's Information Resources Management (IRM) Strategic Plan, specified in OMB Circular A-130, which should fully describe all IT resources at the agency, be prepared in a manner consistent with the CIO role and CIO review described on page 11 of OMB memorandum M-15-14 Management and Oversight of Federal

[81] Ibid.
[82] Ibid.
[83] Ibid.

IT, including the certification statements described in section 51.3, and be consistent with FITARA and other relevant laws as described by instructions in sections 51.19 and 55.[84]

Agency Software Strategies – Centralizing and Improving Software Management
FITARA provides new authorities and responsibilities that CIOs can use to improve their agencies' IT management policies and practices. To improve covered agencies' software management practices, CIOs, in coordination with CAOs and CFOs, [must]:

- [Appoint] a software manager that is responsible for managing, through policy and procedure, all agency-wide commercial and COTS software agreements and licenses. The software manager shall report to the agency CIO and will work in collaboration with the offices of the CIO, CAO, CFO, and other organizations as appropriate.
- Maintain a continual agency-wide inventory of software licenses, including all licenses purchased, deployed, and in use, as well as spending on subscription services (to include provisional (i.e., cloud) software as a service agreement (SaaS)).
- Analyze inventory data to ensure compliance with software license agreements, consolidate redundant applications, and identify other cost-saving opportunities.[85]

Building a Better Federal Marketplace for Laptops and Desktops
The Category Management Leadership Council (CMLC) established an interagency Workstation Category Team (WCT), led by the National Aeronautics and Space Administration (NASA) and comprised of laptop and desktop computer subject matter experts and managers of large Government-wide and agency-wide hardware contracts. As a result of this work, OMB [determined] that agencies must take immediate steps, described in more detail below, to:

1. Standardize laptop and desktop configurations for common requirements;
2. Reduce the number of contracts for laptops and desktops by consolidating purchasing and using a fewer number of high-performing -or best-in-class-contracts; and
3. Develop and modify demand management processes to optimize price and performance.

The WCT [work] with agency CIOs and the vendor community to identify the attributes of standard or upgraded laptops and desktops every six months beginning in the fourth quarter of FY 2015. Furthermore, the WCT [adds or removes] configurations as necessary to adapt to changing agency needs and market trends, such as the increased use of tablets and the transition from traditional computing to virtual infrastructure. [CIOs shall] ensure that at least 80% of their agency's new basic laptop and desktop requirements are satisfied with one of these standard configurations, unless an exception is consistent with an approved IT acquisition strategy or plan, as required by OMB's FITARA implementation guidance, and approved in writing by the agency CIO.[86]

---

[84] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Management Improvement Initiatives and Policies. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf
[85] OMB M-16-12. Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing. June 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf
[86] OMB M-16-02. Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops. October 2015. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-02.pdf

1.4.3 Agency IT Authorities – OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or clarifies IT authorities assigned to agencies. This language directly or indirectly tasks the CIO with duties or responsibilities pertaining to IT budgeting. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with policies is measured.

Planning, Programming, and Budgeting
[Agencies] shall in accordance with FITARA and related OMB policy:

- Ensure that IT resources are distinctly identified and separated from non-IT resources during the planning, programming, and budgeting processes in a manner that affords agency CIOs appropriate visibility and specificity to provide effective management and oversight of IT resources;
- Ensure that the agency-wide budget development process includes the CFO, CAO, and CIO in the planning, programming, and budgeting stages for programs that include IT resources (not just programs that are primarily information-and technology-oriented);
- The agency head, in consultation with the CFO, CAO, CIO, and program leadership, shall define the processes by which program leadership works with the CIO to plan an overall portfolio of IT resources that achieve program and business objectives efficiently and effectively by:
    a. Weighing potential and ongoing IT investments and their underlying capabilities against other proposed and ongoing IT investments in the portfolio; and
    b. Identifying gaps between planned and actual cost, schedule, and performance goals for IT investments and developing a corrective action plan to close such gaps;
- Ensure that the CIO approves the IT components of any plans, through a process defined by the agency head that balances IT investments with other uses of agency funding. Agencies shall also ensure that the CIO is included in the internal planning processes for how the agency uses information resources to achieve its objectives at all points in their life cycle, including operations and disposition or migration;
- Ensure that the CFO, CAO, and CIO define agency-wide policy for the level of detail of planned expenditure reporting for all transactions that include IT resources.[87]

Major IT Business Cases
OMB provides specific policy, procedural, and analytic guidelines for planning, budgeting, acquisition, and management of major IT capital investments, which is defined within the IT Budget - Capital Planning Guidance, Appendix C of the current fiscal year, in addition to general guidance issued in OMB Circular A-11 and OMB Circular A-130.

An agency's Major IT Business Case describe the justification, planning, implementation, and operations of individual capital assets included in the Agency IT Portfolio Summary and serve as key artifacts of the agency's enterprise architecture (EA) and IT capital planning processes. The Major IT Business Case is comprised of two components:

[87] OMB Circular A-130. Managing Information as a Strategic Resource. Page 8.
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

- The Major IT Business Case itself, which provides key high-level investment information to inform budget decisions, including general information and planning for resources such as staffing and personnel.
- The regular information updates to the Major IT Business Case, which provides more temporal information, related to tracking management of an investment, such as projects and activities, risks, and operational performance of the investment. This includes the CIO's responsibility to assess each Major IT Investment pursuant to 40 U.S.C. 11315(c)(2).[88]

Transition to Government-wide Acquisition Strategies and Create Accountability - Consolidate Agency Requirements

To fully leverage the Government's buying power, improve the Government's management of its information resources and drive down costs, agencies must be able to select the right size of service by pooling resources and minimizing the risk of overage charges. Therefore, effective immediately, except as provided in this policy, all covered civilian agencies shall leverage the existing Government-wide GSA mobile solution, in accordance with commercial practices and FAR Part 8.[89]

Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response

This memorandum updates a longstanding OMB policy, first implemented in 2006, to maximize federal agency use of a government-wide solution for acquiring identity protection services when needed. This memorandum requires, with limited exceptions, that when agencies need identity protection services, agencies address their requirements by using the government-wide blanket purchase agreements (BPAs) for Identity Monitoring Data Breach Response and Protection Services awarded by the General Services Administration (GSA), referred to below as the "IPS BPAs."[90]

Guidance to CFO Act Agencies on IT Working Capital Funds

Section B of this guidance is applicable to all CFO Act agencies (as defined in 31 U.S.C. §901 (b)). Under the Modernizing Government Technology (MGT) Act, all CFO Act agencies are authorized to establish an IT Working Capital Fund (WCF). IT WCFs may only be used:

- To improve, retire, or replace existing information technology systems to enhance cybersecurity of existing systems and to improve efficiency and effectiveness of the life of a given workload;
- To transition legacy information technology systems to commercial cloud computing and other innovative commercial platforms and technologies, including those serving more than one covered agency with common requirements;
- To assist and support covered agency efforts to provide adequate, risk-based, and cost-effective information technology capabilities that address evolving threats to information security;
- To reimburse funds transferred to the agency from the Technology Modernization Fund; and

[88] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Information Technology Investments. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[89] OMB M-16-20. Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services. August 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_20.pdf

[90] OMB M-16-14. Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response. July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-14.pdf

- For a program, project, or activity or to increase funds for any program, project, or activity that has not been denied or restricted by Congress.[91]

Evidence Use

Budget submissions also should include a separate section on agencies' most innovative uses of evidence and evaluation, addressing some or all of the issues below.

1. Proposing new evaluations:
    a. Low-cost evaluations using administrative data or new technology;
    b. Evaluations linked to waivers and performance partnerships;
    c. Expansion of evaluation efforts within existing programs;
    d. Systemic measurement of costs and cost per outcome.
2. Using comparative cost-effectiveness data to allocate resources
3. Infusing evidence into grant-making
4. Using evidence to inform enforcement
5. Strengthening agency evaluation capacity – agencies should have a high-level official who is responsible for program evaluation and can:
    a. Develop and manage the agency's research agenda;
    b. Conduct or oversee rigorous and objective studies;
    c. Provide independent input to agency policymakers on resource allocation and to program leaders on program management;
    d. Attract and retain talented staff and researchers, including through flexible hiring authorities such as the Intergovernmental Personnel Act; and
    e. Refine program performance measures, in collaboration with program managers and the Performance Improvement Officer (PIO).[92]

[91] OMB M-18-12. Implementation of the Modernizing Government Technology Act. February 2018. https://www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf

[92] OMB M-12-14. Use of Evidence and Evaluation in the 2014 Budget. May 2012. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2012/m-12-14_1.pdf

1.5 IT Investment Management

1.5.1 CIO Responsibilities – Laws and Executive Orders

CIOs are responsible for the processes for managing, evaluating, and assessing how well the agency is managing its IT resources. This section lists the statutory responsibilities of CIOs related to investment management. The statutory language is *directly pulled* from applicable laws and executive orders. These statutory responsibilities are then implemented through OMB guidance and guidance from other government-wide organizations. This language, along with the language in other sections under the heading "CIO Responsibilities – Laws and Executive Orders," defines the CIO role and gives the CIO their statutory mandate.

General Responsibilities
The head of each covered agency … shall ensure that the [CIO] of the agency has a significant role in—(i) the decision processes for all annual and multi-year planning, programming, budgeting, and execution decisions… and (ii) the management, governance and oversight processes related to [IT].[93]

Information Technology Investments
The Director of the [OMB] shall require in the annual information technology capital planning guidance of the [OMB] the following: That the [CIO] of each covered agency certify that information technology investments are adequately implementing incremental development, as defined in capital planning guidance issued by the [OMB].[94]

The CIO monitors the performance of information technology programs of the agency, evaluates the performance of those programs on the basis of the applicable performance measurements, and advises the head of the agency regarding whether to continue. modify. or terminate a program or project.[95]

Review
A covered agency other than the Department of Defense (I) may not enter into a contract or other agreement for information technology or information technology services, unless the contract or other agreement has been reviewed and approved by the [CIO] of the agency.[96]

A covered agency other than the Department of Defense (II) may not request the reprogramming of any funds made available for information technology programs, unless the request has been reviewed and approved by the [CIO] of the agency.[97]

---

[93] 40 U.S.C. §11319(b)(1)(A). Responsibility for Acquisitions of Information Technology. Resources, planning, and portfolio management. Additional Authorities for Chief Information Officers. https://uscode.house.gov/view.xhtml?req=(title:40%20section:11319%20edition:prelim)
[94] Ibid.
[95] 40 U.S.C. §11315. Responsibility for Acquisitions of Information Technology. Agency Chief Information Officer. https://www.law.cornell.edu/uscode/text/40/11315
[96] 40 U.S.C. §11319(b)(1)(C)(I). Responsibility for Acquisitions of Information Technology. Resources, planning, and portfolio management. Review. https://uscode.house.gov/view.xhtml?req=(title:40%20section:11319%20edition:prelim)
[97] Ibid, (II).

1.5.2 CIO Responsibilities – OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or otherwise clarifies the responsibilities of agency CIOs with regards to investment management. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with these documents is measured.

Strengthening IT Portfolio Governance
Strong oversight of spending through the use of effective investment review boards (IRBs) that include [COOs], CIOs, [CHCOs], CFOs, CAOs, PIOs, program officials, and other key executive decision makers is essential for efficient and effective IT portfolio management. Agencies with rigorous Investment Review Boards (IRBs) ensure that all stakeholder needs are addressed and that decisions are made in the best interest of the agency. Effective IRBs include the use of:

- Enterprise-wide architectures that link business and technology to ensure that IT solutions meet business requirements, as well as identify areas of waste and duplication wherever consolidation is possible; and
- Valuation methodologies used by decision makers to evaluate investments based on their value to the agency and the cost to the taxpayer.

This enables greater consistency and rigor in the process of selecting, controlling and evaluating investments an agency decides to fund, de-fund or terminate. Thus, the most advanced agencies employ their IRBs to implement effective IT solutions using savings gained from eliminating unnecessary and lower value investments, reducing operating costs, and freeing up capital to re-invest and pioneer innovative platforms, consistent with OMB guidance.[98,99]

Ongoing CIO Engagement with Program Managers
The CIO should establish and maintain a process to regularly engage with program managers to evaluate IT resources supporting each agency strategic objective. It should be the CIO and program managers' shared responsibility to ensure that legacy and on-going IT investments are appropriately delivering customer value and meeting the business objectives of programs.[100]

Visibility of IT Planned Expenditure Reporting to CIO
The CFO, CAO, and CIO should define agency-wide policy for the level of detail of planned expenditure reporting for all transactions that include IT resources.[101]

CIO Defines IT Processes and Policies
The CIO defines the development processes, milestones, review gates, and the overall policies for all capital planning, enterprise architecture, and project management and reporting for IT resources. At a

[98] OMB M-13-09. Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management. March 2013. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-09.pdf
[99] OMB M-15-14. Management and Oversight of Federal Information Technology. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf. & 40 U.S.C. §11319. Responsibility for Acquisitions of Information Technology. https://uscode.house.gov/view.xhtml?req=(title:40%20section:11319%20edition:prelim)
[100] Ibid, Common Baseline E1.
[101] Ibid, Common Baseline F1.

minimum, these processes shall ensure that the CIO certifies that IT resources are adequately implementing incremental development (as defined in the below definitions). The CIO should ensure that such processes and policies address each category of IT resources appropriately—for example, it may not be appropriate to apply the same process or policy to highly customized mission-specific applications and back office enterprise IT systems depending on the agency environment. These policies shall be posted publicly at agency.gov/digital strategy, included as a downloadable dataset in the agency's Public Data Listing, and shared with OMB through the Integrated Data Collection (IDC). For more information, see OMB Circular A-130: Management of Information Resources.[102]

CIO Role on Program Governance Boards
[To ensure] early matching of appropriate IT with program objectives, the CIO shall be a member of governance boards that include IT resources (including "shadow IT" or "hidden IT"—see definitions), including bureau IRBs. The CIO shall notify OMB of all governance boards [of which] the CIO is a member and at least annually update this notification.[103]

Shared Acquisition and Procurement Responsibilities
The CIO reviews all cost estimates of IT related costs and ensures all acquisition strategies and acquisition plans that include IT apply adequate incremental development principles.[104]

CIO Role in Recommending Modification, Termination, or Pause of IT Projects or Initiatives
The CIO shall conduct TechStat reviews or use other applicable performance measurements to evaluate the use of the IT resources of the agency. The CIO may recommend to the agency head the modification, pause, or termination of any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation, within the terms of the relevant contracts and applicable regulations.[105]

CIO Role in Review and Approval of Acquisition Strategy and Acquisition Plan
Agencies shall not approve an acquisition strategy or acquisition plan (as described in FAR Part 724) or interagency agreement (such as those used to support purchases through another agency) that includes IT without review and approval by the agency CIO. For contract actions that contain IT without an approved acquisition strategy or acquisition plan, the CIO shall review and approve the action itself. The CIO shall primarily consider the following factors when reviewing acquisition strategies and acquisition plans:

- Appropriateness of contract type;
- Appropriateness of IT related portions of statement of needs or statement of work;
- Appropriateness of above with respect to the mission and business objectives supported by the IT strategic plan; and
- Alignment with mission and program objectives in consultation with program leadership.[106]

[102] Ibid, Common Baseline G1.
[103] Ibid, Common Baseline H1.
[104] Ibid, Common Baseline I1.
[105] Ibid, Common Baseline J1.
[106] Ibid, Common Baseline K1, J1.

CIO Role in Approval of Reprogramming
The CIO must approve any movement of funds for IT resources that requires Congressional notification.[107]

Purchasing to Support Telework
Agency CIOs, in coordination with CAOs shall develop or update policies on purchasing computing technologies and services to enable and promote continued adoption of telework. At the same time, purchasing policies must address the information security threats raised by use of technologies associated with telework. Given the unique mission and nature of each agency, agencies are granted broad discretion in formulating telework purchasing policies to best suit their unique needs. At a minimum, however, agency policies must address the following:

- Selecting and acquiring information technology that best fits the needs of the Federal Government, and is technology and vendor neutral in acquisitions;
- Determination of allowable IT products and services, to include remote access servers, client devices, and internal resources accessible through remote access;
- Prioritizing use of government-wide and agency-wide contracts, to the maximum extent possible, for new acquisitions and renewal of services to leverage the government's buying power;
- Deploying new and modernizing existing agency IT systems and infrastructure to support agency teleworking requirements;
- Compliance of all devices and infrastructure with federal security and privacy requirements; and
- Proper disposal of devices no longer in use to ensure protection of sensitive information.[108]

1.5.3 Agency IT Authorities – OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or clarifies IT authorities assigned to agencies. This language directly or indirectly tasks the CIO with duties or responsibilities pertaining to IT investment management. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with policies is measured.

Role
Agency shall:

1. Conduct definitive technical, cost, and risk analyses of alternative design implementations, including consideration of the full life cycle costs of IT products and services, including but not limited to, planning, analysis, design, implementation, sustainment, maintenance, re-competition, and retraining costs, scaled to the size and complexity of individual requirements; and

[107] Ibid, Common Baseline L1.
[108] OMB M 11-20. Implementing Telework Enhancement Act of 2010 IT Purchasing Requirements. April 2011. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-20.pdf

2. Ensure that all acquisition strategies, plans, and requirements (as described in FAR Part 7), or interagency agreements (such as those used to support purchases through another agency) that include IT are reviewed and approved by the purchasing agency's CIO. purchases through another agency) that include IT are reviewed and approved by the purchasing agency's CIO.[109]

IT Investment Management

Agencies are responsible for establishing a decision-making process that shall cover the life of each information system and include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the IT investments. Agencies shall designate IT investments according to relevant statutes, regulations, and guidance in OMB Circular A-11, and execute processes commensurate with the size, scope, duration, and delivery risk of the investment. The IT investment processes shall encompass planning, budgeting, procurement, management, and assessment. For further guidance related to investment planning, refer to OMB Circular A-11, including the Capital Programming Guide.[110]

Information Management and Access

Agencies shall:

1. Incorporate the following steps, as appropriate, in planning, budgeting, governance, and other policies:
    a. Federal information is properly managed throughout its life cycle, including all stages through which the information passes, such as: creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition;
    b. Federal information is managed with clearly designated roles and responsibilities to promote effective and efficient design and operation of information resources management processes within their agency.
2. Establish policies, procedures, and standards that enable data governance so that information is managed and maintained according to relevant statute, regulations, and guidance.
3. Collect or create information in a way that supports downstream interoperability among information systems and streamlines dissemination to the public, where appropriate, by creating or collecting all new information electronically by default, in machine-readable open formats, using relevant data standards, that upon creation includes standard extensible metadata in accordance with OMB guidance.[111]

Information Technology Investments

Agencies must submit information on their respective information technology (IT) investment portfolios, using the required formats, as applicable, as stated in the [annual] IT Budget – Capital Planning Guidance. This section provides general guidance related to reporting on IT and the templates used to collect that information. Section 25.5 provides electronic links to the definitions and specific reporting instructions and exhibits related to budgeting for investments in IT.[112]

---

[109] OMB Circular A-130. Managing Information as a Strategic Resource. Page 14. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[110] Ibid.

[111] Ibid.

[112] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Section 55.1. 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

Reporting

As part of the Budget process, OMB is required to develop and oversee a process for IT budgeting and portfolio management, with a detailed focus on all major capital investments, to include "analyzing, tracking, and evaluating the risks, including information security risks, and results of all major capital investments made by an executive agency for information systems." 40 U.S.C. 11302. OMB also is responsible for IT Portfolio oversight (44 U.S.C. 3602), i.e., the use of information technologies to enhance access of information and delivery of services; and to increase the effectiveness, efficiency, service quality, or transformation of government operations.[113]

Data Center Consolidation

The head of each covered agency, assisted by the CIO of the agency, is required to submit to OMB annually 1) a comprehensive inventory of the data centers owned, operated, or maintained by or on behalf of the agency, and 2) a multi-year strategy to achieve the consolidation and optimization of these data centers. Each agency, under the direction of its CIO, must submit quarterly updates on their progress towards activity completion, consolidation & optimization metrics, and cost savings realized through the implementation of their strategy.[114]

Investment Management Reporting

An agency's IT investment management and reporting of IT investments must clearly demonstrate that each investment is needed to help meet the agency's strategic goals and mission and show how governance processes are used to plan, select, develop, implement, and operate those IT investments. Furthermore, each IT investment should demonstrate the enabling and improvement of mission and program performance by providing meaningful data. Agencies demonstrate the IT Investment requirements and governance processes through Agency Major IT Business Cases, supporting documentation, Information Resources Management Strategic Plan, Enterprise Roadmap, and Agency IT Portfolio Summary submissions. The agency must further demonstrate how the investment supports a business line or enterprise service performance goal as documented in the agency's enterprise architecture (EA), and annual Enterprise Roadmap submission to OMB.[115]

Baseline Management

[OMB M-10-27 Information Technology Investment Baseline Management Policy memorandum] provides policy direction regarding development of agency IT investment baseline management policies and defines a common structure for IT investment baseline management policy. Baselined plans act as a guide throughout the life of an investment to provide a basis for measuring performance, identify who is accountable for the deliverables, describe the implementation approach and interdependencies, identify key decisions, and embed quality

[113] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Section 55.2. 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[114] OMB M-19-19. Update to Data Center Optimization Initiative (DCOI). 6/25/2019. https://datacenters.cio.gov/assets/files/m_19_19.pdf

[115] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Section 55.4. 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

assurance and reviews. Ultimately, baseline management demonstrates that a project is under financial and managerial control.

To provide a cohesive policy towards baseline management, this memorandum integrates the requirements in OMB Circular A-11, Part 7, and Federal Acquisition Regulation Subpart 34.202 with Federal IT Dashboard practices and guidance. This policy only addresses the establishment, management, and change to investment baselines. Agencies should reference other OMB requirements, including Circular A-130 and the Capital Programming Guide, to describe full lifecycle management of IT capital investments.

