Congressional Research Service
Informing the legislative debate since 1914

Chief Information Officers (CIOs): Agency Roles and Responsibilities

August 1, 2024

Congressional Research Service
https://crsreports.congress.gov
R48147

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48147

August 1, 2024

Meghan M. Stuessy
Analyst in Government Organization and Management

Dominick A. Fiorentino
Analyst in Government Organization and Management

Chief Information Officers (CIOs): Agency Roles and Responsibilities

In the course of fulfilling their missions, federal agencies constantly consume, create, use, and store information from a variety of sources, media formats, and technology platforms. In response to concerns that agencies were not adequately or efficiently managing their information, Congress required each agency to designate a senior official to oversee this function through enactment of the Paperwork Reduction Act of 1980. This position was later renamed the chief information officer (CIO).

Congress passed the Clinger-Cohen Act of 1996 to improve agency investment in and management of information technology (IT) as the use of computing and information technologies became more widespread. This law required the agency CIO to be responsible for some aspects of acquisition and management of IT. Over time, executive branch policy initiatives and legislation have continued to modify and reprioritize the roles and responsibilities of agency CIOs. For example, the Federal Information Technology Acquisition Reform Act (FITARA) in 2014 built upon the Clinger-Cohen Act to establish a framework for tracking, assessing, and managing federal IT investments.

In general, statutorily established agency CIO positions operate within complex ecosystems of agency officials and organizations. These institutional relationships usually involve collaboration and division of labor across agency functions and organizational levels.

In many ways, the development and redevelopment of the CIO position is indicative of Congress's evolving understanding of how information should be managed within agencies. While the CIO is often perceived as an IT position, CIOs are responsible for information management more broadly, of which IT is just one of several means of managing information. CIO responsibilities related to the management of federal information are located in portions of Title 44 of the *U.S. Code*, and responsibilities related to IT management are located in portions of Title 40 of the *U.S. Code*. Both sets of responsibilities are ultimately vested in the agency head, and agency heads further delegate these responsibilities to agency CIOs.

The Paperwork Reduction Act of 1995 generally amended the federal agency information management responsibilities in Title 44 and established the seven categories of responsibilities that endure today: (1) information resources management, (2) information collection and control of paperwork, (3) information dissemination, (4) statistical policy and coordination, (5) records management, (6) privacy and security, and (7) federal IT. Expanding upon the CIO's federal IT management roles, Title 40 also makes the CIO responsible for (1) IT performance management, (2) IT budgeting, and (3) IT capital planning and investment control.

In addition to the roles and responsibilities described in statute, Office of Management and Budget (OMB) *Circular No. A-130: Managing Information as a Strategic Resource*, "establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services." Government-wide, the OMB director is authorized by statute to develop, coordinate, and oversee the implementation of federal information management policies. Multiple offices within OMB may participate in the development of such policies, which may complicate the resulting guidance.

Contents

Figures

Tables

Appendixes

Contacts

In the course of fulfilling their missions, federal agencies constantly consume, create, use, and store information from a variety of sources, media formats, and technology platforms. Through the Paperwork Reduction Act of 1980, Congress required each agency to designate a "senior official," later renamed a chief information officer (CIO), in response to concerns that agencies were not adequately or efficiently managing their information.[1] These agency leaders are to manage government information throughout its life cycle and ensure that each agency carries out its information management activities in an efficient, effective, and economical manner.[2] While agencies may designate additional CIO positions within their subcomponents—often known as a bureaus, administrations, or services—this report focuses on the statutorily designated CIOs at the agency or departmental level.

As the use of computing and information technologies became more widespread across federal agencies and to improve agency investment in and management of information technology (IT), Congress passed the Clinger-Cohen Act of 1996. This law required the agency CIO to be responsible for some aspects of acquisition and management of IT.[3] Over time, executive branch policy initiatives and legislation have continued to modify and reprioritize the roles and responsibilities of agency CIOs. The CIO's interrelated responsibilities with regard to information resources management (IRM) and IT are defined in two intersecting titles of the *U.S. Code* that require CIOs to interact and share responsibilities with many other agency officials in managing agency information.

Information management is crucial to supporting agency operations, informing Congress and the public on agency actions, and facilitiating interactions between the public and the federal government. The Office of Management and Budget (OMB) explains, "Federal information is both a strategic asset and a valuable national resource. It enables the Government to carry out its mission and programs effectively. It provides the public with knowledge of the Government, society, economy, and environment—past, present, and future."[4] Information management is supported by the effective and efficient use of IT. Federal information management and IT management have been an area of continuing interest to Congress.

This report provides an introduction to key concepts and definitions with respect to government information and describes the agency CIO's roles and responsibilities with regard to IRM and IT. The report also describes the CIO's institutional relationships within an agency and intersection with other agency C-suite officials. The report includes a discussion of OMB's interaction with and management of agency CIOs and concludes with issues for Congress.

