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.

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]

Core Activities:

[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

- 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