Agencies [should have created or updated] existing IT investment baseline management policies within 90 days of issuance of this policy and develop training plans for personnel with investment oversight and program management responsibilities that at a minimum address the policies outlined in Appendix A of this memorandum.

Appendix A. Per FAR Subpart 34.2 and OMB's Capital Programming Guide, a supplement to Circular A-11, Part 7, agencies shall implement an Integrated Baseline Review (IBR) or baseline validation process as part of an overall investment risk management strategy.

Agency policy shall address: (I) establishing an investment baseline; (II) rebase lining an investment; (III) notifying OMB of new and changed baselines; (IV) managing and monitoring baselines via the use of performance management systems, (V) Federal IT Dashboard reporting requirements; and (VI) policy specific for Major IT Programs of the Department of Defense.[116]

[116] OMB M-10-27. Information Technology Investment Baseline Management Policy. 6/28/2010. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-27.pdf

1.6 Information Security and Privacy

1.6.1 CIO Responsibilities – Laws and Executive Orders

CIOs are responsible for establishing, implementing, and ensuring compliance with an agency-wide information security program. This section lists the statutory responsibilities of CIOs related to information security and privacy. The statutory language is *directly pulled* from applicable laws and executive orders. These statutory responsibilities are then implemented through OMB guidance and guidance from other government-wide organizations. This language, along with the language in other sections under the heading "CIO Responsibilities - Laws and Executive Orders," defines the CIO role and gives the CIO their statutory mandate.

Federal Information Security Modernization Act
Under the Federal Information Security Modernization Act (FISMA),[117] the CIO must designate a senior official in charge of information security. In most cases, that official is the agency's Chief Information Security Officer (CISO) and works closely with the CIO to protect and secure the information resources of the agency.

Privacy Act Implementation
The publication of appropriate routine uses is required under the Privacy Act and thus would be necessary in order to disclose information for the purpose of executing an agency's obligations to effectively manage and report a breach under FISMA. Disclosures pursuant to a routine use are permissive, not mandatory.[118]

1.6.2 CIO Responsibilities – OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or otherwise clarifies the responsibilities of agency CIOs with regards to information security and privacy. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with policies is measured.

Personal Identifiable Information (PII) Breach Notification
The agency's [SAOP] as well as other senior agency officials, managers, and staff who help evaluate the risk of harm to individuals potentially affected by a breach are responsible for breach notification. In addition, sections of this Memorandum are relevant for an agency's [CIO], Senior Agency Information Security Officers (e.g., [CISO]), and other information technology (IT) and cybersecurity staff who participate in breach response activities.

> **Contracts and Contractor Requirements for Breach Response**
> In addition, the SAOP and CIO shall ensure that the agency's breach response plan and system security authorization documentation clearly define the roles and responsibilities of contractors

[117] Federal Information Security Modernization Act of 2014 (FISMA). https://www.congress.gov/bill/113th-congress/senate-bill/2521/text
[118] 5 U.S.C. § 552a(b)(3). The Privacy Act of 1974. https://www.cia.gov/library/readingroom/docs/pa.pdf

that operate Federal information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII on behalf of the agency.

Identifying Logistical and Technical Support to Respond to a Breach
When identifying technical support to respond to a breach, the CIO shall identify technical remediation and forensic analysis capabilities that exist within the agency and which offices are responsible for maintaining those capabilities. Depending on the size, missions, and structure of each agency, the CIO may find the necessary expertise and technical support within the agency. As a part of this process, however, the CIO may identify gaps in the agency's technical capabilities and therefore should communicate with the CAO and other agency officials on the need to enter into contracts or to explore other options for ensuring that certain functions are immediately available during a time-sensitive response. Additionally, while the SAOP might not lead the technical team, the SAOP should understand the ability of the agency to gather, analyze, and preserve the evidence necessary to support an investigation and identify and assess the risk of harm to potentially affected individuals. The CIO, in coordination with the SAOP, should also consider whether other Federal agencies can support the agency in the event of a breach. Agencies may request technical assistance from US-CERT. In addition, GSA may have BPAs and other guidance for agencies to procure technical services to assist with responding to a breach. (Note: for a complete list of all SAOP requirements see the full memo).[119]

Trusted Internet Connections (TIC) Agency Implementation
[For] TIC program updates to achieve the goal of diversifying technology options for agencies while retaining strong protections for Federal systems and information, OMB, DHS, and the agencies themselves, need to have details of the technologies and defenses deployed across Federal networks. As such, agency CIOs shall maintain an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection in the event OMB, DHS, or others request this information to assist with government-wide cybersecurity incident response or other cybersecurity matters.

Within one year of the release of this memorandum, agencies shall complete updates to their own network and system boundary policies to reflect this memorandum, including guidance regarding potential pilots. Agencies will identify which TIC Use Case will be allowed for the agency. OMB and DHS will track agency implementation through the Federal Information Security Modernization Act of 2014 (FISMA) reporting.[120]

Cybersecurity Strategy and Implementation Plan (CSIP)
The CSIP is the result of a comprehensive review of the Federal Government's cybersecurity policies, procedures, and practices by the Sprint Team[121]. The goal was to identify and address critical cybersecurity gaps and emerging priorities and make specific recommendations to address those gaps

[119] OMB M-17-12. Preparing for and Responding to a Breach of Personally Identifiable Information. 1/3/2017. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf
[120] OMB M-19-26. Update to the Trusted Internet Connections (TIC) Initiative. 9/19/2019. https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf
[121] A 30-day Cybersecurity Sprint Team led by OMB and was comprised of representatives from the National Security Council (NSC), the Department of Homeland Security (DHS), the Department of Defense (DoD), and other Federal civilian and defense agencies.

and priorities. The CSIP will strengthen Federal civilian cybersecurity through the following five objectives:

1. Prioritized Identification and Protection of high value information and assets;
2. Timely Detection of and Rapid Response to cyber incidents;
3. Rapid Recovery from incidents when they occur, and Accelerated Adoption of lessons learned from the Sprint assessment;
4. Recruitment and Retention of the most highly qualified Cybersecurity Workforce talent the Federal Government can bring to bear; and
5. Efficient and Effective Acquisition and Deployment of Existing and Emerging Technology.[122]

Specifically, the CSIP's key actions include:

- All agencies will continue to identify their high value assets (HVAs) and critical system architecture in order to understand the potential impact to those assets from a cyber incident and ensure robust physical and cybersecurity protections are in place. The identification of HVAs will be an ongoing activity due to the dynamic nature of cybersecurity risks.
- All agencies will improve the identity and access management of user accounts on Federal information systems to drastically reduce vulnerabilities and successful intrusions.
- CIOs and [CISO] will also have direct responsibility and accountability for implementation of the CSIP, consistent with their role of ensuring the identification and protection of their agency's critical systems and information.[123]

Telework Security
Agency CIOs must identify a technical point of contact to DHS (FISMA.FNS@dhs.gov) to aid with the implementation of telework security requirements. This point of contact will serve as a technical manager and must have operational and technical expertise to implement the Act within the agency.[124]

1.6.3 Agency IT Authorities – Laws and Executive Orders

This section consists of IT authorities assigned to agencies in laws and executive orders which directly or indirectly task the CIO with duties or responsibilities pertaining to information security and privacy. The statutory language is *directly pulled* from the applicable laws and executive orders. In most cases, the heads of agencies delegate all IT management responsibilities to the CIO, but some functions are explicitly assigned to more than one person (e.g. the CIO in consultation with the CFO). See individual agency policies to determine how instances of dual responsibility are implemented and executed, and what tasks (if any) are required of the agency head but not delegated to the CIO.

[122] OMB M-16-04. Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. 10/30/2015. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf
[123] Ibid.
[124] OMB M-11-27. Implementing the Telework Enhancement Act of 2010: Security Guidelines. 7/15/2011. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-27.pdf

The E-Government Act Requires agencies to conduct a [privacy impact assessment (PIA)][125] before: (i) developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information that –(I) will be collected, maintained, or disseminated using IT; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.[126]

Federal Agency Responsibilities
The head of each agency shall¬ (1) be responsible for¬ (A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of¬ (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency [...]."[127]

1.6.4 Agency IT Authorities – OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or clarifies IT authorities assigned to agencies. This language directly or indirectly tasks the CIO with duties or responsibilities pertaining to information security and privacy. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with policies is measured.

Privacy
The following excerpt is from the Privacy and Information Security section in OMB A-130.[128]

Agencies shall:

- Establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks;
- Designate an SAOP who has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and

[125] A PIA is an analysis of how personal identifiable information (PII) is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.
[126] 44 U.S.C. § 3501. Section 208(b). E-Government Act of 2002. Privacy Provisions. https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
[127] 44 U.S.C. § 3554. Title 44 Public Printing and Documents. Federal Agency Responsibilities. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title44-section3554&num=0&edition=prelim
[128] OMB Circular A-130. Managing Information as a Strategic Resource. Page 16. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

information systems, developing and evaluating privacy policy, and managing privacy risks at the agency;
- Ensure that the SAOP and the agency's privacy personnel closely coordinate with the agency CIO, senior agency information security officer, and other agency offices and officials, as appropriate.

Information Security
To provide proper safeguards, agencies shall ensure that the CIO designates a senior agency information security officer to develop and maintain an agency-wide information security program in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).[129]

Reporting Pursuant to OMB Circular No. A-130, Appendix I
Appendix I of OMB Circular No. A-130 establishes minimum requirements for Federal information security programs, assigns Federal Agency responsibilities for the security of information and information systems, and links Agency information security programs and Agency management control systems established in accordance with OMB Circular No. A-123. The appendix also establishes requirements for Federal privacy programs, assigns responsibilities for privacy program management, and describes how agencies must take a coordinated approach to implementing information security and privacy controls.[130]

[Security Budget Estimates]
[Agency budget estimates] should reflect a comprehensive understanding of OMB security policies, such as OMB Circular A-130, and National Institute of Standards and Technology (NIST) guidance, including compliance with the Federal Information Security Modernization Act, and OMB Memorandum M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements, by:[131]

- Reflecting the cost considerations used to calculate IT security costs (see section 51.19);
- Demonstrating that the costs of security controls are understood and are explicitly incorporated in the life-cycle planning of the overall system, including the additional costs of employing standards and guidance more stringent than those issued by NIST;
- Demonstrating how the agency ensures that risks are understood and continually assessed;
- Demonstrating how the agency ensures that the security controls are commensurate with the risk and magnitude of harm;
- Identifying additional security controls for systems that promote or permit public access, other externally accessible systems, and those that are interconnected with systems over which program officials have little or no control; and
- Demonstrating how the agency ensures the effective use of security and privacy controls, as well as authentication tools to protect privacy for those systems that promote or permit public access.

---

[129] OMB Circular A-130. Managing Information as a Strategic Resource. Page 18. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[130] OMB M-16-17. OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. 7/15/2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf
[131] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Management Improvement Initiatives and Policies. Section 31.8. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

Privacy

Privacy Risk

Once the agency determines that an information system contains Personal Identifiable Information (PII), the agency must then consider the privacy risks and the associated risk to agency operations, agency assets, individuals, other organizations, and the Nation. When considering privacy risks, the agency must consider the risks to an individual or individuals associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their PII.[132]

Privacy Impact Assessments (PIA)

As a general matter, an agency must conduct a privacy impact assessment (PIA) under section 208(b) of the E-Government Act of 2002, absent an applicable exception under that section, when the agency develops, procures, or uses information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. Moreover, a PIA is not a time-restricted activity that is limited to a particular milestone or stage of the information system or PII life cycles. Rather, the privacy analysis must continue throughout the information system and PII life cycles.[133]

Risk Management Framework

Agencies' privacy programs have responsibilities under the Risk Management Framework. The Risk Management Framework provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the information system development life cycle. Agencies should refer to OMB Circular No. A-130 for more detailed guidance regarding the role of agencies' privacy programs under the Risk Management Framework.[134] The CIO Council and the Cyber-ERM Community of Interest updated the Federal ERM Playbook and added a chapter on Cyber-ERM Integration. The chapter provides foundations of Information Security and Cybersecurity that identifies integration points with physical security, addresses privacy, cyber supply-chain risk, incorporates NIST standards, addresses FISMA audits and "enterprise" scope, and other information related to terms, roles, responsibilities and communication flow.

[Privacy Budget Estimates]

[Agency budget estimates] should reflect the Administration's commitment to privacy and consistent with OMB Circular A-130, should include a description of [the] agency's privacy program and the resources required to ensure compliance with applicable privacy requirements,

---

[132] OMB M-16-17. OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. 7/15/2016. Page 44.
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

[133] Ibid.

[134] OMB M-16-17. OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. 7/15/2016. Page 46.
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

develop and evaluate privacy policy, and manage privacy risks. At a minimum, [the] estimate should:

- Demonstrate [awareness] of applicable privacy requirements and has fully assessed he cost to the agency for ensuring compliance with those requirements and managing privacy risks;
- [Reflect the inventory] of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information; and
- [Reflect the consideration of privacy] continuous monitoring strategy and the resources and associated costs required to ensure that privacy controls are effectively monitored on an ongoing basis at an assessment frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.[135]

Designation of the [SAOP]
The head of the agency is ultimately responsible for ensuring that privacy interests are protected and that PII is managed responsibly within the agency.

To ensure that agencies effectively carry out the privacy-related functions described in law and OMB policies, Executive Order 13719 requires the head of each agency to designate or re-designate an SAOP who has agency-wide responsibility and accountability for the agency's privacy program.[136]

[SAOP Reporting Requirements]
Given the importance of privacy, as highlighted in policies such as OMB Circular A-130, Managing Information as a Strategic Resource, and OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, agencies must take appropriate measures to comply with privacy requirements and manage privacy risks.

- SAOPs are required to report annually and must submit each of the following items as separate documents through CyberScope:[137]
    - The agency's privacy program plan;
    - A description of any changes made to the agency's privacy program during the reporting period, including changes in leadership, staffing, structure, and organization;
    - The agency's breach response plan;
    - The agency's privacy continuous monitoring strategy;
    - The Uniform Resource Locator (URL) for the agency's privacy program page, as well as the URL for any other sub-agency, component, and/or program-specific privacy program pages; and,
    - The agency's written policy to ensure that any new collection or use of Social Security numbers (SSNs) is necessary, along with a description of any steps the

[135] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Section 31.8. 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf
[136] OMB M-16-24. Role and Designation of Senior Agency Officials for Privacy. 9/15/2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_24_0.pdf
[137] OMB M-20-04. Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements. 11/19/2019. https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf

agency took during the reporting period to explore alternatives to the use of SSNs as a personal identifier.

High Value Asset (HVA) Program

While the HVA initiative is compatible with and must leverage existing policies and guidelines regarding IT assets, such as those listed above, agencies must also consider their HVA risks from a strategic enterprise-wide perspective. As such, the agency HVA process described herein requires explicit consideration of the following factors:

- Agencies' assessment of risk should not be limited to IT and other technical considerations. HVA risk assessments should incorporate operational, business, mission, and continuity considerations. All key stakeholders of an agency, to include the CFO, CAO, [SAOP], mission, business, and policy owners as well as the CIO and [CISO] organizations, should be engaged in evaluating HVA risks.
- Agencies' assessment of risk should consider not just the risk that an HVA poses to the agency itself, but also the risk of interconnectivity and interdependencies leading to significant adverse impact on the functions, operations, and mission of other agencies.

The Agency HVA Process

Agencies must take a strategic enterprise-wide view of risk that accounts for all critical business and mission functions when identifying HVAs.[138] HVAs are those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification or destruction could cause significant impact to the United States' nations security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. Agencies [must establish] appropriate governance of HVA activities across the enterprise and should integrate HVA remediation activities into agency planning, programming, budgeting, and execution processes. These efforts must align with OMB policy, Federal law and regulations, Federal standards and guidelines, and agency policies, processes, and procedures.[139] For complete details on the agency HVA process see the memo.

Information Security Management

Information Security and Privacy Program Oversight and FISMA Reporting Requirements

[OMB and DHS use] CIO and IG metrics to compile the Annual FISMA Report to Congress and may use this reporting to compile agency-specific or government-wide risk management assessments as part of an ongoing effort in support of Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

At a minimum, CFO Act agencies must update their CIO Metrics quarterly and non-CFO Act agencies must update their CIO metrics on a semiannual basis. Reflecting the Administration's shift from compliance to risk management, as well as the guidance and requirements outlined in OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program, and Binding Operational Directive 18-02, Securing High Value Assets, CIO Metrics are not limited to assessments and capabilities within [NIST] security

[138] OMB M-17-09. Management of Federal High Value Assets. 12/9/2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf

[139] Ibid.

baselines, and agency responses should reflect actual implementation levels. Although FISMA requires an annual IG assessment, OMB strongly encourages CIOs and IGs to discuss the status of information security programs throughout the year.

Cybersecurity Reporting: Overview and Purpose

On May 11, 2017, the President signed the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which outlines a number of actions to enhance cybersecurity across Federal agencies and critical infrastructure partners. Section 1 of the Executive Order reinforces the Federal Information Security Modernization Act of 2014 (FISMA) by holding agency heads accountable for managing the cybersecurity risks to their enterprises. This Memorandum provides implementing guidance on actions required in Section 1 of the Executive Order.[140]

Policy to Require Secure Connections across Federal Websites and Web Services

OMB Memorandum M-15-13 requires that all publicly accessible Federal websites and web service only provide service through a secure connection. The strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS).

[To] promote the efficient and effective deployment of HTTPS, the timeframe for [compliance is outlined below]. This Memorandum requires that Federal agencies deploy HTTPS on their domains using the following guidelines.[141]

- Newly developed websites and services at all Federal agency domains or subdomains must adhere to this policy upon launch.
- For existing websites and services, agencies should prioritize deployment using a risk-based analysis. Web services that involve an exchange of personally identifiable information (PII), where the content is unambiguously sensitive in nature, or where the content receives a high-level of traffic should receive priority and migrate as soon as possible.
- Agencies [should have made] all existing websites and services accessible through a secure connection (HTTPS-only, with HTTP Strict Transport Security (HSTS)) by December 31, 2016.
- The use of HTTPS is encouraged on intranets, but not explicitly required.

FISMA Reporting and Agency Privacy Management

OMB requires that the head of each agency submit, as part of the agency's annual report, a signed electronic copy of an official letter to CyberScope providing a comprehensive overview reflecting his or her assessment of the adequacy and effectiveness of information security

[140] OMB M-17-25. Reporting Guidance for Reporting Progress on Executive Order on Strengthening the Cybersecurity of Federal Network and Critical Infrastructure. 5/19/2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf

[141] OMB M-15-13. Policy to Require Secure Connections across Federal Websites and Web Services. 6/8/2015. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2015/m-15-13.pdf

policies, procedures, and practices, and compliance with the requirements of the Federal Information Security Modernization Act (FISMA) for the agency.[142]

Below are activities explicitly outlined in FISMA:

> CIO/CISO Interviews
> DHS will [conduct] annual interviews with agencies' CIO and [CISO] based on their agency's security posture. Each interview session has three distinct goals:
>
> - Assessing progress towards the administration cybersecurity priorities and other FISMA compliance and challenges;
> - Identifying security best practices and raising awareness of FISMA reporting requirements; and
> - Establishing meaningful dialogue with the agency's senior leadership.
>
> Submit Privacy Documents
> As part of the annual report, Senior Agency Officials for Privacy are to submit the following documents through CyberScope:
> - Description of the agency's privacy training for employees and contractors;
> - Breach notification policy;
> - Progress update on eliminating unnecessary use of Social Security Numbers; and
> - Progress update on the review and reduction of holdings of personally identifiable information.[143]
>
> OMB [requires] agencies to submit these four privacy documents whether or not the documents have changed from versions submitted in previous years.

Information Security Continuous Monitoring (ISCM)
To fully implement ISCM across the Government, agencies shall: 1) Develop and maintain, consistent with existing statutes, OMB policy, NIST guidelines and the CONOPS, an ISCM strategy, and establish an ISCM program that: a. Provides a clear understanding of organizational risk and helps officials set priorities and manage such risk consistently throughout the agency; and b. Addresses how the agency [conducts] ongoing authorizations of information systems and the environments in which those systems operate, including the agency's use of common controls.[144]

Federal Information Security Management Act (FISMA) Agency Reporting Activities
To comply with this guidance, [agencies carry out] the following activities:

1. Establish monthly data feeds to CyberScope;
2. Respond to security posture questions; and

---

[142] OMB M-14-04. Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. 11/18/2013.
https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf
[143] Ibid.
[144] OMB M-14-03. Enhancing the Security of Federal Information and Information Systems. 11/18/2013.
https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

3. Participate in CyberStat accountability sessions and agency interviews.

CyberScope is the platform for the FISMA reporting process. Agencies should note that a Personal Identity Verification card, compliant with Homeland Security Presidential Directive 12 is required for access to CyberScope. No FISMA submissions [are] accepted outside of CyberScope. For information related to CyberScope, please visit: http://max.omb.gov.[145] CIOs, Inspectors General, and Senior Agency Officials for Privacy [all] report through CyberScope. Micro agencies[146] [also] report using this automated collection tool.[147]

Agency Implementation of Identify Credentialing and Access Management (ICAM)
[In] line with the Federal Government's updated approach to modernization, it is essential that agencies' ICAM strategies and solutions shift from the obsolete Levels of Assurance (LOA) model towards a new model informed by risk management perspectives, the Federal resource accessed, and outcomes aligned to agency missions. To set the foundation for identity management and its usage to access physical and digital resources, agencies must implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3 and any successive versions (hereafter referred to as NIST SP 800-63).[148]

[Telework Security Guidelines]
Agencies are expected to implement security telework policies to best suit their unique needs. At a minimum, agency policies must comply with FISMA requirements and address the following:[149]

- Controlling access to agency information and information systems;
- Protecting agency information (including personally identifiable information) and information systems;
- Limiting the introduction of vulnerabilities;
- Protecting information systems not under the control of the agency that are used for teleworking;
- Safeguarding wireless and other telecommunications capabilities that are used for teleworking; and
- Preventing inappropriate use of official time or resources that violates subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

[Telework Security Point of Contact]
Agency CIOs must identify a technical point of contact to DHS (FISMA.FNS@dhs.gov) to aid with the implementation of telework security requirements. This point of contact will serve as a technical

[145] The website MAX.gov is only accessible to federal employees.
[146] According to M-11-33, micro agencies are agencies employing 100 or fewer full time equivalents (FTEs).
[147] OMB M-11-33. FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. 9/14/2011. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-33.pdf
[148] OMB M-19-17. Enabling Mission Delivery through Improved Identity, Credential, and Access Management, 5/21/2019. https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
[149] OMB M 11-27. Implementing the Telework Enhancement Act of 2010: Security Guidelines. 07/15/2011. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-27.pdf

manager and must have operational and technical expertise to implement the [Telework Enhancement Act] within the agency.[150]

[150] Ibid.