Defining and Managing Government Information

Government information policy has grappled with the concept of access to information and, with it, organizing and managing information so that it can be accessed.[5] Members of the public and other agencies may request information for research, oversight, and programmatic purposes. Two key concepts inform the effort to define and manage government information: (1) the information

[1] U.S. Congress, House Committee on Government Operations, Paperwork Reduction Act of 1980, To accompany H.R. 6410, 96th Cong., 2nd sess., March 19, 1980, H. Rept. 96-835, p. 7-8.

[2] P.L. 96-511, 94 Stat. 2819.

[3] P.L. 104-106, §5125, 110 Stat. 684.

[4] OMB, *Circular No. A-130: Managing Information as a Strategic Resource*, July 2016, p. 3, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf.

[5] For more about federal information access, see CRS Report R47058, *Access to Government Information: An Overview*, by Meghan M. Stuessy.

life cycle, where agency information changes over time in terms of audience and use case, and (2) digital modernization, where agencies upgrade and integrate new technologies into their business and service infrastructure.

According to the National Archives and Records Administration (NARA), OMB, and others, the information life cycle concept describes the ways in which information moves and is a method of understanding how laws and policies affect the use of information in the government. Generally, the information life cycle can be thought of as comprising three stages:

1. Creation or receipt,
2. Maintenance and use, and
3. Disposition or destruction.[6]

The stage in which the requested information currently resides impacts whether, and in what format, the requested information may be provided. Further, the life cycle stage of the information can provide indications for how an agency may share the information and what office or officials within an agency are responsible for stewarding the information. For example, when agencies receive information via collection, that process may implicate CIOs and program officials involved in designing the information collection or survey. As another example, if agencies maintain existing records in digital formats, the CIOs may work with agency records officers and archivists to alter the formatting of the information to ensure the information's appropriate functionality and preservation. In these ways, the information life cycle concept can serve as a means of understanding the many activities involved in information management.

In addition, the ways in which government conducts itself has changed from analog and physical, paper-based formats to electronic, born-digital formats. In general, information systems can be thought of as comprising three layers:

1. The storage layer (such as the physical filing system and location of the information);
2. The media layer (such as a paper document, CD-ROM, or cassette and formatting choices); and
3. the message layer (such as the language and content of the information).[7]

The ways in which government conducts itself has changed from analog and physical, paper-based formats to electronic, digital-native formats. Digital information systems may face similar considerations, such as how and where electronic information is stored, what software and coding languages are used, and whether access to the message requires special understanding or knowledge.[8] Because the method of message delivery is defined by the media and storage of the

[6] NARA, "Guide to the Inventory, Scheduling, and Disposition of Federal Records: Records Disposition Overview," https://www.archives.gov/records-mgmt/scheduling/rdo. *OMB Circular A-130* provides additional terminology on the information life cycle. However, this definition is compatible with the simplified NARA definition used in the text of this report. *Circular A-130* reads, "'Information life cycle' means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion" (OMB, *Circular No. A-130*, p. 29).

[7] For more information, see "Government Information Management in the Future" within CRS Report R45014, *Government Printing, Publications, and Digital Information Management: Issues and Challenges*, by R. Eric Petersen. See also Jean-François Blanchette, "A Material History of Bits," *Journal of the American Society for Information Science and Technology*, vol. 62, no. 6 (June 2011), pp. 1042-1057.

[8] See, for example, the conceptual model discussing the layers of digital services in OMB, "Digital Government: Building a 21st Century Platform to Better Serve the American People," May 23, 2012, https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html.

information, expertise in managing digital information is enmeshed with management of information overall.

Establishment of the CIO

The Paperwork Reduction Act of 1980 required each agency head to designate a "senior official" to report directly to the agency head and carry out responsibilities related to the coordination of federal information policy.[9] The corresponding House Committee on Government Operations report stated, "This realignment should provide for greater coordination among the agency's information activities as well as greater visibility within the agency."[10] The Senate Committee on Governmental Affairs emphasized that these senior agency officials should understand "the value of working closely with their own agency information management personnel who are familiar with abstracting, indexing, and disseminating information."[11]

Under the Clinger-Cohen Act of 1996, the terminology of "senior official" was redesignated as the "Chief Information Officer."[12]

Information Resources Management (IRM)

The term *information resources management* first appeared in statute in the Paperwork Reduction Reauthorization Act of 1986.[13] Congress incorporated the information life cycle concept into the initial definition of the term as the "planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies."[14] Subsequently in 1995, the definition was split, where *information resources* was defined as "information and related resources, such as personnel, equipment, funds, and information technology," and *information resources management* was instead the process of managing such resources "to accomplish agency missions and to improve agency performance."[15]

The splitting of these definitions may in part reflect a growing sense in Congress that IRM should not be treated as a generic pursuit of efficiency but as integral to supporting agency missions and improving programmatic outcomes.[16] In a report on the Paperwork Reduction Act of 1995, the Senate Governmental Affairs Committee found:

---

[9] P.L. 96-511, 94 Stat. 2819.