1.7 Architecture

1.7.1 CIO Responsibilities – Laws and Executive Orders

This section lists the statutory responsibilities of CIOs related to their agency's architecture. The statutory language is *directly pulled* from applicable laws and executive orders. These statutory responsibilities are then implemented through OMB guidance and guidance from other government-wide organizations. This language, along with the language in other sections under the heading "CIO Responsibilities - Laws and Executive Orders," defines the CIO role and gives the CIO their statutory mandate.

Definition
[The] term "information technology architecture," with respect to an executive agency, means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals.

General Responsibilities
The [CIO] of an executive agency is responsible for:

- Providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this subtitle, consistent with chapter 35 of title 44 and the priorities established by the head of the executive agency;
- Developing, maintaining, and facilitating the implementation of a sound, secure, and integrated information technology architecture for the executive agency; and
- Promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency.[151]

1.7.2 CIO Responsibilities – OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or otherwise clarifies the responsibilities of agency CIOs with regards to their agency's architecture. See sections on OMB Memoranda and OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with policies is measured.

Enterprise Architecture
Agencies shall develop an enterprise architecture (EA) that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture. The agency's EA shall align to their IRM Strategic Plan. The EA should incorporate agency plans for significant upgrades, replacements, and

[151] 40 U.S.C. Subtitle III. Chapter 113. Subchapter II. § 11315. Title 40 Public Buildings, Property and Works. https://www.govinfo.gov/content/pkg/USCODE-2011-title40/pdf/USCODE-2011-title40-subtitleIII-chap113-subchapII-sec11315.pdf

disposition of information systems when the systems can no longer effectively support missions or business functions.[152]

[152] OMB Circular A-130.Managing Information as a Strategic Resource. Page 6. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

1.8 Information Resources and Data

1.8.1 Agency IT Authorities – Laws and Executive Orders

This section consists of IT authorities assigned to agencies in laws and executive orders which directly or indirectly task the CIO with duties or responsibilities pertaining to information resources and data. The statutory language is *directly pulled* from the applicable laws and executive orders. In most cases, the heads of agencies delegate all IT management responsibilities to the CIO, but some functions are explicitly assigned to more than one person (e.g. the CIO in consultation with the CFO). See individual agency policies to determine how instances of dual responsibility are implemented and executed, and what tasks (if any) are required of the agency head but not delegated to the CIO.

Agency Commitments to Records Management Reform
The head of each agency shall:

- Ensure that the successful implementation of records management requirements in law, regulation, and this memorandum is a priority for senior agency management;
- Ensure that proper resources are allocated to the effective implementation of such requirements; and within 30 days of the date of this memorandum, [should have designated] in writing to the Archivist of the United States (Archivist), a senior agency official to supervise the review required by subsection (b) of this section, in coordination with the agency's Records Officer, [CIO], and General Counsel.

Within 120 days of the date of this memorandum, each agency head [should have submitted] a report to the Archivist and the Director of [OMB] that:[153]

- Describes the agency's current plans for improving or maintaining its records management program, particularly with respect to managing electronic records, including email and social media, deploying cloud-based services or storage solutions, and meeting other records challenges;
- Identifies any provisions, or omissions, in relevant statutes, regulations, or official NARA guidance that currently pose an obstacle to the agency's adoption of sound, cost-effective records management policies and practices; and
- Identifies policies or programs that, if included in the Records Management Directive required by section 3 of this memorandum or adopted or implemented by NARA, would assist the agency's efforts to improve records management.

1.8.2 Agency IT Authorities – OMB Guidance

This section consists of language from OMB guidance that further demarcates, expands upon, or clarifies IT authorities assigned to agencies. This language directly or indirectly tasks the CIO with duties or responsibilities pertaining to information resources and data. See sections on OMB Memoranda and

[153]44 U.S.C. Chapter 31. § 3101. Title 44 Public Printing and Documents.
https://uscode.house.gov/view.xhtml?path=/prelim@title44/chapter31&edition=prelim

OMB Circulars for more information about these forms of OMB guidance. See sections on OIG and GAO to review how compliance with policies is measured.

Policy
Agencies shall establish a comprehensive approach to improve the acquisition and management of their information resources by: performing information resources management activities in an efficient, effective, economical, secure, and privacy-enhancing manner; focusing information resources planning to support their missions; implementing an IT investment management process that links to and supports budget formulation and execution; and rethinking and restructuring the way work is performed before investing in new information systems.[154]

Inventory
Agencies shall:

- Maintain an inventory of the agency's major information systems, information holdings, and dissemination products, at the level of detail that OMB and the agency determine is most appropriate for overseeing and managing the information resources; and
- Maintain an inventory of the agency's information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency functions.[155]

Information Management
[Agencies] shall:

- Continually facilitate adoption of new and emerging technologies, and regularly assess the following throughout the life of each information system: the inventory of the physical and software assets associated with the system; the maintainability and sustainability of the information resources and infrastructure supporting the system; and actively determine when significant upgrades, replacements, or disposition is required to effectively support agency missions or business functions and adequately protect agency assets.[156]

Risk Management
[Agencies] shall:

- Consider information security, privacy, records management, public transparency, and supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed;
- Develop plan, in consultation with CIOs, Senior Agency Officials for Records Management (SAORMs), and Senior Agency Officials for Privacy (SAOPs), for information systems and

[154] OMB Circular A-130. Managing Information as a Strategic Resource. Page 4. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[155] OMB Circular A-130. Managing Information as a Strategic Resource. Page 5. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[156] Ibid.

components that cannot be appropriately protected or secured and ensure that such systems are given a high priority for upgrade, replacement, or retirement.[157]

Records Management
Agencies shall:

- Designate a [SAORM] who has overall agency-wide responsibility for records management;
- Ensure agency records managed by the SAORM are treated as information resources and follow the requirements in this Circular.[158]

Data Management

Data Quality Plan
Agencies that have determined they are subject to the DATA Act reporting must develop and maintain a Data Quality Plan that considers the incremental risks to data quality in Federal spending data and any controls that would manage such risks in accordance with OMB Circular No. A-123. The purpose of the Data Quality Plan is to identify a control structure tailored to address identified risks.[159]

Improving Data Quality
Recognizing that the value of data as a Federal asset hinges on the reliability, validity and overall quality of the data itself, and consistent with OMB Circular No. A-123, agencies should leverage existing functions within the organization that currently monitor and assess risk.[160]

Requirements
All executive agencies are required by OMB Circular No. A-123 to integrate ERM processes and internal controls and are required to include consideration of internal controls over reporting in their annual assurance statement.[161]

Open Data and [Records Management Budget Estimates]
[Agency budget estimates] should reflect data sets that have been prioritized through [the] agency's engagement with customers as specified in OMB Memorandum M-13-13, Open Data Policy –Managing Information as an Asset. [These] estimates should also reflect work necessary to meet the requirements of OMB Memorandum M-12-18, Managing Government Records Directive, OMB Circular A-130, the E-Government Act, and OMB's guidance. Initiatives should create a customer-centered electronic presence.[162]

---

[157] OMB Circular A-130. Managing Information as a Strategic Resource. Page 6. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[158] OMB Circular A-130. Managing Information as a Strategic Resource. Page 19. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
[159] OMB M-18-16. Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk. 6/6/2018. Page 4. https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-16.pdf
[160] OMB M-18-16. Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk. 6/6/2018. Page 8. https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-16.pdf
[161] Ibid.
[162] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Section 31.8. 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

Establish Integral Digital Governance
A strong governance structure will help agencies develop coherent priorities, set up lines of accountability, and satisfy the public's expectation of the best possible level of service. Agencies must manage their websites and digital services not as discrete individual IT projects, but as part of a comprehensive strategy covering all their digital information and services.

- As required in the Digital Government Strategy[163], every agency [should have established] a plan for governing its digital services, including websites and data.[164]

Implement Information Security and Privacy Controls
FISMA and OMB Circular A-130 require each Federal Agency to develop, document, and implement an agency-wide information security program for the information and information systems that support the agency's operations and assets, including those provided or managed by another agency, contractor, or other source. FISMA also provides for the development and maintenance of minimum controls to protect Federal information and information systems. Moreover, OMB Circular A-130 requires agencies to develop, implement, document, maintain, and oversee an agency-wide privacy program including people, processes, and technologies. Each agency-wide privacy program must implement privacy controls and verify that those controls are operating as intended and continuously monitored and assessed.

- Agencies must follow the policies, principles, standards, and guidelines on information security and privacy, in accordance with FISMA and other laws. Each agency is already required to implement security and privacy policies as set forth in OMB Circular A-130 and [NIST] Special Publication 800-44, Guidelines on Securing Public Web Servers; and other associated standards and 800 series guidelines from NIST. (Note: for a complete list of detailed requirements see the referenced memo.)[165]

Electronic Records
Section I: Implementation Guidance for all Agencies: All Federal agencies (CFO Act and non-CFO Act) must meet the following targets in order to begin the transition to a fully electronic government.

By 2019, Federal agencies will manage all permanent electronic records in an electronic format. By December 31, 2019, all permanent electronic records in Federal agencies will be managed electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format. Federal agencies have been required to manage all (permanent and temporary) email records in an electronic format since 2016 and are expected to continue to do so.

By 2022, Federal agencies will manage all permanent records in an electronic format and with appropriate metadata. By December 31, 2022, all permanent records in Federal agencies will be managed electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format. This does not apply to permanent records accessioned into NARA or transferred

[163] The White House. Digital Government Strategy. https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html
[164] OMB M-17-06. Policies for Federal Agency Public Websites and Digital Services. 11/8/2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-06.pdf
[165] Ibid.

for storage into Federal Records Centers before December 31, 2022. After December 31, 2022, all agencies will transfer permanent records to NARA in electronic formats and with appropriate metadata, in accordance with NARA regulations and transfer guidance, except where an agency has been granted an exception under procedures to be developed by NARA under paragraph 2.2, below.

By 2022, Federal agencies will manage all temporary records in an electronic format or store them in commercial records storage facilities. By December 31, 2022, all temporary records in Federal agencies will be managed electronically to the fullest extent possible. Agencies that receive an exception under paragraph 2.2 may continue to produce and store records in analog formats, but inactive records eligible for transfer after December 31, 2022 must be stored in commercial storage facilities. This does not apply to temporary records that are transferred for temporary storage into Federal Records Centers before December 31, 2022. By December 31, 2022, all agencies must close agency-operated records storage facilities and transfer inactive, temporary records to Federal Records Centers or commercial records storage facilities. Temporary, analog records that become eligible for transfer after December 31, 2022 must be transferred to commercial storage facilities that meet NARA records storage requirements.

Federal agencies will maintain robust records management programs that comply with the Federal Records Act and its regulations. Agencies must continue the following practices to ensure agency records are appropriately retained, stored, and transferred according to their disposition schedules.

- Designate a [SAORM] who is at the Assistant Secretary level or equivalent and has direct responsibility for ensuring that the agency efficiently and appropriately complies with all applicable records management statutes, regulations, and policy, including the requirements of this memorandum.
- Designate an Agency Records Officer who is responsible for overseeing agency recordkeeping requirements and operations and holds the NARA Certificate of Federal Records Management Training.
- Annually inform all agency personnel of their records management responsibilities in law, regulation, and policy, and provide training specific to the practices and policies of the organization.
- Ensure all records created or maintained by the agency are covered by a NARA-approved records schedule and permanent records are transferred to the National Archives when they reach their scheduled disposition date.
- Ensure NARA-approved records schedules are updated as business practices transition to electronic workflows.[166]

Federal Data Strategy – Purpose & Overview

[The Federal Data Strategy[167]] enables agencies-and Government as an enterprise to use and manage Federal data to serve the American people, including the critical twin goals of getting optimal value from our data assets and of protecting security, privacy, and confidentiality. It provides a common set of data principles and best practices in implementing data innovations that drive more value for the public. The Strategy complements statutory requirements and OMB information policy and guidance, and incorporates relevant changes proposed by agency and public comments received in response to M-19-

[166] OMB M-19-21. Transition to Electronic Records. 6/28/2019. https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-21.pdf

[167] Federal Data Strategy, Leveraging Data as a Strategic Asset. https://strategy.data.gov/

01: Request for Agency Feedback on the Federal Data Strategy.[168] Annual Action Plans specify measurable actions to implement the practices that are the priorities for a given year, providing timelines for implementation and identification of responsible parties. Agencies implement the Federal Data Strategy by adhering to the Action Steps in yearly action plans in accordance with OMB guidance.

Freedom of Information Act (FOIA) Portal

This memorandum provides instructions for agencies' Chief FOIA Officers on actions that agencies must take to ensure interoperability with the National FOIA Portal [foia.gov]. This memorandum is authorized and required by the FOIA Improvement Act of 2016, 5 U.S.C. § 552(m). "It requires agencies to provide information and complete necessary actions that will facilitate interoperability with the National FOIA Portal, through which a member of the public can submit a request for information to any Federal agency from angle website."[169]

Improve Customer Service Delivery

Each CFO Act agency ("agency" or "agencies") that directly provides significant services to individuals or to private and governmental entities will improve customer service through the following activities:

- Publish Customer Service Plans – …each agency will post a customer service plan ("plan") to its Open Government website. The plan will identify implementation steps for the customer service activities outlined in EO 13571, including a high-level discussion of the process by which a "signature initiative" to use technology to improve the customer experience will be designed and executed. The plan will prepare agencies to integrate specific customer service goals into annual agency performance plans and reports, as called for by the Government Performance and Results Modernization Act (GPRA) of 2010.
- Establish a Customer Service Task Force – To facilitate the exchange of best practices and the development of agency customer service plans and signature initiatives, OMB will coordinate a Customer Service Task Force ("Task Force"), comprised of agencies that provide significant services, that will meet regularly…. each agency should identify a senior official, who will be responsible for the customer service plan and related agency goals, to represent the agency on the Task Force … Before final publication …, participating agencies will conduct a peer review of their customer service plans.
- Advance Customer Service through Innovative Technology – With advances in technology and improvements in service delivery systems, customers' expectations continue to rise. To meet these expectations and increase efficiency, the Federal Government must incorporate increasingly common, lower cost self-service options that leverage technology, such as those accessed by the Internet or mobile phone.[170]
- The IDEA[171] aims to improve the digital experience for government customers and reinforces existing requirements for federal public websites.

---

[168] OMB M-19-18. Federal Data Strategy - A Framework for Consistency. 6/4/2019. https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf

[169] OMB M-19-10. Guidance for Achieving Interoperability with the National Freedom of Information Act (FOIA) Portal On FOIA.gov. 2/12/2019. https://www.whitehouse.gov/wp-content/uploads/2019/02/M-19-10.pdf

[170] OMB M-11-24. Implementing Executive Order 13571 on Streamlining Service Delivery and Improving Customer Service. 6/13/2011. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-24.pdf

[171] GSA. 21st Century Integrated Digital Experience Act. https://digital.gov/resources/21st-century-integrated-digital-experience-act/

02

SECTION

INFORMATION TECHNOLOGY LAWS

2. Laws

2.1 Federal Information Technology Acquisition Reform Act (2014)

The Federal Information Technology Acquisition Reform Act (FITARA), passed in December 2014, strengthened the role of agency CIOs and provided greater accountability for the delivery of IT capabilities across the Federal Government. To assist with agency implementation, OMB released OMB Memorandum M-15-14: Management and Oversight of Federal Information Technology[172] in June 2015.

FITARA outlines specific requirements related to:

1. Agency CIO Authority Enhancements
2. Enhanced Transparency and Improved Risk Management in IT Investments
3. Portfolio Review
4. Data Center Consolidation Initiative[173]
5. Expansion of Training and Use of IT Cadres
6. Maximizing the Benefit of the Federal Strategic Sourcing Initiative
7. Governmentwide Software Purchasing Program

Among other provisions, FITARA codified elements of existing Federal CIO initiatives. In addition, FITARA requires the Federal CIO, in conjunction with federal agencies, to:

- Refocus the Federal Data Center Consolidation Initiative (FDCCI) from consolidation to optimization, to include adoption of cloud services;
- Set forth a process for agency IT portfolio review and oversight;
- Improve transparency and risk management of IT investments;
- Identify and publish cost savings and optimization improvements;
- Provide public updates on cumulative cost savings and optimization improvements; and
- Review agencies' data center inventories and management strategies.

FITARA requires federal agencies to submit annual reports that include:

- Comprehensive data center inventories,
- Multiyear strategies to consolidate and optimize data centers,
- Performance metrics and a timeline for agency action, and
- Yearly calculations of investment and cost savings related to FITARA implementation.[174]

See Reporting Calendar for additional information on FITARA reporting activities.

[172] OMB M-15-14. Management and Oversight of Federal Information Technology. 6/10/2015. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2015/m-15-14.pdf
[173] OMB M-19-19. Update to Data Center Optimization Initiative (DCOI). 6/25/2019. https://datacenters.cio.gov/assets/files/m_19_19.pdf
[174] Congressional Research Service. The Current State of Federal Information Technology Acquisition Reform and Management. 2/03/2020. https://fas.org/sgp/crs/misc/R44843.pdf

Figure 1 identifies twelve practices,[175] including four overarching ones, considered vital to implementing FITARA published by GAO.

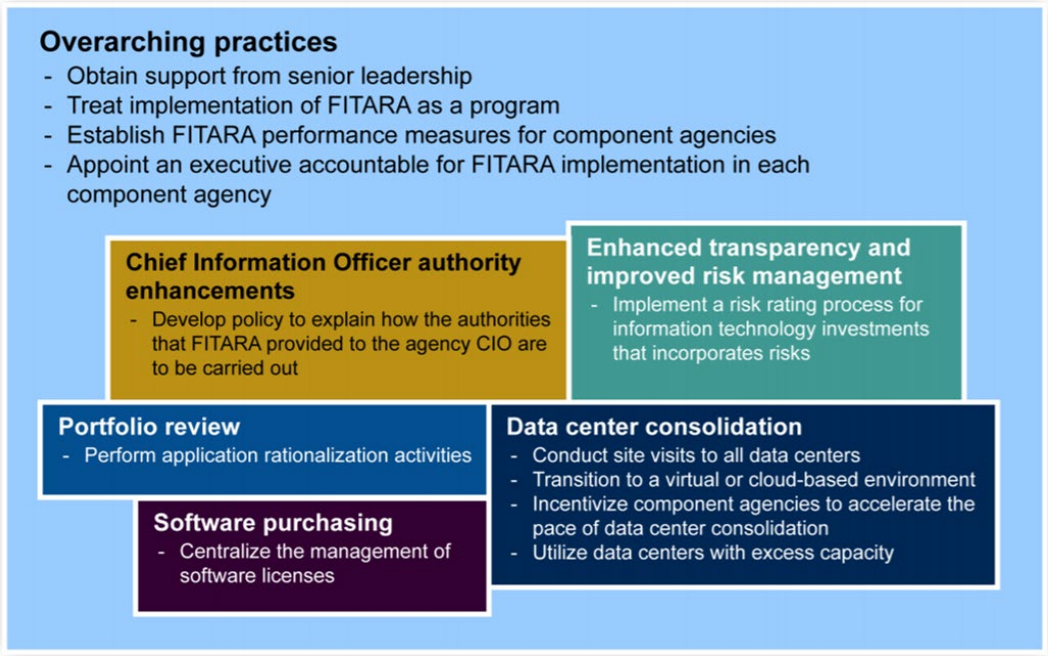

Figure 1: Practices for Effectively Implementing FITARA

2.2 Clinger Cohen Act (1996)

The Information Technology Management Reform Act (ITMRA) and the Federal Acquisition Reform Act (FARA) were signed into law as part of the National Defense Authorization Act for Fiscal Year 1996 and were subsequently designated the Clinger Cohen Act of 1996. This was the first time in law that agency CIO positions were established with designated roles and responsibilities. Clinger Cohen also directs Federal agencies to focus more on the results achieved through IT investments and streamlined the Federal IT procurement process, detailing how agencies approach the selection and management of IT projects.[176]

As part of the law, OMB is required to establish a budget process for analyzing, tracking, and evaluating, the risks and results of IT projects. This guidance has evolved and now encompasses the annual CPIC budget process. In addition, OMB was required to perform review of information resources management activities and ensure that adequate information security policies and procedures are in place across Federal agencies.

[175] GAO-19-131. Effective Practices Have Improved Agencies' FITARA Implementation. April 2019. https://www.gao.gov/assets/700/698751.pdf

[176] DOD. Department of Defense Chief Information Officer Desk Reference. 2006. https://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf

2.3 Federal Information Security Modernization Act (2002)

The Federal Information Security Modernization Act (FISMA), first enacted in 2002 and updated in December 2014, established roles and responsibilities for OMB, DHS, and agency CIOs to provide accountability for the delivery of information security capabilities.[177] The 2014 FISMA update simplifies existing reporting to eliminate inefficient or wasteful reporting, while adding new reporting requirements for major information security incidents. FISMA requires the head of each Federal agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Additionally, FISMA requires agency heads to report on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise.[178]

FISMA requires agencies to report the status of their information security programs to OMB and requires Inspectors General (IG) to conduct annual independent assessments of those programs. OMB and DHS collaborate with interagency partners to develop the CIO FISMA metrics, and with IG partners to develop the IG FISMA metrics to facilitate these processes. 0MB also works with the Federal privacy community to develop [SAOP] metrics. These three sets of metrics together provide a comprehensive picture of an agency's cybersecurity and privacy performance.[179]

The legislation also provides DHS with authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices. FISMA codifies DHS's authority to administer the implementation of information security policies for non-national security Executive Branch systems, including providing technical assistance and deploying technologies to these systems. It also places the federal information security incident center (a function fulfilled by US-CERT[180]) within DHS by law.

2.4 Chief Financial Officers Act (1990)[181]

The CFO Act gave OMB new authority and responsibility for directing federal financial management, modernizing the government's financial management systems, and strengthening financial reporting. The act also created the new position of Deputy Director for Management at OMB, who is to be the government's chief official responsible for financial management. While the CFO Act emphasizes improved financial management, it also charges OMB's Deputy Director for Management with overseeing many of the federal government's general management functions. These functions include information policy, procurement policy, property management, and productivity improvement.

The CFO Act also establishes a new Office of Federal Financial Management in OMB to carry out these governmentwide financial management responsibilities. To head this office, the act establishes the

---

[177] CISA. Federal Information Security Modernization Act. https://www.cisa.gov/federal-information-security-modernization-act

[178] CISA. Fiscal Year 2020 CIO FISMA Metrics. https://www.cisa.gov/sites/default/files/publications/FY%202020%20FISMA%20CIO%20Metrics_v1.pdf

[179] OMB M-20-04. Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements. 11/19/2019. https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf

[180] CISA. US-CERT. https://us-cert.cisa.gov/

[181] GAO. The Chief Financial Officers Act: a Mandate for Federal Financial Management Reform. September 1991. https://www.gao.gov/special.pubs/af12194.pdf

position of Controller, an individual who is to possess "demonstrated ability and practical experience in accounting, financial management, and financial systems." This individual will handle day-to-day operations to ensure that financial operations are being properly carried out governmentwide.

The 24 CFO Act Agencies include:

- Agency for International Development
- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Education
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of Housing and Urban Development
- Department of the Interior
- Department of Justice
- Department of Labor
- Department of State
- Department of Transportation
- Department of the Treasury
- Department of Veterans Affairs
- Environmental Protection Agency
- General Services Administration
- National Aeronautics and Space Administration
- National Science Foundation
- Nuclear Regulatory Commission
- Office of Personnel Management
- Small Business Administration
- Social Security Administration

2.5 Privacy Act (1974)

The Privacy Act[182] establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by Federal agencies. A system of records is defined as a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one

[182] 5 U.S.C. § 552a. Title 5 Government Organizations and Employees. https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf

of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records and sets forth various agency record-keeping requirements.[183]

2.6 Government Performance and Results Act (1993)[184]

The GPRA Modernization Act of 2010 was enacted in January 2011. The Act modernized the Federal Government's performance management framework, retaining and amplifying some aspects of the Government Performance and Results Act of 1993 (GPRA 1993) while also addressing some of its weaknesses. GPRA 1993 established strategic planning, performance planning and performance reporting for agencies to communicate progress in achieving their missions. The GPRA Modernization Act established some important changes to existing requirements. Subsequently, the GPRA Modernization Act of 2010 (GPRAMA) was enacted, which significantly expanded and enhanced the statutory framework for federal performance management.[185] Agencies are required to develop a five-year strategic plan outlining its mission, long-term goals for the agency's major functions, performance measures, and reporting results.

Building on lessons agencies have learned in setting goals and reporting performance, a heightened emphasis is placed on priority-setting, cross-organizational collaboration to achieve shared goals, and the use and analysis of goals and measurement to improve outcomes. The GPRA Modernization Act serves as a foundation for engaging leaders in performance improvement and creating a culture where data and empirical evidence play a greater role in policy, budget and management decisions.

The purposes of the GPRA Modernization Act of 2010 are to:

- Improve the confidence of the American people in the capability of the Federal Government, by systematically holding Federal agencies accountable for achieving program results;
- Improve program performance by requiring agencies to set goals, measure performance against those goals and report publicly on progress;
- Improve Federal program effectiveness and public accountability by promoting a focus on results, service quality and customer satisfaction;
- Help Federal managers improve service delivery, by requiring that they plan for meeting program goals and by providing them with information about program results and service quality;
- Improve congressional decision-making by providing information on achieving statutory objectives and on the relative effectiveness and efficiency of Federal programs and spending; Improve internal management of the Federal Government; and
- Improve usefulness of performance and program information by modernizing public reporting.

[183] 5 U.S.C. § 552a. Privacy Act of 1974. https://www.justice.gov/opcl/privacy-act-1974

[184] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Section 200.4. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[185] Public Law 111-352. GPRA Modernization Act of 2010. https://www.govinfo.gov/content/pkg/PLAW-111publ352/html/PLAW-111publ352.htm

2.7 Paperwork Reduction Act (1980 and 1995) [186]

The Paperwork Reduction Act (PRA) of 1980 established, within OMB, [OIRA]. It requires the Director of OMB to appoint an Administrator as head of OIRA and makes the Director responsible for any functions delegated to the Administrator about the development and implementation of federal information policies and standards.

The Paperwork Reduction Act (PRA) of 1995 gives OMB authority over the collection of certain information by Federal agencies. It is intended, "among other things, to 'ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the Federal Government' and to 'improve the quality and use of Federal information to strengthen decision-making, accountability, and openness in Government and society.'"[187] The Act requires agencies to plan for the development of new collections of information and the extension of ongoing collections well in advance of sending an information collection request to OMB. Agencies must:

- Seek public comment on proposed collections of information by placing a notice in the Federal Register;
- Certify to OMB that efforts have been made to reduce the burden of the collection; and
- Review and approve information collection requests internally before submitting them to OMB.

Although the scope of the PRA has changed over the years, its underlying policy standards remain the same. The PRA seeks to:

- Minimize the paperwork burden on the public and other entities;
- Ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared, and disseminated by or for the Federal Government;
- Improve the quality and use of Federal information to strengthen decision making, accountability, and openness in Government and society;
- Minimize the cost to the Federal Government of creating, collecting, maintaining, using, disseminating, and disposing of information; and
- Ensure the integrity, quality, and utility of the Federal statistical system.[188]

2.8 Government Paperwork Elimination Act (1998)[189]

The Government Paperwork Elimination Act (GPEA) seeks to "preclude agencies or courts from systematically treating electronic documents and signatures less favorably than their paper

[186] 44 U.S.C. Chapter 35. Paperwork Reduction Act of 1980. https://digital.gov/resources/paperwork-reduction-act-44-u-s-c-3501-et-seq/

[187] OMB. Memorandum for the Heads of Executive Departments and Agencies, And Independent Regulatory Agencies. 4/7/2010. http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/PRAPrimer_04072010.pdf.

[188] OPM. Paperwork Reduction Act (PRA) Guide. 4/27/2011. https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf

[189] OMB. Implementation of the Government Paperwork Elimination Act. https://obamawhitehouse.archives.gov/omb/fedreg_gpea2/

counterparts", so that citizens can interact with the Federal government electronically (S. Rep. 105-335). It requires Federal agencies, by October 21, 2003, to provide individuals or entities that deal with agencies the option to submit information or transact with the agency electronically, and to maintain records electronically, when practicable. It also addresses the matter of private employers being able to use electronic means to store, and file with Federal agencies, information pertaining to their employees. GPEA states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. It also encourages Federal government use of a range of electronic signature alternatives.

2.9 Information Quality Act (2000)[190]

Section 515 of Public Law 106-554, known as the Information Quality Act, required the [OMB] to promulgate guidance to agencies ensuring the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by Federal agencies. OMB's government-wide guidelines, published as interim final on September 28, 2001 (66 F.R. 49718) and finalized on February 22, 2002 (67 F.R. 8452)[191], can be found on [Reginfo.gov]. Federal agencies were also required by Section 515 to publish their own agency specific guidelines no later than one year after OMB's guidelines.

2.10 Freedom of Information Act (2000)[192]

Allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States government. FOIA defines agency records subject to disclosure, outlines mandatory disclosure procedures, and grants exemptions to the statute.

The FOIA provides that when processing requests, agencies should withhold information only if they reasonably foresee that disclosure would harm an interest protected by an exemption, or if disclosure is prohibited by law. Agencies should also consider whether partial disclosure of information is possible whenever they determine that full disclosure is not possible and they should take reasonable steps to segregate and release nonexempt information. The Office of Information Policy at the Department of Justice is responsible for issuing government-wide guidance on the FOIA as part of its responsibilities to encourage all agencies to fully comply with both the letter and the spirit of the FOIA.

[190] OMB. Agency Information Quality Guidelines. https://obamawhitehouse.archives.gov/omb/inforeg_agency_info_quality_links/

[191] Federal Register. Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies; Republication. 2/22/2002. https://www.federalregister.gov/documents/2002/02/22/R2-59/guidelines-for-ensuring-and-maximizing-the-quality-objectivity-utility-and-integrity-of-information

[192] DOJ. What is FOIA? https://www.foia.gov/about.html

2.11 Confidential Information Protection and Statistical Efficiency Act (2002)

Enacted to protect the confidentiality of information acquired from the public. The Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), Title V of the E-Government Act of 2002 (Pub. L. No. 107-347), has two subtitles.[193]

Subtitle A, Confidential Information Protection, concerns confidentiality and statistical uses of information. The purposes of Subtitle A are:

1. To ensure that information supplied by individuals or organizations to an agency for statistical purposes under a pledge of confidentiality is used exclusively for statistical purposes;
2. To ensure that individuals or organizations who supply information under a pledge of confidentiality to agencies for statistical purposes will neither have that information disclosed in identifiable form to anyone not authorized by this title nor have that information used for any purpose other than a statistical purpose; and
3. To safeguard the confidentiality of individually identifiable information acquired under a pledge of confidentiality for statistical purposes by controlling access to, and uses made of, such information.

CIPSEA Subtitle A protects information that is acquired for exclusively statistical purposes under a pledge of confidentiality. This subtitle of the law applies to all Federal agencies that acquire information under these carefully prescribed conditions. The protection of information collected under this law is supported by a penalty of a Class E Felony for a knowing and willful disclosure of confidential information.

CIPSEA Subtitle B promotes statistical efficiency through limited sharing of business data among three designated statistical agencies, the Bureau of the Census (Census), the Bureau of Economic Analysis (BEA), and the Bureau of Labor Statistics (BLS). The purposes of Subtitle B are:

1. To authorize the sharing of business data among Census, BEA, and BLS for exclusively statistical purposes;
2. To reduce the paperwork burdens imposed on businesses that provide requested information to the Federal Government;
3. To improve the comparability and accuracy of Federal economic statistics by allowing Census, BEA, and BLS to update sample frames, develop consistent classifications of establishments and companies into industries, improve coverage, and reconcile significant differences in data produced by the three agencies; and
4. To increase understanding of the United States economy, especially for key industry and regional statistics, to develop more accurate measures of the impact of technology on productivity growth, and to enhance the reliability of the Nation's most important economic indicators, such as the National Income and Product Accounts.

[193] OMB. Implementation Guidance for Title V of the E-Government Act. October 2006. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/inforeg/proposed_cispea_guidance.pdf

2.12 Digital Accountability and Transparency Act (2014)[194]

Enacted to improve the quality and transparency of Federal award data.

On September 26, 2006, Federal Funding Accountability and Transparency Act (FFATA) was signed into law. The legislation required that federal contract, grant, loan, and other financial assistance awards be displayed on a publicly accessible and searchable website to give the American public access to information on how their tax dollars are being spent. On May 9, 2014, DATA Act was signed into law creating the purpose of the DATA Act Team. The legislation expanded FFATA to:

- Include all direct agency spending and link federal contract, grant, and loan spending to specific agency programs;
- Set government-wide standards for financial data so we can accurately show consistent, reliable, and searchable data;
- Simplify reporting, streamline requirements for reporting, and reduce the cost of complying with the requirements, while improving transparency; and
- Improve the quality of the data at USAspending.gov by holding agencies accountable.

2.13 Geospatial Data Act (2018)

Codifies the Federal Geographic Data Committee and supports the National Spatial Data Infrastructure

The Geospatial Data Act of 2018 (GDA) became law on October 5, 2018. The GDA was included as a component of the FAA Reauthorization Act (P.L. 115-254, Subtitle F). The GDA codifies the committees, processes, and tools used to develop, drive, and manage the National Spatial Data Infrastructure (NSDI) and recognizes responsibilities beyond the Federal government for its development. The GDA reflects growing recognition of the essential role of geospatial data and technology in understanding and managing our world and highlights the need to support their continuing development as critical investments for the Nation.[195]

The GDA reduces duplicative efforts and facilitates the efficient procurement of geospatial expertise, technology, services, and data from the rapidly growing geographic community in the United States. The GDA:

- Aligns business strategies and technology;
- Ensures that resources are managed in accordance with the Nation's needs and priorities; and
- Ensures that all technology resources and employees are utilized in a manner that provides the best value for the Nation

[194] Bureau of the Fiscal Service. About the Data Transparency Program. 6/8/2020. https://fiscal.treasury.gov/data-transparency/history-overview.html

[195] Federal Geographic Data Committee. Geospatial Data Act of 2018. https://www.fgdc.gov/gda/gda-fact-sheet-may-2019.pdf

2.14 Evidence-Based Policy Making Act (2018)[196]

Establishes processes for the federal government to modernize data management practices, evidence-building functions, and statistical efficiency.

The Foundations for Evidence-Based Policymaking Act (or OPEN Government Data Act, Pub.L. 115–435) is a United States law that requires the federal government to modernize its data management practices.

The bill requires agencies to submit annually to [OMB] and Congress a systematic plan for identifying and addressing policy questions. The plan must include, among other things:

- Questions for developing evidence to support policymaking;
- Data the agency intends to collect, use, or acquire to facilitate the use of evidence in policymaking;
- Methods and analytical approaches that may be used to develop evidence to support policymaking; and
- Challenges to developing evidence to support policymaking, including any statutory or other restrictions to accessing relevant data.

Each agency shall designate a senior employee as Evaluation Officer to coordinate evidence-building activities and an official with statistical expertise to advise on statistical policy, techniques, and procedures.

2.15 Open Government Data Act (2018)

Requires public government data assets to be published as machine-readable data, and each agency shall develop and maintain a comprehensive data inventory and designate a Chief Data Officer.

On January 14, 2019, the Open, Public, Electronic and Necessary (OPEN) Government Data Act,[197] as part of the Foundations for Evidence Based Policymaking Act, became law. The OPEN Government Data Act makes Data.gov a requirement in statute, rather than a policy. It requires federal agencies to publish their information online as open data, using standardized, machine-readable data formats, with their metadata included in the Data.gov catalog. Data.gov is working with an expanded group of federal agencies to include their datasets in Data.gov as they implement the new law. In addition, the law requires that GSA work with [OMB] and the Office of Government Information Services to establish an "online repository of tools, best practices, and schema standards to facilitate the adoption of open data practices across the Federal Government." This new repository, which will be an update and expansion of Project Open Data, will also be available on Data.gov.[198]

---

[196] CIO. Foundations for Evidence-Based Policymaking Act of 2018. https://www.cio.gov/policies-and-priorities/evidence-based-policymaking/

[197] Open, Public, Electronic, and Necessary Government Data Act. 3/29/2017. https://www.congress.gov/bill/115th-congress/house-bill/1770

[198] GSA. Data.gov at Ten and the OPEN Government Data Act. 5/31/2019. https://www.data.gov/meta/data-gov-at-ten-and-the-open-government-data-act/

2.16 Creating Advanced Streamlined Electronic Services for Constituents Act (2019)

Enacted in 2019, the Creating Advanced Streamlined Electronic Services for Constituents (CASES) Act directs OMB to require each federal agency to accept electronic identity proofing and authentication processes that allow an individual, under the [Privacy Act of 1974], to access the individual's records or to provide prior written consent for the disclosure of the individual's records.[199] The bill modernizes the way members of Congress receive permission from constituents before contacting federal agencies on their behalf. Instead of a paper submission, constituents who request casework from their congressional representatives every year have the option of submitting a privacy release form electronically.

2.17 Internet of Things Cybersecurity Improvement Act of 2020

Enacted in 2020 to establish minimum security standards for [Internet of Things (IoT)] devices owned and controlled by the federal government. This law gives authority to the CIO to prohibit the head of any agency from "procuring or obtaining, renewing a contract to procure or obtain, or using an [IoT] device" if they find through a mandatory review process that the use of the device prevents compliance with NIST standards and guidelines.

The CIO can waive this requirement only if:

- the waiver is necessary in the interest of national security;
- procuring, obtaining, or using such device is necessary for research purposes; or
- such device is secured using alternative and effective methods appropriate to the function of such device.[200]

2.18 IT Modernization Centers of Excellence Program Act

Enacted in 2020 to establish a program to facilitate the adoption of modern technology by executive agencies. This law codifies the GSA Centers of Excellence (CoEs) Program including the ten existing CoEs and any future ones. It creates a requirement for federal agencies to cooperate on information technology efforts including:

- A commercial cloud computing system that includes
    - end-to-end migration planning and an assessment of progress towards modernization;
    - a cybersecurity and governance framework that promotes industry and government risk management best practice approaches, prioritizing efforts based on risk, impact, and consequences.
- Tools to help an individual receive support from and communicate with an executive agency.
- Contact centers and other related customer supports.

---

[199] Creating Advanced Streamlined Electronic Services for Constituents Act of 2019. https://www.congress.gov/bill/116th-congress/senate-bill/435

[200] Public Law 116-207. IoT CyberSecurity Improvement Act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668/text

- Efficient use of data management, analysis, and reporting.
- The optimization of infrastructure, including for data centers, and the reduction of operating costs.
- Artificial intelligence[201]

[201] Public Law 116-194. Information Technology Modernization Centers of Excellence Program Act. https://www.congress.gov/116/plaws/publ194/PLAW-116publ194.pdf

03
SECTION

OTHER IT AUTHORITIES

3. Other Authorities

3.1 Executive Orders (EOs)

An EO is a declaration by the president which has the force of law, usually based on existing statutory powers, and requiring no action by the Congress. They are numbered consecutively, so executive orders may be referenced by their assigned number, or their topic. A sitting U.S. President may overturn an existing executive order[202] by issuing another executive order to that effect.[203]

Recent relevant EOs:

- Executive Order 13800 (EO 13800)[204]

3.2 OMB Circulars

An OMB Circular provides instructions or information issued to Federal agencies which are expected to have a continuing effect of two years or more.[205] Circulars are one of the primary ways OMB provides detailed instructions and information to Federal agencies. Importantly, Circulars standardize implementation guidance for Federal agencies across an array of policy areas and topics that are central to the Federal Government's management and budget processes.

Circular A-130:[206]

- In July 2016, [OMB] revised Circular A-130, Managing Information as a Strategic Resource[207], to reflect changes in law and advances in technology. The revisions also ensure consistency with executive orders, presidential directives, recent OMB policy, and National Institute of Standards and Technology standards and guidelines.
- The Circular establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy. It also emphasizes the role of both privacy and security in the Federal information life cycle. Importantly, it represents a shift from viewing security and privacy requirements as compliance exercises to understanding security and privacy as crucial elements of a comprehensive, strategic, and continuous risk-based program at Federal agencies.

---

[202] Federal Register. Executive Orders. All Executive Orders Since 1994. https://www.federalregister.gov/presidential-documents/executive-orders

[203] American Bar Association. What Is an Executive Order? 10/9/2020. https://www.americanbar.org/groups/public_education/publications/teaching-legal-docs/what-is-an-executive-order-/

[204] Executive Order 13800. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 5/11/2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[205] OMB. Circulars. https://www.whitehouse.gov/omb/information-for-agencies/circulars/

[206] CIO. Circular A-130 Managing Information As a Strategic Resource. https://www.cio.gov/policies-and-priorities/circular-a-130/

[207] Ibid.

Circular A-11:[208]

- The OMB Circular A-11 is a United States government document issued by the Office of Management and Budget in the form of a written advisory that provides information related to the preparation of the various budgets of agencies of the Federal Government. It is the primary document instructing these agencies in methods, requirements, and terminology for submissions to be reviewed for approval.

3.3 OMB Memoranda

The OMB memoranda provides Federal agencies with instructions and implementation guidance for specific management priorities or legislative requirements. They provide annual updates, such as for FISMA reporting requirements, or have longer term guidance for agency implementation. While some memoranda have built in expiration dates, there have been some examples of previous memoranda being rescinded, such as in M-17-15[209] and M-17-26.[210]

See list of relevant OMB memorandums at https://www.whitehouse.gov/omb/information-for-agencies/memoranda/.

3.4 DHS Binding Operational Directive (BOD)

A BOD is a compulsory direction to executive branch departments and agencies for purposes of safeguarding federal information and information systems.[211] Federal agencies are required to comply with these DHS-developed directives. The Department of Homeland Security (DHS) has the statutory responsibility, in consultation with OMB, to administer the implementation of agency information security policies and practices for information systems, which includes assisting agencies and providing certain government-wide protections. A BOD is a compulsory direction to an agency for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk in accordance with policies, principles, standards, and guidelines issued by the Director of OMB.[212] As part of that responsibility, DHS is authorized to develop and oversee the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidance developed by the Director of OMB and requirements of FISMA.