[10] U.S. Congress, House Committee on Government Operations, *Paperwork Reduction Act of 1980*, To accompany H.R. 6410, 96th Cong., 2nd sess., March 19, 1980, H. Rept. 96-835, p. 7.

[11] The Senate Committee on Governmental Affairs is the predecessor to the current Senate Committee on Homeland Security and Governmental Affairs. U.S. Congress, Senate Governmental Affairs Committee, *Paperwork Reduction Act of 1980*, To Accompany S. 1411 To Improve the Economy and Efficiency of the Government and the Private Sector by Improving Federal Information Policymaking, and for Other Purposes, 96th Cong., 2nd sess., August 8, 1980, S. Rept. 96-930, p. 33.

[12] P.L. 104-106, §5125, 110 Stat. 684. This provision was originally enacted as part of the Information Technology Management Reform Act of 1996, in Division E of P.L. 104-106 (110 Stat. 679), the National Defense Authorization Act for Fiscal Year 1996 (110 Stat. 186). Subsequently, Section 808 of P.L. 104-208 (110 Stat. 3009-393) retitled Divisions D (the Federal Acquisition Reform Act of 1996, 110 Stat. 642) and E as the Clinger-Cohen Act of 1996.

[13] P.L. 99-591.

[14] P.L. 99-591, 100 Stat. 3341-336.

[15] P.L. 104-13, 109 Stat. 166.

[16] U.S. Congress, Senate Governmental Affairs Committee, *Paperwork Reduction Act of 1995*, 104th Cong., 1st sess., February 14, 1995, S.Rept. 104-8 (Washington: GPO, 1995), p. 20.

> Information, as a resource, is not simply a matter of questions answered or systems acquired. Information must be reliable, accurate, complete, accessible, and timely if it is to be used by agency managers to make decisions and take actions in fulfilling agency missions. Accordingly, investments in information resources must be managed as a part of a coordinated, performance-oriented approach to "recognize and address the interconnectivity among the stages of the information life cycle."[17]

This discussion of acquiring information systems also pointed to the emerging policy area of IT management.

Information Technology (IT) Management

The Clinger-Cohen Act emerged out of growing concern about the federal government's ability to develop and maintain IT infrastructure and personnel. In 1994, a subcommittee of the Senate Committee on Governmental Affairs detailed what it described as systemic problems in federal IT procurement and ineffective oversight of IT programs.[18] Reflecting Congress's focus on IT improvements, the renamed CIO position would have a dual focus: The information policy roles previously assigned to agency "senior officials" would also include new IT management roles and responsibilities. In a conference report to accompany Clinger-Cohen, Congress stated that agency CIOs would be "responsible for providing information and advice regarding information technology and information resources management to the head of the agency, and for ensuring that the management and acquisition of agency information technology is implemented consistent with the provisions of this law."[19] Clinger-Cohen also extensively modified federal IT acquisition policy and procurement management. In doing so, it assigned certain IT management roles and responsibilities to agency CIOs, including developing and maintaining IT systems and evaluating, assessing, and reporting on IT improvements.[20]

In 2014, the Federal Information Technology Acquisition Reform Act (FITARA) built upon the Clinger-Cohen Act to establish a framework for tracking, assessing, and managing federal IT investments.[21] FITARA also introduced a split in the IT management responsibilities assigned to CIOs based on agency size. While the CIO roles and responsibilities under Clinger-Cohen apply to all executive agencies, certain provisions of FITARA apply only to agencies identified in the Chief Financial Officers (CFO) Act of 1990, as well as their subordinate components.[22] CIOs at these larger agencies are required to advise agency heads on capital planning and investment control (CPIC) processes to acquire, use, maintain, and dispose of IT.[23]

---

[17] Ibid., p. 17.

[18] As the ranking minority member of the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Senator William Cohen directed a staff study of major government IT integration and modernization efforts in progress. See U.S. Sen. William S. Cohen, *Computer Chaos: Billions Wasted Buying Federal Computer Systems, Investigative Report*, report from minority staff of the Senate Subcommittee on Oversight of Government Management (Washington: October 12, 1994).

[19] U.S. Congress, Conference Committee, National Defense Authorization Act for Fiscal Year 1996, conference report to accompany S. 1124, 104th Cong., 2nd sess., H.Rept. 104-450, January 22, 1996, p. 977.

[20] See CRS Report RL30661, *Government Information Technology Management: Past and Future Issues (The Clinger-Cohen Act)*, by Jeffrey W. Seifert (available to congressional clients upon request).