See list of DHS BODs at https://cyber.dhs.gov/directives/.[213]

---

[208] GSA. 2019 Revision to OMB Circular A-11, Part 6: Strengthening the Policy Framework for Improving Program and Service Delivery. 8/14/2019. https://www.performance.gov/a-11-revision/

[209] OMB M-17-15. Rescission of Memoranda Relating to Identity Management. 1/19/2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-15.pdf

[210] OMB M-17-26. Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda. 6/15/2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-26.pdf

[211] 44 U.S.C. § 3552(b)(l). Title 44 Public Printing and Documents. https://www.govinfo.gov/content/pkg/USCODE-2014-title44/pdf/USCODE-2014-title44-chap35-subchapII-sec3552.pdf

[212] DHS. Binding Operational Directive 18-01. Enhance Email and Web Security. 10/16/2017. https://cyber.dhs.gov/assets/report/bod-18-01.pdf

[213] DHS. Binding Operational Directives. https://cyber.dhs.gov/directives/

04

SECTION

KEY STAKEHOLDERS

4. Key Stakeholders

4.1 Overview of Key Stakeholders

CIOs must maintain relationships with many stakeholders both within their agency and across the Federal government to effectively perform their duties. These stakeholders' roles and titles will vary from agency to agency, and it is common for one person to perform more than one of these functions simultaneously.

Agency CXOs are the executives who lead agency management functions, along with the CIO these roles are the Chief Acquisition Officer (CAO), Chief Data Officer (CDO), Chief Financial Officer (CFO), Chief Human Capital Officer (CHCO), and Chief Information Security Officer (CISO). Executives leading these management functions work closely with the Performance Improvement Office (PIO), agency head and Chief Operating Officer (COO) to ensure that mission support resources are effectively and efficiently aligned and deployed to achieve the agency mission. This includes such activities as routinely leading efforts to set goals, make results transparent, review progress, and make course corrections as needed to ensure that the agency's management functions are effective in supporting agency goals and objectives.

Beyond the "C-Suite" and their corresponding councils, CIOs also should maintain working relationships with their agency's Legislative Affairs office to ensure they are aware of Congressional proceedings or interests which may pertain to their agency's IT portfolio as well as their Senior Agency Official for Privacy (SAOP). OMB Desk Officers and Resource Management Officers (RMOs) are also key sources of support on management and budget topics, respectively.

4.2 Chief Acquisition Officer (CAO)[214]

To ensure that acquisition issues receive high-level management attention, the Services Acquisition Reform Act of 2003 (SARA) established the position of the CAO. CAOs work closely with other senior executives government-wide and within their agencies to continuously improve the federal acquisition system. CAOs have several major areas of prioritized responsibility:

- Buy Smarter: CAOs should work with CFOs, CIOs, and CHCOs to increase the agency's use of government-wide and agency-wide strategic sourcing vehicles will save money and reduce duplication. supporting the agency's CIO in ongoing IT portfolio investment reviews, and working with the CFO to target administrative savings opportunities, will also help the agency buy smarter.
- Strengthen the Acquisition Workforce: CAOs should work with the agency's CHCO and principal program managers to develop and implement the annual Acquisition Human Capital Plan, and work with the CIO to determine how best to support IT acquisition, such as through the development of specialized IT acquisition cadres.
- Building the Right Supplier Relationships: CAOs should lead efforts to, among other things, improve the value of contractor past performance assessments and increase the transparency

[214] OMB. Clarifying Chief Acquisition Officer Roles and Responsibilities. 10/18/2012. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/procurement/memo/cao-roles-and-responsibilities.pdf

of contractor business integrity data so that the Federal Government only does business with reputable firms.

- Advance Mission Performance: CAOs should also work closely with agency leaders, such as the COO, PIO, and key mission program managers that depend heavily on acquisition, to help define acquisition needs that will advance agency goals and objectives in the most cost-effective manner possible. CAOs should ensure acquisition strategies are aligned with, and driven by, mission program and performance objectives, such as those established in an agency's strategic plans, or those that support the achievement of agency priority goals.

CAO Council

The CAO Council was established pursuant to Section 16 of the Office of Federal Procurement Policy Act, as amended, 41 USC 403, et seq.[215] It is chaired by OMB's Deputy Director for Management[216] and consists of a diverse group of acquisition professionals in the Executive Branch established to provide a senior level forum for monitoring and improving the federal acquisition system.

The Council works closely with the Administrator, Office of Federal Procurement Policy, and the Federal Acquisition Regulatory Council to promote these business practices in the acquisition system. It promotes effective business practices that ensure the timely delivery of best value products and services to the agencies, achieve public policy objectives, and further integrity, fairness, competition, and openness in the federal acquisition system. CAO.gov is where the Council shares priorities, key technology policies, news, and the programs and events sponsored by the Council.[217]

4.3 Chief Data Officer (CDO)[218]

The CDO of an agency shall be designated on the basis of demonstrated training and experience in data management, governance (including creation, application, and maintenance of data standards), collection, analysis, protection, use, and dissemination, including with respect to any statistical and related techniques to protect and de-identify confidential data. The agency CDO will be a trusted partner for the agency CIO in developing and implementing policies and statutory requirements related to the management of agency data.

Agency CDO responsibilities include:

- [Responsible] for lifecycle data management;
- Coordinate with any official in the agency responsible for using, protecting, disseminating, and generating data to ensure that the data needs of the agency are met;
- Manage data assets of the agency, including the standardization of data format, sharing of data assets, and publication of data assets in accordance with applicable law;
- Ensure that, to the extent practicable, agency data conforms with data management best practices;

[215] 41 U.S.C. § 1101. Office of Federal Procurement Policy Act. https://www.govinfo.gov/content/pkg/USCODE-2011-title41/pdf/USCODE-2011-title41-subtitleI-divsnB-chap11-subchapI-sec1101.pdf

[216] OMB M-04-13. Chief Acquisition Officers Council. May 2004. https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-13.html#att

[217] CAO. Chief Acquisition Officers Council. https://cao.gov/cao-home

[218] 44 U.S.C. § 3520. Chief Data Officers. https://www.law.cornell.edu/uscode/text/44/3520

- Engage agency employees, the public, and contractors in using public data assets and encourage collaborative approaches on improving data use;
- Support the Performance Improvement Officer of the agency in identifying and using data to carry out the functions described in section 1124(a)(2) of title 31[219];
- Support the Evaluation Officer of the agency in obtaining data to carry out the functions described in section 313(d) of title 5[220];
- Review the impact of the infrastructure of the agency on data asset accessibility and coordinate with the [CIO] of the agency to improve such infrastructure to reduce barriers that inhibit data asset accessibility;
- Ensure that, to the extent practicable, the agency maximizes the use of data in the agency, including for the production of evidence (as defined in section 3561[221]), cybersecurity, and the improvement of agency operations;
- Identify points of contact for roles and responsibilities related to open data use and implementation;
- Serve as the agency liaison to other agencies and [OMB] on the best way to use existing agency data for statistical purposes (as defined in section 3561[222]).

CDO Council

The CDO Council established by the Evidence Act[223] includes all agency Chief Data Officers, the Administrator of the Office of Electronic Government (or designee), the Administrator of the Office of Information and Regulatory Affairs (or designee), and an Ex Officio Member (to represent all Chief Information Officers and Evaluation Officers). The CDO Council meets regularly to:

- Establish government-wide best practices for the use, protection, dissemination, and generation of data;
- Promote and encourage data sharing agreements between agencies;
- Identify ways in which agencies can improve upon the production of evidence for use in policymaking; consult with the public and engage with private users of Government data and other stakeholders on how to improve access to data assets of the Federal Government; and
- Identify and evaluate new technology solutions for improving the collection and use of data.

The CDO Council's resources will reflect consultation with the public and engagement with private users of government data and other stakeholders on how to improve access to Federal data assets. In addition, the CDO Council will identify and evaluate new technology solutions for improving the collection and use of data. The CDO Council will share responsibility with other government-wide councils that conduct statutory, data-related activities, such as the Interagency Council on Statistical Policy (ICSP) and the Evaluation Officer Council. OMB expects that the activities of these multiple councils will be coordinated through the OMB Federal Data Policy Committee.

---

[219] 31 U.S.C. § 1124(a)(2). Performance Improvement Officers. https://www.law.cornell.edu/uscode/text/31/1124#a_2

[220] 5 U.S.C. § 313(d). Evaluation Officers. https://www.law.cornell.edu/uscode/text/5/313#d

[221] 44 U.S.C. § 3561. Definitions. https://www.law.cornell.edu/uscode/text/44/3561

[222] Ibid.

[223] Public Law 115-435. Foundations for Evidence-Based Policymaking Act of 2018. https://www.congress.gov/bill/115th-congress/house-bill/4174

4.4 Chief Financial Officer (CFO)

The agency CFO delivers timely, accurate, and reliable financial information to decision makers through efficient and effective financial systems and business processes, fosters effective stewardship of public funds, and safeguards fiscal integrity through effective internal controls. The CFO ensures compliance with federal financial integrity legislation, including the CFO Act. The Office of the CFO leads efforts to examine, identify, and implement administrative cost reduction initiatives and improve efficiencies across the agency.

An agency CIO should partner with the CFO to effectively manage the agency's IT budget and portfolio. Aligning IT investments to the agency's strategic business plans will ensure that IT investments are viewed as a key part.

An agency CFO is to report directly to the agency head on financial management matters. The CFO's responsibilities are to include the following:

- Developing and maintaining integrated accounting and financial management systems;
- Directing, managing, and providing policy guidance and oversight of all agency financial management personnel, activities, and operations;
- Approving and managing financial management systems design and enhancement projects;
- Developing budgets for financial management operations and improvements;
- Overseeing the recruitment, selection, and training of personnel to carry out agency financial management functions;
- Implementing agency asset management systems, including systems for cash management, credit management, debt collection, and property and inventory management and control; and
- Monitoring the financial execution of the agency budget in relation to actual expenditures.[224]

CFO Council

The CFOC was established by the Chief Financial Officers Act of 1990[225] to advise and coordinate the activities of the member agencies. The CFO Council is composed of CFOs and Deputy CFOs of large federal agencies, the Deputy Director for Management at OMB chairs the organization. It was established to advise and coordinate on member agency matters, including:

- Consolidating and modernizing of financial systems;
- Improving the quality of financial information;
- Financial data and information standards;
- Internal controls;
- Legislation affecting financial operations and organizations; and
- Any other financial management matters.

[224] GAO. The Chief Financial Officers Act. September 1991. https://www.gao.gov/special.pubs/af12194.pdf

[225] Public Law 101-576. Chief Financial Officers Act of 1990. https://www.govinfo.gov/content/pkg/STATUTE-104/pdf/STATUTE-104-Pg2838.pdf

CFO.gov is where the Council shares priorities, key technology policies, news, and the programs and events sponsored by the Council.[226]

4.5 Chief Human Capital Officer (CHCO)

The agency CHCO plays an important role in supporting agency strategic planning and performance improvement efforts by ensuring human capital plans, strategies, and investments advance organizational goals set forth in the agency's strategic and annual plans. Each CHCO serves as their agency's chief policy advisor on all human resources management issues and is charged with selecting, developing, training, and managing a high-quality, productive workforce. The chief functions of the agency CHCO include:

- Setting the workforce development strategy of the agency;
- Assessing workforce characteristics and future needs based on the agency's mission and strategic plan;
- Aligning the agency's human resources policies and programs with organization mission, strategic goals, and performance outcomes;
- Developing and advocating a culture of continuous learning to attract and retain employees with superior abilities;
- Identifying best practices and benchmarking studies, and
- Applying methods for measuring intellectual capital and identifying links of that capital to organizational performance and growth.[227]

CHCO Council

The CHCO Council was formally established by the Chief Human Capital Officers Act of 2002. The Act provides that the Director of OPM serves as Chairperson of the Council, and the Deputy Director for Management of OMB serves as Vice Chairperson. The members of the CHCO Council include the Director of OPM, the Deputy Director for Management of OMB, and Chief Human Capital Officers of Executive Departments. Other members may be designated by the Chairperson including CHCOs of other Executive Agencies and members designated on an ex officio basis.

The purposes of the Council are to:

- Advise OPM, OMB, and agency leaders on human capital strategies and policies, as well as on the assessment of human capital management in Federal agencies.
- Inform and coordinate the activities of its member agencies on such matters as modernization of human resources systems, improved quality of human resources information, and legislation affecting human resources management operations and organizations.
- Assist member CHCOs and other officials with similar responsibilities in fulfilling their individual responsibilities to:
    - Implement the laws governing the Federal civil service, as well as the rules and regulations of the President, OPM, and other agencies with regulatory authority that affects Federal employees;

[226] CFO. Chief Financial Officers. https://www.cfo.gov/about-the-council/

[227] Public Law 107-296. Chief Human Capital Officers Act of 2002. https://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

- In accordance with those laws and regulations, advise and assist agency heads and other senior officials in carrying out their responsibilities for selecting, developing, training, and managing a high-quality, productive workforce in accordance with merit system principles;
- Assess workforce characteristics and future needs and align the agency's human resources policies and programs with the agency's mission, strategic goals, and performance objectives;
- Advocate and assure a culture of continuous learning and high performance, developing and implementing effective strategies to attract, develop, manage, and retain employees with superior abilities;
- Identify human capital best practices and benchmarks and apply those exemplars to their agencies and the Federal Government as a whole.
- Provide leadership in identifying and addressing the needs of the Federal Government's human capital community, including training and development.

CHCOC.gov is where the Council shares priorities, key technology policies, news, and the programs and events sponsored by the Council.[228]

4.6 Chief Information Officers Council (CIOC)[229]

CIOs from the 24 CFO Act agencies are invited and encouraged to participate in the CIO Council which was codified into law under the e-Government Act of 2002[230]. The CIO Council is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources.

The U.S. federal CIO and the CIO Council establish standards against which the success of all agency programs can be measured, including:

- Monitoring the year-to-year performance improvement of Federal Government programs
- Attracting and retaining a high-performance IT workforce
- Optimizing Federal Government information resources and investments
- Aligning IT solutions with Federal enterprise business processes
- Adopting and sharing best IT management practices
- Managing risk and ensuring privacy and security

The e-Government Act of 2002[231] outline the CIO Council's responsibilities which include:

1. Developing recommendations for the Director of OMB on government information resources management policies and requirements;
2. Sharing experiences, ideas, best practices, and innovative approaches related to information resources management;

---

[228] Ibid.

[229] CIO Council. https://www.cio.gov/about/vision/

[230] Public Law 107–347. e-Government Act of 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

[231] Ibid.

3. Assisting the Federal CIO in the identification, development, and coordination of multi-agency projects and other innovative initiatives to improve Government performance through the use of information technology;
4. Promoting the development and use of common performances for agency information resources management; and
5. Working with the Office of Personnel Management to assess and address the hiring, training, classification, and professional development of the Federal IT workforce.

The CIO Council has 4 committees and many working groups. The committees include:

- The Services, Strategies and Infrastructure Committee
- Innovation Committee
- IT Workforce Committee
- CISO Council

4.7 Chief Information Security Officer (CISO)[232]

The agency CISO plays a key role in working with the agency CIO to ensure information security requirements are properly implemented. In most cases, the agency's internal policies delegate management of the agency's information to the CIO, who has the authority under FISMA to delegate tasks related to information security to the agency CISO. FISMA does not instruct agencies on how to develop or maintain their information security programs; it simply lists agencies' information security responsibilities. As a result, no two CISO roles are exactly the same. Some CISOs are responsible for all information security tasks at their agency, while others work with separate operations centers or take on tasks outside of information security to help with organizational priorities. Although FISMA allows for these nuances, CIOs and CISOs are ultimately statutorily responsible for information security, so they must be aware of the range of information security responsibilities assigned to agencies.

An agency CIO should view their CISO as a trusted partner and advisor for developing and implementing information security requirements. While each agency's organizational and reporting structure may be different, building a productive relationship between the CIO and CISO is essential for effective IT and security management.

CISO Council

The CISO Council is a committee under the CIO Council led by the Federal CISO and an agency Vice-Chair. Its membership consists of agency CISOs from the 24 CFO Act Executive branch agencies.

4.8 Chief Operating Officer (COO)

As envisioned by the Government Performance and Results Act (GPRA) Modernization Act of 2010 (GPRAMA), the agency COO is responsible for providing overall organization management to improve and achieve the mission and goals of the agency. COOs provide organizational leadership to improve performance of both mission and management functions. They bring together other leaders and staff within the agency, including component managers, program and project managers, research and evaluation experts, and other leaders of key management functions such as the CIO, the CFO, the [CHCO], the CAO, and PIO. With leadership from the COO, these and other agency leaders collectively

[232] CIO Council. CISO Handbook. https://www.cio.gov/assets/resources/CISO_Handbook.pdf

solve problems and pursue opportunities that help the agency operate more effectively and efficiently.[233]

4.9 Office of Executive Councils

The Office of Executive Councils resides in the Office of Government-wide Policy at GSA. This office coordinates engagement and policy development across the CXO ecosystem. The Executive Councils consists of the following inter-agency communities:

- Chief Information Officers Council (CIOC)[234]
  - See Chief Information Officers Council section for full description.
- Chief Data Officers Council (CDOC)[235]
  - See Chief Data Officer (CDO) section for full description.
- Chief Acquisition Officers Council (CAOC)[236]
  - See Chief Acquisition Officer (CAO) section for full description.
- Chief Financial Officers Council (CFOC)[237]
  - See Chief Financial Officer (CFO) section for full description.
- Chief Human Capital Officers Council (CHCOC)[238]
  - See Chief Human Capital Officer (CHCO) section for full description.
- Federal Privacy Council (FPC)[239]
  - See Senior Agency Official for Privacy (SAOP) section for full description.
- Performance Improvement Council (PIC)[240]
  - See the Performance Improvement Council (PIC) section for full description.
- President's Management Council (PMC)[241]
  - See the President's Management Council (PMC) section for full description.

4.10 OMB Budget Resource Management Offices (RMOs)[242]

OMB has five RMOs, organized by agency and by program area. These offices, together with OMB's Budget Review Division, help to carry out OMB's central activity of assisting the President in overseeing the preparation of the Federal Budget and supervising its administration of Executive Branch agencies.

---

[233] OMB M-18-19. Improving the Management of Federal Programs and Projects through Implementing the Program Management Improvement Accountability Act (PMIAA). 6/25/2018. https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-19.pdf

[234] CIO Council. https://www.cio.gov/

[235] OMB M-19-23. Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Leaming Agendas, Personnel, and Planning Guidance. 7/10/2019. https://www.whitehouse.gov/wp-content/uploads/2019/07/M-19-23.pdf

[236] CAO. Chief Acquisition Officers Council. https://cao.gov/cao-home

[237] CFO. About the Chief Financial Officers Council. https://www.cfo.gov/about-the-council/

[238] CHCOC. Council Charter. https://www.chcoc.gov/content/council-charter

[239] FPC. Vision and Purpose. https://www.fpc.gov/learn-about-federal-privacy-program/

[240] PIC. Performance Improvement Council. https://www.pic.gov/who-we-are/the-council/

[241] GSA. President's Management Council (PMC). https://www.gsa.gov/governmentwide-initiatives/shared-solutions-and-performance-improvement/presidents-management-council-pmc

[242] The White House. The Mission and Structure of the Office of Management and Budget. https://obamawhitehouse.archives.gov/omb/organization_mission/#:~:text=In%20helping%20to%20formulate%20the,agencies%20to%20set%20funding%20priorities.

In helping to formulate the President's spending plans, RMOs assess the effectiveness of agency programs, policies, and procedures, weigh competing funding demands within and among agencies, and help work with agencies to set funding priorities. Once the Budget is enacted, RMOs are responsible for the execution of Federal budgetary policies and provide ongoing policy and management guidance to Federal agencies. As part of these and other responsibilities, RMOs provide analysis and evaluation, oversee implementation of policy options, and support government-wide management initiatives.

Visit MAX.gov[243] to find agency assigned RMOs.

4.11 Performance Improvement Council (PIC)[244]

The PIC, a government-wide body that supports cross-agency collaboration and best practice sharing, was established under Executive Order 13450[245] in 2007 and codified in law under the GPRA Modernization Act of 2010. The PIC is chaired by the Deputy Director for Management at OMB within EOP. The membership of the PIC includes PIOs and associated staff from federal agencies.[246] PIC.gov is where the Council shares priorities, news, and information about key performance management topics.[247]

4.12 President's Management Council (PMC)[248]

The PMC advises the President and OMB on government reform initiatives, provides performance and management leadership throughout the Executive Branch, and oversees implementation of government-wide management policies and programs. The PMC comprises the [COO] of major Federal Government agencies, primarily Deputy Secretaries, Deputy Administrators, and agency heads from GSA and OPM.

4.13 Congress / Legislative Affairs

Established by Article I of the Constitution, the Legislative Branch consists of the House of Representatives and the Senate, which together form the United States Congress. The Constitution grants Congress the sole authority to enact legislation and declare war, the right to confirm or reject many Presidential appointments, and substantial investigative powers.[249]

Within federal agencies are legislative affairs offices that coordinate legislative activity for the agency and serve as the primary liaison to Members of Congress and their congressional staff. They develop and implement strategies to advance their agency's legislative initiatives, respond to inquiries from Congress, and keep senior leadership and OMB informed about the activities of Congress.

---

[243] The website MAX.gov is only accessible to federal employees.

[244] PIC. Performance Improvement Council. https://www.pic.gov/who-we-are/the-council/

[245] The White House. Executive Order 13450 - Improving Government Program Performance. 11/13/2007. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/performance_pdfs/eo13450.pdf

[246] PIC. About the Council. https://www.pic.gov/who-we-are/the-council/

[247] Ibid.

[248] GSA. President's Management Council (PMC). https://www.gsa.gov/governmentwide-initiatives/shared-solutions-and-performance-improvement/presidents-management-council-pmc

[249] The White House. The Legislative Branch. https://www.whitehouse.gov/about-the-white-house/the-legislative-branch/

Agency CIOs are subject to testify before Congress to articulate the agency's position on proposed legislation and/or progress towards initiatives, policies, and programs.

4.14 General Counsel

The General Counsel is the chief legal officer of the agency, providing legal advice and representation to GSA officials while ensuring implementation of GSA's statutory responsibilities. The lawyers within an agency's Office of General Counsel provide legal counsel to agency policy-makers, providing critical input to rules, regulations, and guidance documents that are promulgated and issued to implement an agency's statutory obligations. Each agency's OGC varies in organization and structure to meet individual agency-specific mission and needs.

An agency's general counsel can be an important partner for the CIO on a variety of IT-related initiatives. Your agency's GC will be a key stakeholder in IT procurement and contract management, as well as meeting policy and statutory requirements for IT management and information security compliance.

4.15 Senior Agency Official for Privacy (SAOP)[250]

The SAOP, designated by the head of each agency, has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.

- **Policy Making:** The SAOP shall have a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals that have privacy implications. In this role, the SAOP shall ensure that the agency considers and addresses the privacy implications of all agency regulations and policies, and shall lead the agency's evaluation of the privacy implications of legislative proposals, congressional testimony, and other materials pursuant to OMB Circular No. A-19.7.
- **Compliance:** The SAOP shall have a central role in overseeing, coordinating, and facilitating the agency's privacy compliance efforts. In this role, the SAOP shall ensure that the agency complies with applicable privacy requirements in law, regulation, and policy. Relevant authorities include, but are not limited to, the Privacy Act of 1974; the Paperwork Reduction Act of 1995; the E-Government Act of 2002; the Health Insurance Portability and Accountability Act of 1996; OMB Circular A-130; Privacy Act Implementation: Guidelines and Responsibilities; 13 OMB Circular A-108; OMB's Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988; and OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
- **Risk Management:** The SAOP shall manage privacy risks associated with any agency activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems. The SAOP's review of privacy risks shall begin at the earliest planning and development stages of agency actions and policies that involve PII and continue throughout the life cycle of the programs or information

[250] OMB M-16-24. Role and Designation of Senior Agency Officials for Privacy. 9/15/2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m_16_24_0.pdf

systems. Appropriately managing privacy risks may require agencies to take steps beyond those required in law, regulation, and policy.

Federal Privacy Council (FPC)[251]

- The FPC is the principal interagency forum to improve the privacy practices of agencies and entities acting on their behalf. The work of the Federal Privacy Council shall strengthen protections of people's personal information and privacy rights across the Federal Government. To achieve this purpose, the Federal Privacy Council shall: support interagency efforts to protect privacy and provide expertise and assistance to agencies; expand the skill and career development opportunities of agency privacy professionals; improve the management of agency privacy programs by identifying and sharing lessons learned and best practices; and promote collaboration between and among agency privacy professionals to reduce unnecessary duplication of efforts and to ensure the effective, efficient, and consistent implementation of privacy policy government-wide.[252] FPC.gov is where the Council shares priorities, key privacy policies, news, and the programs and events sponsored by the Council.[253]

4.16 Senior Agency Official for Records Management (SAORM)[254]

The Federal Records Act (FRA) requires the head of each Federal agency to establish and maintain an active, continuing program for the economical and efficient management of the records of the agency. To this end, the SAORM acts on behalf of the agency head to ensure the agency efficiently and appropriately complies with all applicable records management statutes, regulations, NARA policy, and OMB policy. The SAORM bridges the gap between the agency head and the Agency Records Officer in order to provide strategic direction for the agency's records management program.

The SAORM also promotes effective records management at a senior level by seeing across program offices in the deployment of individual IT systems. The SAORM advocates for the records management program ensuring adequate resources are embedded into the agency's Strategic Information Resources Management (IRM) Plan.[255] The SAORM must directly, and regularly, work with the Agency Records Officer and other appropriate officials to oversee the successful implementation of the agency's records management program.

The SAORM must coordinate the agency's records management program with other related disciplines such as information security, risk management, data management, and knowledge management. This may also include programs related to discovery, privacy, and the Freedom of Information Act (FOIA). As

[251] FPC. Vision and Purpose. https://www.fpc.gov/learn-about-federal-privacy-program/
[252] FPC. Vision and Purpose. https://www.fpc.gov/vision-and-purpose/
[253] Ibid.
[254] NARA Bulletin 2017-02. Guidance on Senior Agency Officials for Records Management. 9/28/2017. https://www.archives.gov/records-mgmt/bulletins/2017/2017-02-html
[255] 44 U.S.C. §3506. US Federal Information Policy. Federal Agency Responsibilities. https://www.law.cornell.edu/uscode/text/44/3506

the agency's information framework develops and matures, the SAORM should integrate the records management program within the framework.

The SAORM's overall responsibilities include:

- Setting the vision and strategic direction for the agency records management program, including incorporating these goals into the agency's Strategic IRM Plan;
- Advocating for the agency's records management program and ensuring that it documents the organization's activities and decisions;
- Ensuring the agency protects records against unauthorized removal or loss and ensures all agency staff are informed of their records management responsibilities as defined in NARA regulations and guidance;
- Submitting reports to NARA, supporting records management inspections, and other oversight activities;
- Ensuring agency staff are informed of and receive training on their records management responsibilities as defined in NARA regulations and guidance;
- Formally designating the Agency Records Officer and informing NARA in writing of this decision; and
- Ensuring compliance with NARA requirements for electronic records including:

    - Managing all permanent electronic records electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format; and
    - Managing all email records electronically and retaining them in an appropriate electronic system that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records consistent with NARA-approved disposition authorities and regulatory exceptions.

05
SECTION

KEY ORGANIZATIONS

5. Key Organizations

5.1 Office of Management & Budget (OMB)

OMB is responsible for overseeing Federal agencies' information technology practices. As a part of this core function, OMB develops and ensures implementation of policies and guidelines that drive enhanced technology performance and budgeting across the Executive Branch. The Federal CIO heads OMB's Office of E-Government and Information Technology (E-Gov), which develops and provides direction in the use of Internet-based technologies. The two major policies and guidelines are FITARA and FISMA.

With FITARA, the Common Baseline was set forth and the role of Agency CIOs was expanded with increased responsibilities through the National Defense Authorization Act for Fiscal Year 2015.[256] Per OMB M-15-14, the specific requirements of FITARA include:

- Agency CIO Authority Enhancements
- Enhanced Transparency and Improved Risk Management in IT Investments
- Portfolio Review
- Federal Data Center Consolidation Initiative
- Expansion of Training and Use of IT Cadres
- Maximizing the Benefit of the Federal Strategic Sourcing Initiative
- Governmentwide Software Purchasing Program[257]

With FISMA, information security requirements were set forth based on NIST compliance documents.[258] FISMA requires annual evaluations of the information security program at each federal agency, which are reviewed by DHS and OMB, and incorporated into an annual report to Congress. FISMA states:

- The Director [OMB] shall oversee agency information security policies and practices, including developing and overseeing the implementation of policies, principles, standards, and guidelines on information security.
- Not later than March 1 of each year, the Director [OMB], in consultation with the Secretary [DHS], shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year.

Each year, not later than such date established by the Director [OMB], the head of each agency shall submit to the Director [OMB] the results of [their agency's] evaluation required under this section.[259]

---

[256] Public Law 113-291. Sec. 831. National Defense Authorization Act for Fiscal Year 2015. https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf#page=148%5D

[257] OMB M-15-14. Management and Oversight of Federal Information Technology. 6/10/2015. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf

[258] NIST. Federal Information Security Management Act (FISMA) Implementation Project. https://www.nist.gov/programs-projects/federal-information-security-management-act-fisma-implementation-project

[259] CIO Council. CISO Handbook. https://www.cio.gov/assets/resources/CISO_Handbook.pdf

5.2 General Services Administration (GSA)

GSA provides many services to the Federal Government. CIOs should be aware that GSA provides management and administrative support and establishes acquisition vehicles for agencies' use. GSA's information technology acquisition services and offerings are updated along with government-wide policy and are offered through collaboration with DHS, OMB, and other organizations both inside and outside the Federal Government.

GSA collaborates with OMB to sponsor Executive Councils for inter-agency communication and also assist OMB in the development of government-wide policies and guidance.[260]

GSA also has an important role in procuring products and services for the government and administers the Federal Acquisition Service (FAS).[261] The FAS possesses the capability to deliver comprehensive products and services across the government at the best possible value. The continuum of solutions available through FAS include:

- Products and Services
- Technology
- Motor Vehicle Management
- Transportation
- Travel
- Procurement and Online Acquisition Tools

Technology Transformation Services

GSA's Technology Transformation Services (TTS) applies modern methodologies and technologies to improve the lives of the public and public servants. They help agencies make their services more accessible, efficient, and effective with modern applications, platforms, processes, personnel, and software solutions.[262]

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[263] The program was established through an OMB Memorandum in December 2011[264] and included the FedRAMP Joint Authorization Board (JAB), which is made up of representatives from DOD, DHS, and GSA. The JAB must authorize any cloud services that will hold federal data. Additionally, GSA established the FedRAMP Program Management Office (PMO) which provides the process for Executive departments and agencies, as well as cloud service providers (CSPs), to adhere to the FedRAMP security authorization requirements created by the JAB.

---

[260] GSA.Shared Solutions and Performance Improvement. https://www.gsa.gov/governmentwide-initiatives/shared-solutions-and-performance-improvement

[261] GSA. Federal Acquisition Service. https://www.gsa.gov/about-us/organization/federal-acquisition-service

[262] GSA. Technology Transformation Services. https://www.gsa.gov/about-us/organization/federal-acquisition-service/technology-transformation-services

[263] FedRAMP. FedRAMP Authorization. https://www.fedramp.gov/about/

[264] FedRAMP. Policy: Security Authorization of Information Systems in Cloud Computing Environments. 12/8/2011. https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

Per FISMA, agencies must authorize the information systems they use, and these requirements apply to cloud services through FedRAMP. As with FISMA, FedRAMP utilizes the NIST SP 800-53 security controls as a baseline, with additional controls unique to cloud computing. As of September 2020, there have been 200 authorized cloud products through FY19-20, which is up from 100 authorizations between FY13-18.[265]

Information on agency authorization for a cloud service offering (CSO) can be found at FedRAMP.gov.

Data Center and Cloud Optimization Initiative Program Management Office (DCCOI PMO)

The GSA DCCOI PMO[266] helps agencies meet the legislative requirements of FITARA, as well as OMB M-19-19, Update to Data Center Optimization Initiative (DCOI).[267] The DCCOI PMO is OMB's managing partner of the DCOI and manages the Cloud and Infrastructure Community of Practice (C&I CoP), supports Cloud Smart and provides best practices and a procurement guide for cloud technology, and supports Application Rationalization by capturing best practices and case studies and assisting agencies with pilots and ongoing implementation support. CIOs may leverage the C&I CoP's expertise and utilize the DCCOI PMO's capabilities including agency-specific DCOI IDC analysis, Cloud Smart, and Application Rationalization processes.

5.3 Department of Homeland Security (DHS)

The Cybersecurity Information Sharing Act of 2015 gives responsibility to the DHS, Director of National Intelligence (DNI), Department of Defense (DoD) and Department of Justice (DOJ) to "develop procedures to share cybersecurity threat information with private entities, non federal agencies, state, tribal, and local governments, the public, and entities under threats."[268] FISMA 2014 amended FISMA 2002 by "codifying DHS authority" to oversee information security policies for non-national security federal Executive Branch systems.[269]

In accordance with CISA, DHS must establish processes where private sector entities can share information about cybersecurity threats with the Federal Government. DHS manages the delivery and adoption of BODs to federal agencies.

The United States Computer Emergency Readiness Team (US-CERT) works within DHS to prevent cyberthreats and coordinate incident response activities. US-CERT works with federal agencies, private sector, research entities, state and local government and international groups to protect the national technology landscape.[270] The Continuous Diagnostics and Mitigation (CDM) Program "delivers

---

[265] FedRAMP. FedRAMP Reaches 200 Authorizations. 9/17/2020. https://www.fedramp.gov/fedramp-reaches-200-authorizations/

[266] CIO Council. The DCCOI PMO. https://www.cio.gov/about/members-and-leadership/cloud-infrastructure-cop/about-the-DCCOI-PMO/

[267] OMB M-19-19. Update to Data Center Optimization Initiative (DCOI). 6/25/2019. https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-19-Data-Centers.pdf

[268] S.754 - Cybersecurity Information Sharing Act of 2015. https://www.congress.gov/bill/114th-congress/senate-bill/754

[269] CISA. The Federal Information Security Modernization Act of 2014. https://www.cisa.gov/federal-information-security-modernization-act

[270] US-CERT. Infosheet. https://us-cert.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf

automated tools" to federal agencies to build defense against threats to the national technology infrastructure.[271]

Cybersecurity and Infrastructure Security Agency (CISA)
CISA is one of the newest federal agencies, established as an independent operational component of DHS in 2018 through the expansion of DHS's National Protection and Programs Directorate (NPPD). CISA is responsible for the national capacity to defend against cyber-attacks, and CISA works with the federal government to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard ".gov" networks. Additionally, CISA houses the National Risk Management Center (NRMC) which is tasked with planning, analysis, and collaboration to identify and address significant risks to critical infrastructure.

CISA's Cybersecurity Division is the focal point for cybersecurity and related IT systems, and is tasked with seven primary functions:

1. Capability Delivery
2. Threat Hunting
3. Operational Collaboration
4. Vulnerability Management
5. Capacity Building
6. Strategy, Resources & Performance
7. Cyber Defense Education & Training

CISA also maintains a Cyber Resource Hub[272] which includes a range of voluntary cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. Additional information including Best Practices, case studies, training and exercises, and information about CISA's Annual National Cybersecurity Summits can be found on the CISA.gov website.

Continuous Diagnostic Mitigation (CDM) Program
The CDM Program works under CISA to strengthen the cybersecurity of federal departments and agencies. CDM offers "industry-leading, commercial off-the-shelf (COTS) tools to support technical modernization as threats change." This program meets FISMA mandates and delivers four main objectives: reducing threats at the agency level, increasing visibility into the strengths of federal cybersecurity, improving cybersecurity response capabilities, and streamlining FISMA reporting.

US-CERT
US-CERT works under CISA to prevent cyberthreats and coordinate incident response activities. US-CERT works with federal agencies, private sector, research entities, state and local government and international groups to protect the national technology landscape.[273]

[271] CISA. Continuous Diagnostics and Mitigation (CDM). https://www.cisa.gov/cdm
[272] CISA. Cyber Resource Hub. https://www.cisa.gov/cyber-resource-hub
[273] US-CERT. Infosheet. https://us-cert.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf

Core Activities:

- Providing cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities.
- Developing timely and actionable information for distribution to Federal departments and agencies; state, local, tribal, and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations.
- Responding to incidents and analyzing data about emerging cybersecurity threats.
- Collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.[274]

5.4 National Institute of Standards and Technology (NIST)[275]

A bureau of the Department of Commerce (DOC), NIST provides Federal standards and technical resources on information security that CISOs use to ensure agencies effectively manage risk, and OIG uses to evaluate maturity. OMB and DHS leverage NIST guidance as they develop mandates and initiatives. NIST creates mandatory Federal Information Processing Standards (FIPS) and provides management, operational, and technical security guidelines on a broad range of topics, including incident handling and intrusion detection, the establishment of security control baselines and strong authentication.

- NIST publications are collected online in the Computer Security Resource Center (CSRC). NIST develops standards and guidance through a deliberative process with both Federal and civilian input.
- The Framework for Improving Critical Infrastructure Cybersecurity(referred to as the NIST Cybersecurity Framework)[276] provides a common taxonomy and mechanism for organizations to:
    - Describe their current and target cybersecurity postures,
    - Identify and prioritize opportunities for improvement,
    - Assess progress toward their target, and
    - Communicate among internal and external stakeholders about cybersecurity risk.
- Each agency's OIG considers FIPS and SPs when evaluating the effectiveness of agency information security programs. NIST encourages tailoring of guidance to agency needs. OIG expects those tailoring decisions and associated risk decisions to be reflected in the organization's policies, procedures, and guidance.
- The NIST Risk Management Framework (RMF)[277] provides a foundational process that integrates security and risk management activities into the system development life cycle and brings many of the NIST documents together into an overall approach to managing risk.
- NIST's National Cybersecurity Center of Excellence (NCCoE) is a collaborative hub where industry organizations, Government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues.

[274] CIO Council. CISO Handbook. https://www.cio.gov/assets/resources/CISO_Handbook.pdf
[275] CIO Council. CISO Handbook. https://www.cio.gov/assets/resources/CISO_Handbook.pdf
[276] USDOC. NIST Cybersecurity Framework. https://www.nist.gov/cyberframework
[277] NIST. FISMA Implementation Project. https://csrc.nist.gov/projects/risk-management/rmf-overview

5.5 Government Accountability Office (GAO)

GAO, headed by the Comptroller General of the United States, is an independent, nonpartisan agency that works for Congress. As part of their mission to investigate how the Federal Government spends taxpayer dollars, they conduct evaluations of agencies' information security policies and practices.[278] The House Committee on Oversight and Reform working with GAO releases a scorecard every six months evaluating federal agencies' implementation of FITARA.[279]

In 2004, GAO recommended to Congress in GAO-04-823 a restructuring of the IT management and reporting responsibilities for the CIO. The GAO identified the full scope of the CIO role and any needed revisions to the Clinger-Cohen Act to increase the efficiency and strength of this title in GAO-11-634. A 2017 GAO forum identified key tasks and actions to strengthen FITARA and enhance the CIO role. In 2018, GAO published a report GAO-18-93 with proposals to OMB and 24 federal agencies to increase CIO efficiency in fulfilling their responsibilities in each of six IT management areas. OMB released FITARA guidance requiring CAOs to accurately inform CIOs of IT contracts for revision and approval. GAO explored in GAO 18-42 the role of CIOs in reviewing and approving IT acquisitions. In the findings, GAO strongly advised federal agencies to "involve the acquisition office in their process to identify IT acquisitions for CIO review, as required by OMB."[280]

GAO Auditing

GAO is an independent, nonpartisan agency that is headed by the Comptroller General and works for Congress and is tasked with examining how taxpayer dollars are spent and providing Congress and federal agencies with objective and reliable information to help the government save money and work more efficiently.[281] One of the GAO's functions is auditing government entities in order to provide essential accountability and transparency over government programs, as well as providing best practices. GAO works with the House Committee on Oversight and Reform to release a scorecard every six months grading federal agencies on their implementation of FITARA. The FITARA scorecard reflects agency performance in eight FITARA-related categories: incremental development, risk reporting, portfolio management, data-center consolidation, software licensing, modernizing government technology, information security management, and CIO reporting structure.[282] GAO's auditing standards can be found in the Yellow Book and GAO provides additional standard-setting guides such as the Financial Audit Manual, Federal Information Systems Controls Audit Manual, and the Standards for Internal Control in the Federal Government, also known as the Green Book.[283] GAO's reports are submitted to Congress and in the reports, GAO will often make recommendations to OMB and agencies. One recent and relevant GAO report is GAO-18-93, [Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities] which identified

[278] GAO. About GAO - Overview. https://www.gao.gov/about/

[279] House Committee on Oversight and Reform. FITARA 9.0. 12/11/2019 https://oversight.house.gov/legislation/hearings/fitara-90

[280] GAO-18-42. Agencies Need to Involve Chief Information Officers in Reviewing Billions of Dollars in Acquisitions. January 2018. https://www.gao.gov/assets/690/689345.pdf

[281] GAO. About GAO - Overview. https://www.gao.gov/about

[282] House Committee on Oversight and Reform. FITARA 9.0. 12/11/2019 https://oversight.house.gov/legislation/hearings/fitara-90

[283] GAO. About GAO - Role as an Audit Institution. https://www.gao.gov/about/what-gao-does/audit-role/

problems, made recommendations, and helped lead to EO 1388, [Enhancing the Effectiveness of Agency Chief Information Officers].[284]

5.6 Office of the Inspector General (OIG)

The Inspector General Act of 1978 created twelve Offices of Inspector General and by 2019, this number grew to "74 statutory Inspector General's operating in the federal government."[285] Congress passed the IG Act to assign duties to each OIG to investigate and audit programmatic activities, foster efficiency and prevent "fraud and abuse in the programs administered by each agency."[286]

OIG conducts investigations and reviews to oversee the efficiency, effectiveness, financial health and safety of the agencies they serve. FISMA requires each agency's Inspector General (IG) to conduct a yearly independent review of informational security practices. The CIO Council in collaboration with OMB, DHS and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) develops metrics for these evaluations which are updated annually.

5.7 National Archives and Records Administration (NARA)

NARA preserves documents, materials and records involving the Federal Government.[287] NARA collects and maintains declassified information and makes it available for research purposes. In 2019, OMB issued Memorandum M-19-21 providing guidance to all federal agencies to manage records digitally by December 31, 2022, requiring NARA to be accessible in a fully electronic format.[288] This terminated any paper or hard copy systems involving the maintenance of electronic records.

NARA defines essential records as documentation allowing agencies to fulfill their operational needs under a national security threat or emergency, or to safeguard the legal and financial rights of the Federal Government.[289] NARA directs the heads of federal agencies with specific responsibilities in managing essential records including:

- Create and maintain records for the agency;
- Establish programs to manage records to properly identify information for public disclosure and in a digital format, among other standards;
- Transfer of records to record centers;
- Developing protections to prevent loss of records; and
- Notifying Archivist of unlawful activities.

---

[284] GAO-18-93. Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities. August 2018. https://www.gao.gov/assets/700/693668.pdf

[285] Congressional Research Service. Statutory Inspectors General in the Federal Government: A Primer. 1/3/2019. https://crsreports.congress.gov/product/pdf/R/R45450

[286] H.R.8588 - Inspector General Act of 1978. https://www.congress.gov/bill/95th-congress/house-bill/8588

[287] NARA. About the National Archives. https://www.archives.gov/about

[288] OMB M-19-21. Transition to Electronic Records. 6/28/2019. https://www.archives.gov/files/records-mgmt/policy/m-19-21-transition-to-federal-records.pdf

[289] NARA. Essential Records Guide. August 2018. https://www.archives.gov/files/records-mgmt/essential-records/essential-records-guide.pdf

NARA's Code of Federal Regulations require agencies to establish electronic information systems and evaluate them to check for accuracy. Otherwise, "agencies must submit an SF 115, Request for Records Disposition Authority, to NARA."[290]

[290] 36 C.F.R. §1236.26(a). Electronic Records Management. https://www.ecfr.gov/cgi-bin/text-idx?SID=2cb32d56fb6af59e4b4ee022f092b321&mc=true&node=pt36.3.1236&rgn=div5

06
SECTION

POLICIES & INITIATIVES

6. Policies & Initiatives

6.1 President's Management Agenda (PMA)

The PMA lays out a long-term vision for modernizing the Federal Government in key areas that will improve the ability of agencies to deliver mission outcomes, provide excellent service, and effectively steward taxpayer dollars on behalf of the American people.

- **Mission:** The American people count on the Federal Government every day, from national security to infrastructure to food and water safety. Public servants must be accountable for mission-driven results but must also have the necessary tools and resources to deliver.
- **Service:** Federal customers range from small businesses seeking loans, to families receiving disaster support, to veterans owed proper benefits and medical care. They deserve a customer experience that compares to—or exceeds—that of leading private sector organizations, yet most Federal services lag behind the private sector.
- **Stewardship:** Effective stewardship of taxpayer funds is a crucial responsibility of Government, from preventing fraud to maximizing impact. Taxpayer dollars must go to effective programs that produce results efficiently.

Cross Agency Priority (CAP) Goals[291]

CAP Goals [are] established to drive implementation of the PMA and tackle critical government-wide challenges that cut across agencies. The CAP Goals provide the components of the Federal Government Performance Plan required by the GPRA Modernization Act of 2010. CAP Goals are a tool used by leadership to accelerate progress on a limited number of Presidential priority areas where implementation requires active collaboration among multiple agencies. Long-term in nature, CAP Goals drive cross-government collaboration to tackle government-wide management challenges affecting most agencies.

CAP Goals fall into four categories: key drivers of transformation, cross-cutting priority areas, functional priority areas and mission priority areas.

6.2 PortfolioStat

PortfolioStat is a tool for agencies to use to assess the current maturity of their [IT portfolio] and make decisions on eliminating duplication across their organizations.[292] Launched by OMB in March of 2012, PortfolioStat has yielded over $2.57 billion[293] in savings or cost avoidance.

PortfolioStat consists of a yearly review of agency portfolio management between the Federal CIO and senior agency officials. In addition to helping agencies achieve financial savings through reform efforts, PortfolioStat analyzes agency progress using a variety of performance metrics designed to measure

[291] The White House. Cross-Agency Priority Goals Overview. https://www.performance.gov/CAP/overview/

[292] OMB. PortfolioStat. https://itdashboard.gov/#analyze-pstat

[293] OMB M-12-10. Implementing PortfolioStat. 3/30/2012. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2012/m-12-10_1.pdf

whether agencies are delivering their IT investments on budget and on schedule, driving innovation to meet customer needs, and adequately protecting Federal IT Assets and Information.[294]

To support this process, OMB is requiring that each agency take the following actions:

- Designate Lead for Initiative
- Complete a High-Level IT Portfolio Survey
- Establish a Commodity IT Investment Baseline
- Submit a Draft Plan to Consolidate Commodity IT
- Hold PortfolioStat Session
- Submit a Final Plan to Consolidate Commodity IT
- Migrate at Least Two Duplicative Commodities IT Services
- Document Lessons Learned

PortfolioStat is a data-driven tool that agencies use to assess the current maturity of their IT portfolio management processes and select PortfolioStat action items to strengthen their IT portfolio. Covered agencies shall hold PortfolioStat sessions on a quarterly basis with OMB, the agency CIO, and other attendees. These sessions were previously annual and required the attendance of the agency deputy secretary (see Implementing PortfolioStat (M-12-10), Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management (M-13-09), and Fiscal Year 2014 PortfolioStat (M-14-08).[295]

6.3 TechStat

A TechStat is a face-to-face, evidence-based accountability review between OMB and a covered agency of an IT program with that agency's leadership. TechStat sessions are a tool for getting ahead of critical problems in an investment, turning around underperforming investments, or terminating investments if appropriate. Agencies report the outcomes of all TechStat sessions through the quarterly IDC process.[296]

6.4 Capital Planning and Investment Control (CPIC)

The Clinger Cohen Act of 1996 requires OMB to establish a budget process of analyzing, tracking, and evaluating the risks and results of IT projects. The law requires federal executive departments and agencies use the CPIC process outlined by OMB Circular A-130.[297]

CPIC is a systematic approach to selecting, managing, and evaluating information technology investments. Every year, agencies report IT investments to OMB to inform the President's Budget.[298]

---

[294] OMB. PortfolioSTAT. https://itdashboard.gov/#analyze-pstat

[295] OMB M-15-14. Management and Oversight of Federal Information Technology. 6/10/2015. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf

[296] OMB. Implementation Guide - FITARA. https://management.cio.gov/implementation/

[297] OMB Circular A-130. Managing Information as a Strategic Resource. Policy. July 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[298] USDA. Capital Planning and Investment Control. https://www.ocio.usda.gov/about-ocio/information-resource-management/capital-planning-and-investment-control

OMB requires agency CIOs, SAOPs, CFOs, and budget officers coordinate to ensure that IT budget data is consistent with the agency's budget submission.

6.5 Technology Business Management (TBM)

TBM is an IT management framework that implements a standard way to categorize IT costs, technologies, resources, applications, and services in order to disaggregate IT spending into consistent categories to provide CIOs with a detailed understanding of their organization's IT costs. These categories include the Finance View, IT View, and the Business View. Additionally, TBM further enables FITARA implementation and helps to benchmark IT spending, improve acquisitions, and enhance understanding of IT investment costs. Full realization of TBM is intended to connect IT to business value, support partnerships between IT and mission teams throughout agencies, and break down data silos across organizations.[299]

GSA worked with the Department of Education (ED) to develop the TBM Playbook which is designed to assist federal agencies as they begin TBM implementation by offering guidance and lessons learned.[300] The seven plays to improve chances of beginning a successful TBM implementation include:

- Identify key players and stakeholders
- Determine current state
- Identify measurable desired outcome
- Start aligning data
- Look for insights
- Rollout and adoption
- Keep maturing the TBM implementation

6.6 Data Center and Cloud Optimization Initiative (DCCOI)

M-19-19, enacted in June 2019, established the DCCOI which replaced the previous DCOI from M-16-19. Compared to M-16-19, key features of M-19-19 include:

- Continuation of the development freeze for new and current data centers;
- Continuation of consolidation and closure of existing data centers;
- Alignment of consolidation and closure of existing data centers with the Cloud Smart[301] strategy;
- Continuation of the DCCOI PMO;
- Increased alignment with the PMA;[302]
- Broadening of the exemptions for some data centers from closures that did not fit the definition set forth in M-16-19 (e.g. unique examples from embassy file servers to dam floodgate controls, federal labs and research facilities) with provisional exemptions applied by OMB after justified agency requests;
- Updated closures and cost savings targets; and

[299] CIO Council. Technology Business Management. https://www.cio.gov/policies-and-priorities/tbm/
[300] GSA. Technology Business Management Playbook. https://tech.gsa.gov/playbooks/tbm/
[301] OMB. Federal Cloud Computing Strategy. https://cloud.cio.gov/strategy/
[302] The White House. President's Management Agenda. https://www.performance.gov/PMA/PMA.html

- Updated performance metrics to focus less on averages and more on continuous improvement.

In terms of specific performance metrics, M-19-19 adds a metric for planned hours of availability for each data center, updates the advanced energy metering, virtualization, and server utilization metrics, and removes the energy efficiency and facility utilization metrics.

6.7 Federal Data Strategy

The Federal Data Strategy, conceptualized in the 2018 PMA[303] and issued by OMB as M-19-18 in June 2019, provides a framework of operational principles and best practices to help agencies leverage consistent data infrastructure and strong data governance over the next ten years.[304] The Federal Data Strategy is complementary to current statutory requirements and OMB information policy and guidance. Included in the Federal Data Strategy is a set of principles including Ethical Governance, Conscious Design, and Learning Culture, as well as a set of 40 practices to guide agency data management activities.

To assist with implementing the Federal Data Strategy, OMB provided the 2020 Federal Data Strategy Action Plan[305] which identifies six Agency Actions, four Community of Practice Actions, and ten Shared Solution Actions to be completed in 2020, the initial implementing year. The 2020 Action Plan can be found at strategy.data.gov. The 2021 Federal Data Strategy Action Plan is in final review as of this publication.

6.8 High Value Assets (HVAs)

The HVA initiative was created in 2015 by OMB and DHS and established the capability for CFO Act agencies to assess agency HVAs, identify critical areas of weakness, and develop plans to remediate those weaknesses. HVAs are those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification or destruction could cause significant impact to the United States' nations security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. Guidance and policies germane to HVAs include: the Cybersecurity Strategy and Implementation Plan (CSIP) which was issued as OMB Memorandum M-16-04 in October 2015,[306] the initial implementing guidance for management of Federal HVAs which was issued by OMB as Memorandum M-17-09[307] in December 2016, and

[303] The White House. President's Management Agenda. April 2018. https://www.whitehouse.gov/wp-content/uploads/2018/03/Presidents-Management-Agenda.pdf
[304] OMB M-19-18. Federal Data Strategy - A Framework for Consistency. 6/4/2019. https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf
[305] PMA. Federal Data Strategy 2020 Action Plan. https://strategy.data.gov/assets/docs/2020-federal-data-strategy-action-plan.pdf
[306] OMB M-16-04. Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. 10/30/2015. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf
[307] OMB M-17-09. Management of Federal High Value Assets. 12/9/2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf

Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure[308] which was issued in May 2017.

New guidance for the HVA program was issued by OMB as Memorandum M-19-03 in December 2018.[309] This guidance consolidates and updates the previous requirements and rescinds the prior OMB memoranda, while also expanding the applicability of the HVA program from CFO Act agencies to all agencies. Agencies must take a strategic, enterprise-wide view of cyber risk to unify the protection of HVAs against evolving cyber threats. Specifically, agencies must:

- Designate an integrated agency-level office, team, or other governance structure to enable the incorporation of HVA activities (e.g. assessment, remediation, incident response) into broader agency planning activities for information system security and privacy management, and COOs must regularly coordinate with these governance structures to ensure HVA activities are executed in a timely manner.
- Establish, evaluate, and update HVA information sharing agreements with OMB, DHS, and other agencies to promote cross-agency sharing, coordination, and cooperation.

The M-19-03 guidance also establishes a new categorization system for the designation of HVAs by agencies. Agencies may designate Federal information or a Federal information system as an HVA if it relates to one or more of the following categories: Informational Value, Mission Essential, or Federal Civilian Enterprise Essential. Additionally, while agencies are principally responsible for their HVA designation, OMB and DHS reserve the right to designate HVAs at agencies based on potential impact to national security.

6.9 Budget Line of Business (LoB)

The Budget LoB on MAX.gov[310] is a partnership between the PMO housed at the Department of Education, the Budget Systems Branch at OMB, and 27 partner agencies.[311] The goal of the Budget LoB is working together in order to build budget offices for the future by sharing information and best practices across the Federal Government. The focus of the Budget LoB is centered around three categories: processes, technology, and training and career development. Specific products include a solutions catalog which includes a comprehensive list of products, use cases, and training developed by the community, a budget systems inventory which reviews the systems agencies are using for various budget processes, project management for ongoing projects, as well as hosting training and events. The Budget LoB offers a monthly newsletter, monthly Task Force meetings, workgroup meetings once every few months, as well as a federal detailee program for emerging leaders.

Budget Process

[308] Executive Order 13800. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 5/11/2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[309] OMB M-19-03. Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program. 12/10/2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

[310] The website MAX.GOV is only accessible to federal employees.

[311] OMB. About the Budget LOB. https://community.max.gov/display/Budget/About+the+Budget+LoB

Each year, Congress works on a federal budget for the next fiscal year. The government's fiscal year runs from October 1 of one year to September 30 of the next.[312] Planning begins two years in advance; the work actually begins in the executive branch the year before the budget is to go into effect. First, federal agencies create budget requests and submit them to OMB. OMB will refer to the agency requests as it develops the president's budget proposal. The president submits his budget proposal to Congress early the next year. Then Congress, which the Constitution puts in charge of spending and borrowing, starts its work.

Find the detailed budget timeline on the Budget LOB's page on MAX.gov[313] and in the annual OMB Circular A-11.

6.10 Federal Acquisition Regulation (FAR)

The FAR is the set of rules governing the federal government's purchasing process, it is jointly issued by DoD, GSA, and NASA and applies to most agencies in the Executive Branch. A few of the exceptions include agencies which use the DoD: Defense Federal Acquisition Regulations Supplement (DFARS) or the Navy Marine Corps Acquisition Regulation Supplement (NMCARS) or exempt agencies such as the USPS and FDIC.[314] The FAR includes 53 parts which each address a component of the acquisition process, the first twelve parts address general government acquisition matters and acquisition planning, while the remaining parts include other topics such as contracts, contracting, labor laws, taxes, and small businesses.[315] Of note, information technology is Part 39 of the FAR. Overall, the FAR defines the process for sealed bidding, competitive negotiation, cost principles contracts, social-economic obligations, commercial items acquisitions, as well as relevant terms and conditions.

[312] GSA. The Federal Government's Budget Process. https://www.usa.gov/budget#item-213709

[313] The website MAX.gov is only accessible to federal employees.

[314] Federal Deposit Insurance Corporation. Introduction to the Federal Acquisition Regulation (FAR). https://www.fdic.gov/about/diversity/sbrp/45.pdf

[315] Federal Acquisition Regulation (FAR). FY 2019. https://www.acquisition.gov/sites/default/files/current/far/pdf/FAR.pdf

07
SECTION

REPORTING & REPORTING CALENDAR

7. Reporting

7.1 Integrated Data Collection (IDC)

The IDC is the OMB Office of the Federal CIO's (OFCIO) quarterly reporting mechanism to capture data and information related to PortfolioStat, DCOI, and other OFCIO-led initiatives. Agencies determine the individuals responsible for IDC reporting and tend to include a team of individuals from across an agency with a leader who reports to the CIO, Deputy CIO, or CISO. These individuals for each agency can be found in the IDC section of MAX.gov.[316]

OFCIO established the Information Collection Review Board (ICRB)[317] to manage the IDC process on a quarterly basis and make any necessary changes to the reporting instructions. The ICRB ensures that the IDC process is efficient and gathers relevant data while limiting the burden on participating agencies[318].

Each quarter, OFCIO produces the Quarterly IDC Instructions that documents reporting fields and requirements. OFCIO also solicits feedback from reporting agencies and partners to improve the reporting process and remove unnecessary data collections when appropriate. The "Quarter-By Quarter IDC Timeline & Changes" table on MAX.gov collects from the May 2018 IDC quarter and each quarter thereafter, new engagements related to any agency-led TechStats, OMB-led TechStats, or OMB engagements like PortfolioStats; information regarding past engagements; and reporting on any agreed-upon action items resulting from those sessions.[319]

For more information consult the Reporting Calendar.

7.2 CPIC Reporting

The CPIC reporting process includes all stages of capital programming including planning, budgeting, procurement, management, and assessment. OMB's reporting requirements are communicated to federal executive departments and agencies through the annual updates to OMB Circular A-11, Section 55.[320] CIOs are expected to coordinate to ensure that IT budget data is consistent with the agency's budget submission and are also expected to provide a CIO Evaluation Report for all Major Investments and Part 3 Standard Investments. Agency CPIC information is collected through the annual E-Gov MAX collection, which includes the collection of IT investment information for the Previous Year's (PY) actual spend, Current Year (CY) estimated spend, and requested spend in the President's Budget request for the Budget Year (BY). The CPIC reporting process heavily leverages the TBM framework to gain increased granularity about IT spend across federal executive departments and agencies.[321]

---

[316] The website MAX.gov is only accessible to federal employees.

[317] OMB. E-Gov Integrated Data Collection (IDC). https://community.max.gov/x/LhtGJw

[318] Participation varies by reporting activity. See subsequent sections for agency requirements.

[319] OMB. E-Gov Integrated Data Collection (IDC). Attachments. Quarterly IDC Instructions November 2020. https://community.max.gov/pages/viewpage.action?pageId=658905902

[320] CIO Council. Capital Planning and Investment Control (CPIC). https://www.cio.gov/policies-and-priorities/cpic/

[321] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

Agencies are no longer required to submit an IT Resources Statement as part of their agency budget submission to OMB. Other IT related materials are required, as detailed in Section 55, and submitted according to the following IT CPIC Milestones:

- August
    - Draft Agency IT Investment Portfolio Summary submission
    - Verification that the required E-Gov/Line of Business (LoB) contribution levels are being included in the agency's budget plans
- September
    - Agency IT Portfolio Summary submission
    - Agency IT Portfolio Summary Details
- January
    - Final Agency IT Portfolio Summary and IT Portfolio Summary Details based on the President's Budget submissions
- June
    - Optional Mid-Session Review submission

To the extent possible, align budget accounts with programs, distinguishing among components that contribute to different strategic objectives.[322]

For more information consult the Reporting Calendar.

7.3 DCOI Reporting

DCOI reporting is performed through three methods: a data center inventory reported to OMB quarterly, a DCOI strategic plan updated annually, and a list of FITARA milestones updated quarterly.[323] These submissions are expected to be submitted under the direction of the CIO. Additionally, agency-reported public data can be viewed on the IT Dashboard.[324]

The Data Center Inventory involves the quarterly submission of data containing the full inventory of data centers by CFO-Act agencies to OMB for data center and DCOI implementation oversight. This inventory is collected as a part of the IDC and is generally collected for Q1 by the end of February, Q2 by the end of May, Q3 by the end of August, and Q4 by the end of November, though specific dates may vary.[325]

The DCOI Strategic Plan is required as a part of FITARA and involves the annual publication of strategic plans describing the agency's consolidation and optimization strategy. The strategic plan publications each year is reported as a part of the Q2 IDC process for that year and should be published at "[agency].gov/digitalstrategy" in the Data Center Optimization Initiative Strategic Plans category.[326]

---

[322] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Section 51. 2020. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[323] OMB. DCOI - Reporting. https://datacenters.cio.gov/reporting/

[324] OMB. IT Dashboard. https://itdashboard.gov/

[325] OMB. E-Gov Integrated Data Collection (IDC). https://community.max.gov/x/LhtGJw

[326] OMB. Implementation Guidance - FITARA. DCOI Strategic Plan Schema. https://management.cio.gov/schema/#DCOI

Furthermore, agencies are also required to identify at least five FITARA milestones per fiscal year to be achieved through DCOI. These milestones should be published at "[agency].gov/digitalstrategy/FITARAmilestones.json'' and should be updated quarterly as progress is achieved and then reviewed in PortfolioStat sessions.[327]

For more information consult the Reporting Calendar.

7.4 FISMA Reporting

FISMA metrics are aligned to the five functions outlined in NIST's Framework for Improving Critical Infrastructure and Cybersecurity: Identify, Protect, Detect, Respond, and Recover. Annually, OMB releases a memorandum establishing FISMA reporting guidance and deadlines with additional details provided through CyberScope and MAX.[328] FISMA documents are available on the cisa.gov website for each fiscal year of FISMA, while the memorandums are available on the whitehouse.gov website.[329]

Typically, the memorandum is released around October or November for the upcoming fiscal year, see OMB M-20-04 for the FY20 guidance.[330] The memorandum will also specify the reported performance metrics with any Cross Agency Priorities (CAP), as well as provide instructions on report content and details for the development of annual agency FISMA reports. Typical CAP metrics include specific metrics around the categories of Information Security Continuous Monitoring, Identify and Credential Access Management, Anti-Phishing and Malware Defense.

FISMA data is assessed both quarterly and annually. Quarterly, as mandated by OMB and the NSC, agencies are required to collect FISMA performance metrics data and upload the results into CyberScope. This collection typically involves multiple persons working with the responsible POC and is then reviewed by the CISO and CIO prior to being uploaded. The Annual FISMA Report typically consists of three main sections:

- CIO: Implementation of FISMA CAP measures and base measures
- SAOP: Implementation of a Privacy Program in compliance with the Privacy Act
- IG: Questions about security and privacy programs independently answered by the agency IG

Typically, these sections will be completed by the relevant teams within agencies, incorporated into the annual report, reviewed, and then are required to be approved and signed by the head of the agency. Additionally, agencies may also use this time to conduct a FISMA self-assessment to assess and support their FISMA compliance.

---

[327] OMB. Implementation Guidance - FITARA. https://management.cio.gov/

[328] GSA. FISMA Implementation Guide. CIO-IT Security-04-26. 4/16/2019. https://www.gsa.gov/cdnstatic/FISMA_Implementation_Guide_%5BCIO-IT_Security-04-26_Rev2%5D_04-16-2019.pdf

[329] CISA. Federal Information Security Modernization Act. https://www.cisa.gov/federal-information-security-modernization-act

[330] OMB M-20-04. Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements. 11/19/2019. https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf

Finally, the annual report is also required to be submitted to the Chairperson and Ranking Member of the House Committee on Oversight and Government Reform, the House Committee on Homeland Security, the House Committee on Science, Space, and Technology, the Senate Committee on Homeland Security and Government Affairs, the Senate Committee on Commerce, Science, and Transportation, the appropriate authorization and appropriations committees in both the House and Senate, as well as to the GAO and to the Comptroller General of the United States. For more information consult the Reporting Calendar.

7.5 FITARA Reporting

FITARA requires federal agencies to submit annual reports that include:

- Comprehensive data center inventories,
- Multiyear strategies to consolidate and optimize data centers,
- Performance metrics and a timeline for agency action, and
- Yearly calculations of investment and cost savings related to FITARA implementation.[331]

See FITARA section for more information.

7.6 FISMA Report to Congress

OMB publishes a FISMA Annual Report to Congress[332] each fiscal year which includes data reported by agencies to OMB and CISA highlighting government-wide cybersecurity programs and initiatives, and agencies' progress to enhance federal cybersecurity from the past year and into the future. Part of what is included in agencies' evaluations submitted to OMB include independent evaluations by the IG or independent external auditor for each agency which determines the effectiveness of the information security policies, procedures, and practices supporting their agency's information security programs.[333] The FISMA Annual Report to Congress can be found at www.whitehouse.gov.

For more information consult the Reporting Calendar.

[331] Congressional Research Service. The Current State of Federal Information Technology Acquisition Reform and Management. 2/03/2020. https://fas.org/sgp/crs/misc/R44843.pdf

[332] The White House. Federal Information Security Modernization Act of 2014. Annual Report to Congress. FY 2018. https://www.whitehouse.gov/wp-content/uploads/2019/08/FISMA-2018-Report-FINAL-to-post.pdf

[333] GAO-19-545. Agencies and OMB Need to Strengthen Policies and Practices. July 2019. https://www.gao.gov/assets/710/700588.pdf

8. Reporting Calendar

Federal agencies are required by OMB to participate in several reporting activities for the planning, programming, management, and execution of IT. The following Reporting Calendar outlines those reporting activities and the periods for which they take place during the year.

January

- CPIC Final Submission (after budget pass-back)
- Q1 CIO FISMA Reporting
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

February

- Quarterly Integrated Data Collection Submissions
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

March

- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

April

- Q2 CIO FISMA Reporting
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

May

- Annual Data Center Optimization Initiative Strategic Plan Update
- Quarterly Integrated Data Collection Submissions
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

June

- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

July

- Q3 CIO FISMA Reporting
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

August

- Quarterly Integrated Data Collection Submissions
- CPIC Test
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

September

- CPIC Submission
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

October

- Annual CIO, IG, and SAOP FISMA Reporting
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

November

- Quarterly Integrated Data Collection Submissions
- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

December

- Monthly Update to IT Dashboard project data
- Monthly Update to CIO Risk Evaluations

08
SECTION

ADDITIONAL RESOURCES

9. Additional Resources

9.1 CIO Council Resources

Report to the President on Federal IT Modernization

In May 2017, President Trump issued Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,[334] which commissioned the Federal IT Modernization Report to describe the legal, policy, and budgetary considerations around federal network architectures and provide recommendations to improve security, make Federal IT more agile and responsive, and make infrastructure more cost effective.

The Report to the President on Federal IT Modernization[335] was produced in December 2017 and outlines the White House's American Technology Council and the Office of Science and Technology Policy's vision and recommendations to modernize citizen-facing services. The report incorporates feedback from more than 100 companies and individuals, as well as extensive input from agencies and IT policy experts throughout the federal government.

The report chiefly recommended network modernization and consolidation, a shift toward shared services to enable future network architectures, and providing additional resources for federal network IT modernization. All recommendations made in the report were to be completed no more than 365 days after publication, and there are not current, ongoing requirements. The report heavily influenced the PMA, which established the White House's 2018 priorities.[336]

Application Rationalization Playbook

In collaboration with OMB and GSA, the Application Rationalization Playbook[337] was developed and finalized in June 2019 by the Federal CIOC in support of the Federal Cloud Computing Strategy,[338] also known as "Cloud Smart". It was designed for IT Portfolio Managers to consider their agency's approach to IT modernization. Additional guidance and policies germane to application rationalization include: the Federal IT Modernization Report[339] which was issued in December 2017; EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure which was issued in May 2017; and Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing which was issued by OMB as Memorandum M-16-12.

---

[334] Executive Order 13800. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 5/11/2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[335] CIO Council. Report to the President on Federal IT Modernization. December 2017. https://www.cio.gov/assets/resources/Report-to-the-President-on-IT-Modernization-Final.pdf

[336] The White House. President's Management Agenda. April 2018. https://www.performance.gov/PMA/Presidents_Management_Agenda.pdf

[337] CIO Council. The Application Rationalization Playbook. https://www.cio.gov/assets/files/Application-Rationalization-Playbook.pdf

[338] OMB. Federal Cloud Computing Strategy. https://cloud.cio.gov/strategy/

[339] CIO Council. Report to the President on Federal IT Modernization. December 2017. https://www.cio.gov/assets/resources/Report-to-the-President-on-IT-Modernization-Final.pdf

Application rationalization helps federal agencies mature IT portfolio management capabilities, empower leaders to make informed decisions, and improve the delivery of key mission and business services. It requires buy-in from stakeholders across the enterprise, including senior leaders, technology staff members, cybersecurity experts, business leads, financial practitioners, acquisition and procurement experts, and end user communities. Rationalization efforts rely on leadership support and continual engagement with stakeholders to deliver sustainable change. The playbook addresses challenges and opportunities for IT leaders, managers, and technical practitioners, and offers suggestions on how to overcome structural, logistical, and other significant barriers to success.

SOFIT

In January 2017, the CIOC released the State of Federal IT (SOFIT) report, which provided a comprehensive examination of the successes and challenges facing the Federal IT policy landscape. In addition, it provides recommendations on a variety of initiatives in order to improve Federal IT.

Future of the Federal IT Workforce Update

Drawing upon the workforce-related CAP Goals in the PMA, and building on the success of SOFIT, the CIOC undertook a similar examination of the Federal IT workforce and developed the Future of the Federal IT Workforce Update[340] report in May 2020 as an update to SOFIT.

The update is organized around five Primary Issue Areas (PIAs) which form the essential actions required to build an IT workforce for the future. Each PIA is dependent upon the others, and together they form the pillars of a modern, adaptable, and effective Federal IT workforce.

- **Recruit/Hire:** As an increasing number of Federal employees near retirement eligibility, it is essential that Government is able to quickly and efficiently recruit and hire the best IT talent in order to adapt to constantly evolving technologies.
- **Retain:** Government will need to offer its IT workforce opportunities for growth, access to cutting-edge technological tools, and rewards for high performance so they will want to continue to serve agency missions and the public good.
- **Reskill:** Agency-specific and Governmentwide training opportunities will keep IT workers flexible and adaptable in order to keep up with both the pace of innovation and changes that will continue to disrupt the way we conduct work.
- **Augment:** The Federal IT workforce must continue to be supported by agile, flexible groups from both within Government and the private sector, providing surge capacity, access to expertise in cutting-edge process improvements, and emerging or highly specialized technological capabilities.
- **Measure:** Without sufficient qualitative and quantitative data, it will be impossible to gauge successes. Opportunities to leverage data will be identified in order to chart the best path forward by providing a focus on measuring alongside each of the other PIAs.

[340] CIO Council. Future of the Federal IT Workforce Update. May 2020. https://www.cio.gov/assets/resources/Future_of_Federal_IT_Workforce_Update_Public_Version.pdf

The Drivers of the Future of the IT Workforce underpin each of the PIAs. The PIAs must be examined in the light of every driver and the roles these drivers play in shaping the workforce. The considerations for each driver of the future can be described as follows:

- **Innovation:** The increasing pace of technological change is constantly impacting the modern workplace. Recent years have seen changes ranging from the adoption of new programming languages and cloud-based applications to paradigm shifts in emerging technologies, such as robotic process automation and machine learning. Additional training and collaboration opportunities will enable the IT workforce to be flexible enough to adapt to these changes, enabling agencies to execute their missions.
- **Mobility:** Increased flexibility in all of the PIAs will allow the Federal Government to adapt to the workforce of the future. This includes providing vertical career mobility and rewarding high performers, as well as horizontal career mobility opportunities such as reskilling, detailing, and industry exchange programs.
- **Cybersecurity:** All IT work requires some degree of security knowledge and protections, from basic sharing of unclassified documents to defending the nation's most critical IT assets. As such, a skilled and qualified IT workforce is needed to manage an increasingly complex array of security policies and tools to mitigate evolving threats.
- **Collaboration:** As the world grows increasingly more interconnected, so must the Federal IT workforce. This includes coordinating across agencies and cross-functional teams. With the rise of regional offices and improved telework technologies, a more geographically dispersed workforce can now be productive over vast physical distances.
- **Agility:** The Federal Government needs to adapt and scale its use of technology more quickly than ever before. In addition to utilizing agile development methodology and continuous improvement, processes and procedures must also minimize downtime and be adaptable to changing circumstances and expectations in the workforce.

CISO Handbook

This handbook gives CISOs an overview of their roles and responsibilities in relation to Federal cybersecurity. It highlights laws, policies, tools, and initiatives that can be used to create or amend cybersecurity programs.[341]

This handbook aims to:

- Educate and inform new and existing CISOs about their role in successfully implementing Federal cybersecurity;
- Provide resources to help CISOs responsibly apply risk management principles to help Federal agencies meet mission objectives; and
- Make CISOs aware of laws, policies, tools, and initiatives that can assist them as they develop or improve cybersecurity programs for their organizations.

[341] CIO Council. Guidance for Chief Information Security Officers (CISO). https://www.cio.gov/resources/ciso-handbook/

9.2 NIST Resources

NIST Risk Management Framework (RMF)
The NIST RMF[342] provides a foundational process that integrates security and risk management activities into the system development life cycle and brings many of the NIST documents together into an overall approach to managing risk. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.[343]

CIOs must conduct program portfolio reviews as part of CPIC to ensure that all programs and the CIO are meeting the requirements of FITARA. This includes a CIO evaluation report to OMB for major IT investments that relate to mission delivery and mission support services investments and standard IT services investments that pertain to IT infrastructure, IT security, and IT management investments. However, CIO evaluations can also be provided for other investment types at the CIOs discretion.

NIST Publications
NIST publishes and creates archives of standards, guidelines, recommendations, and research relating to the security and privacy of information and information systems.

Some examples include:

- Federal Information Processing Standards (FIPS) – FIPS establish mandatory requirements for information processing.
- NIST Special Publications (SPs) – SPs provide guidance for developing agency-wide information security programs, including guidelines, technical specifications, recommendations, and reference materials. NIST SPs comprise multiple sub-series:
    - The NIST SP 800-series focuses on computer security, and
    - The NIST SP 1800-series provides cybersecurity practice guides.
- NIST Internal or Interagency Reports (NISTIRs) – NISTIRs are reports of research findings, including background information for FIPS and SPs.
- NIST Information Technology Laboratory Bulletins (ITL Bulletins) – ITL Bulletins are monthly overviews of NIST's security and privacy publications, programs, and projects.

NIST Cybersecurity Framework (CSF)
The NIST CSF is a tool originally developed for the private sector that agencies must implement to manage cybersecurity risk in accordance with Executive Order 13800. The CSF can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program.

An organization can use the CSF as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. It can help an organization determine which activities are most important to critical service delivery, prioritize expenditures and maximize the impact of investment. The CSF is designed to complement existing business and cybersecurity operations. It provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in

[342] NIST. Risk Management Framework (RMF) Overview. https://csrc.nist.gov/projects/risk-management/rmf-overview
[343] Ibid.

an organization's cybersecurity practices. It also provides a general set of processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The CSF consists of three parts: the CSF Core, the CSF Profile and the CSF Implementation Tiers. The CSF Core is a set of cybersecurity activities, outcomes and informative references that are common across organizations, providing detailed guidance for developing individual organizational profiles. CSF Profiles help the organization align its cybersecurity activities with its business requirements, risk tolerances and resources. The CSF Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

Figure 2, Notional Information and Decision Flows within an Organization,[344] describes a common flow of information and decisions at the executive, business/process, and implementation/operations levels within an organization.

OMB and DHS have organized the CIO FISMA metrics around the Cybersecurity Framework, leveraging it as a standard for managing and reducing cybersecurity risks and using the core functions to organize the information agencies must submit.

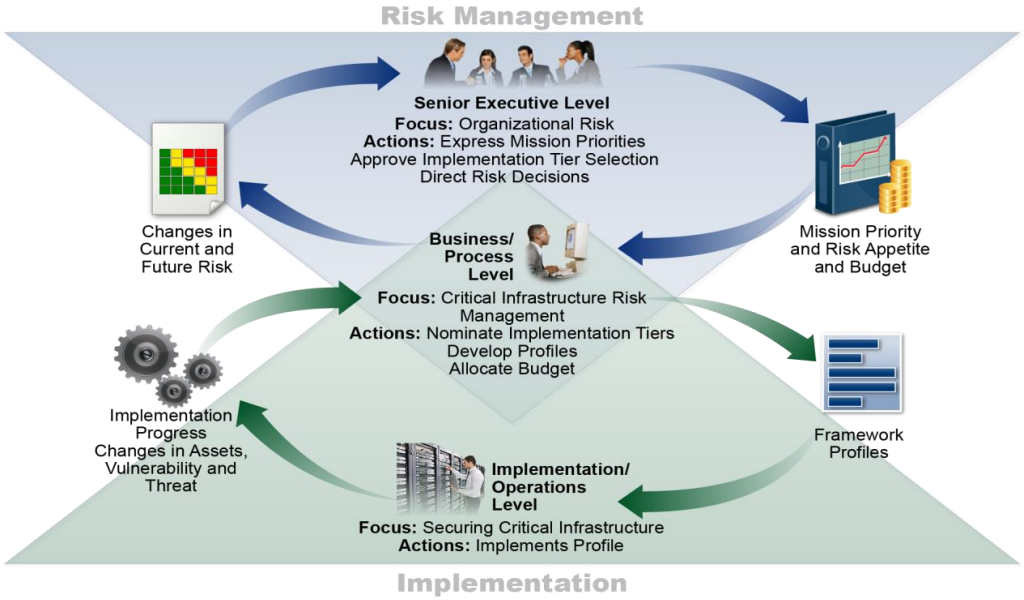

Figure 2: Notional Information and Decision Flows within an Organization

National Initiative for Cybersecurity Education (NICE) Framework

The NICE Cybersecurity Workforce Framework (NICE Framework)[345] is led by NIST at the DOC. The NICE Framework serves as a guide with a collection of common language, classifications, and vocabulary to describe cybersecurity activities and employees. It is meant for a variety of audiences including employers, current and prospective jobs holders, and academic advisors.

[344] NIST. Framework for Improving Critical Infrastructure Cybersecurity. Page. 12. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[345] US-CERT. NICE Cybersecurity Workforce Framework. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

The NICE Framework includes the following:

- Categories (7)
  - A high-level cluster of common cybersecurity functions
- Specialty Areas (33)
  - Specific areas of cybersecurity work
- Work Roles (52)
  - Detailed lists of cybersecurity work necessary for someone to be aware of to fulfill a job function
- Capability Indicators
  - Combines education, certification, training, experiential learning and continuous learning useful to help someone succeed in a role[346]

9.3 DHS Resources

National Initiative for Cybersecurity Careers and Studies (NICCS)
NICCS, an official website of CISA, is an online resource for cybersecurity training. The courses in the training catalog are cybersecurity focused and delivered by accredited universities, National Centers of Academic Excellence, federal agencies, and other training providers. Each course is mapped to the National Cybersecurity Workforce Framework, the foundation of the National Initiative for Cybersecurity Education (NICE) effort to standardize the cybersecurity field.[347]

Federal Virtual Training Environment (FedVTE)
The FedVTE provides free online cybersecurity training to federal, state, local, tribal, and territorial (SLTT) government employees, federal contractors, US military veterans and the public. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis.[348]

Training, as referred to in the Future of the Federal IT Workforce Update[349] report, is a fundamental component of reskilling opportunities within the Federal Government and helps further the goal of enhancing the national cybersecurity posture. By ensuring that all IT workers have cybersecurity training that is broad enough to at least cover the basics of good cyber hygiene, the potential decreases for breaches to occur through phishing attacks or the introduction of malware.

Register for FedVTE training at https://fedvte.usalearning.gov/.

FISMA Metrics
Each year, three sets of FISMA metrics are developed and used to evaluate the performance of agency cybersecurity and privacy programs.

---

[346] Ibid.
[347] US-CERT. Learn about NICCS. https://niccs.us-cert.gov/about-niccs/learn-about-niccs
[348] US-CERT. Federal Virtual Training Environment (FedVTE). https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte
[349] CIO Council. Future of the Federal IT Workforce Update. May 2020. https://www.cio.gov/assets/resources/Future_of_Federal_IT_Workforce_Update_Public_Version.pdf

1. FISMA CIO metrics are developed by OMB and DHS in close coordination with members of the CIO and CISO Communities and assess the degree to which agencies have implemented certain cybersecurity-related policies and capabilities. CFO Act agencies report this information on a quarterly basis, and non-CFO Act agencies report this information twice annually. These metrics ensure demonstrable progress from agencies' in implementing the Administration's priorities and best practices.
2. FISMA IG metrics are developed by the CIGIE, in collaboration with OMB and DHS, and are used to provide the independent assessment required under FISMA.
3. FISMA SAOP metrics are used to assess the maturity of agency privacy programs. Both the FISMA IG and FISMA SAOP metrics are collected on an annual basis and, along with the fourth quarter FISMA CIO metrics, are reported in the Annual FISMA Report.[350]

FISMA metrics from the current and previous years can be found at CISA.gov for FISMA documents.

9.4 GSA Resources

Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SINs)
GSA, in collaboration with DHS and OMB, developed the Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SINs) to make it easier for agencies to procure quality cybersecurity services.[351]The program is designed to provide government organizations with access to cybersecurity vendors and to meet the IT security requirements outlined in OMB M-19-03,[352] M-17-12,[353] and the CISO Handbook.[354] They are available through the Multiple Award Schedule (MAS) IT procurement process.

The scope of HACS SINs includes five categories of cybersecurity services for which vendors in the GSA eLibrary have passed a technical evaluation for the categories:

- High Value Asset Assessments
    - Risk and Vulnerability Assessments (RVA)
    - Security Architecture Review (SAR)
    - Systems Security Engineering (SSE)
- RVA
- Cyber Hunt
- Incident Response

[350] CIO Council. CISO Handbook. Page 25. https://www.cio.gov/assets/resources/CISO_Handbook.pdf
[351] GSA. IT Security: GSA's Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN). https://interact.gsa.gov/document/it-security-gsas-highly-adaptive-cybersecurity-services-hacs-special-item-number-sin
[352] OMB M-19-03. Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program. 12/10/2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf
[353] OMB M-17-12. Preparing for and Responding to a Breach of Personally Identifiable Information. 1/3/2017. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf
[354] CIO Council. Guidance for Chief Information Security Officers (CISO). https://www.cio.gov/resources/ciso-handbook/

- Penetration Testing[355]

To purchase HACS solutions through the MAS IT procurement process, see the link to the GSA website which includes a HACS Ordering Guide, the HACS SIN vendor listing on the GSA eLibrary, available experts to advise federal agencies on HACS procurement, as well as materials for state and local government ordering and sample Statement of Work (SOW) and Request for Quote (RFQ) Templates.

9.5 OPM Resources

Hiring Guidance
As outlined in the Future of the Federal IT Workforce Report, inefficiencies in the hiring process has contributed to the Federal government's struggle to bring in talent to the IT workforce in a timely and efficient manner. For example, average times to hire are between 110-170 days based on security clearance level, which is four times longer than in industry.[356] As noted by GAO, these struggles have led to challenges in recruiting and retaining CIOs and IT personnel.[357] In order to bring in skilled IT talent, agency CIOs have increasingly used Special Hiring Authorities, such as Schedule A, to meet specific hiring needs that have not been met by the regular hiring process.

Schedule A has been repeatedly granted by OPM for the hiring of digital services staff working on IT projects for the past several fiscal years but has been limited to Modernization, Smarter IT Delivery, and cloud migration projects. An additional hiring flexibility was released by OPM in October 2018 to meet critical technical and cybersecurity needs; this guidance provides direct hire authorities for a variety of STEM and cybersecurity positions.

OPM's most recent regulation was released in April 2019 as the Delegation of Direct-Hire Appointing Authority for IT Positions[358] which builds on the PMA and EO 13833 and provides two CIO direct hire authorities: one for a severe shortage of candidates, and one for a critical hiring need. Both of these authorities provide for an appointment lasting up to four years with an additional four-year appointment at the agency's discretion. This direct hire authority (DHA) expands agencies' ability to maximize DHA for meeting critical IT hiring challenges beyond the government-wide DHA for IT, which is limited to IT positions related to information security.

Federal Employee Viewpoint Survey (FEVS)
FEVS is administered annually by OPM and is a voluntary survey of all permanent federal employees. The survey was initially administered bi-annually as the Federal Human Capital Survey (FHCS) beginning in 2002 and has been administered in its current form since 2010. The survey measures employees' perceptions of whether, and to what extent, conditions characteristic of successful organizations are

[355] GSA. Highly Adaptive Cybersecurity Services (HACS). https://www.gsa.gov/technology/technology-products-services/it-security/highly-adaptive-cybersecurity-services-hacs
[356] CIO Council. Future of the Federal IT Workforce Update. May 2020. https://www.cio.gov/assets/resources/Future_of_Federal_IT_Workforce_Update_Public_Version.pdf
[357] GAO-19-723T. Talent Management Strategies to Help Agencies Better Compete in a Tight Labor Market. 9/25/2019. https://www.gao.gov/assets/710/701649.pdf
[358] OPM. Delegation of Direct-Hire Appointing Authority for IT Positions. 4/5/2019. https://www.chcoc.gov/content/delegation-direct-hire-appointing-authority-it-positions

present in their agencies.[359] There are typically around 100 questions and the survey takes about 25 minutes to answer. It is typically released around mid-year and respondents have around six weeks to complete the survey electronically, the typical response rate is above 40% among the more than 1.4 million permanent federal employees. Once the survey period is completed, OPM weighs and analyzes the data and ensures the final data set reflects the agency composition and demographic makeup of the Federal workforce within plus or minus 1 percentage point. The final product is published as an OPM report and provides agency leaders insight into areas where improvements have been made, as well as where improvements are needed.

[359] OPM. Federal Employee Viewpoint Survey. https://www.opm.gov/fevs/about/