[21] P.L. 113-291, Title VIII, Subtitle D, of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015; 128 Stat. 3438.

[22] The CFO Act of 1990 (31 U.S.C. §901(b), P.L. 101-576, 104 Stat. 2838) enacted into law a financial management and reporting framework in the executive branch. See CRS Report R46877, *Federal Information Technology (IT) Budgeting Process in the Executive Branch: An Overview*, by Dominick A. Fiorentino.

[23] 40 U.S.C. §11302. OMB *Memorandum M-15-14*, "Management and Oversight of Federal Information Technology," (continued...)

Differing Definitions of *Agency*

Executive agencies: Using the Title 44, of the *U.S. Code* definition, CIO roles and responsibilities enacted under Clinger-Cohen apply to a larger set of agencies, including "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency."[24] This definition excludes the Government Accountability Office; the Federal Election Commission; the governments of the District of Columbia and of the territories and possessions of the United States and their various subdivisions; and government-owned, contractor-operated facilities, including laboratories engaged in national defense research and production activities.

CFO Act agencies: Certain CIO roles responsibilities enacted under FITARA apply only to larger agencies known as "CFO Act agencies," of which there are currently 24. The CFO Act of 1990 enacted into law a financial management and reporting framework in the executive branch. The legislation also created the role of CFO and deputy CFO at large executive agencies who have certain statutory responsibilities related to financial management and reporting.[25]

Roles and Responsibilities

The roles and responsibilities of the CIO are generally described in two intersecting titles of the *U.S. Code*: Titles 40 and 44. In addition, OMB issued *Circular No. A-130*: *Managing Information as a Strategic Resource*, further describing objectives and duties for agency heads, CIOs, and other agency officials with respect to information management.

Reflecting the development of key government information management concepts, CIO responsibilities related to the coordination of federal information policy are located in portions of Title 44 of the *U.S. Code*, and responsibilities related to IT management are located in portions of Title 40 of the *U.S. Code*. Both sets of responsibilities are ultimately vested in the agency head, but statute requires that the agency head delegate certain of these responsibilities to agency CIOs.[26] In the case of Title 40, this delegation to the CIO is accomplished through a reference to Title 44, which lists the use and investment of IT in a manner consistent with applicable management policies as one of an agency's information policy obligations.[27]

CIO duties are described differently in Title 44 and Title 40. The CIO is to ensure agency compliance with portions of Title 44, whereas the CIO is to provide advice and other assistance to the agency head and other senior agency management with regard to Title 40.[28] Because IRM permeates agency processes, CIOs by statute and practice interact with many internal and external stakeholders, such as other agencies, agency components, and program officials.[29] These

provides "implementation guidance for the Federal Information Technology Acquisition Reform Act (FITARA) and related information technology (IT) management practices." See OMB, *Memorandum No. M-15-14: Management and Oversight of Federal Information Technology*, June 10, 2015, p. 1, https://www.whitehouse.gov/omb/information-for-agencies/memoranda/.

[24] 44 U.S.C. §3502.

[25] 31 U.S.C. §901(b).

[26] See 44 U.S.C. §3506(a) and 40 U.S.C. §11311 for the vesting of responsibilities in the agency head. See 44 U.S.C. §3506(a)(2)(A) and 40 U.S.C. §11315(b) for the further delegation of these responsibilities to agency CIOs.

[27] 40 U.S.C. §11315(b) and 44 U.S.C. §3506(h).

[28] 44 U.S.C. §3506(a)(3) and 40 U.S.C. §11315(b)(1).

[29] 44 U.S.C. §3502(7). Under Section 3506(a)(4), agency program officials are "responsible and accountable for information resources assigned to and supporting the programs under such official" and are expected to "define program information needs and develop strategies, systems, and capabilities to meet those needs" in consultation with the CIO and agency chief financial officer (or comparable official).

differences may complicate agency reporting structures and hierarchies, and this is further explored in "CIO Institutional Relationships" below.

Statutory Definitions of Key Terms

U.S. Code Titles 40 and 44

Information resources: information and related resources, such as personnel, equipment, funds, and IT.

Information resources management: the process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public.

Information system: discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information technology: any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

Coordination of Federal Information Policy: 44 *U.S. Code* Chapter 35

For purposes of federal information policy in Title 44, Chapter 35, of the *U.S. Code*, the head of each agency is to designate a CIO who reports directly to the agency head and carries out agency responsibilities.[30] The Paperwork Reduction Act of 1995 generally amended federal agency information management responsibilities and established the seven categories of responsibilities that endure today:[31]

1. IRM,
2. information collection and control of paperwork,
3. information dissemination,
4. statistical policy and coordination,
5. records management,
6. privacy and security,[32] and
7. federal IT.[33]

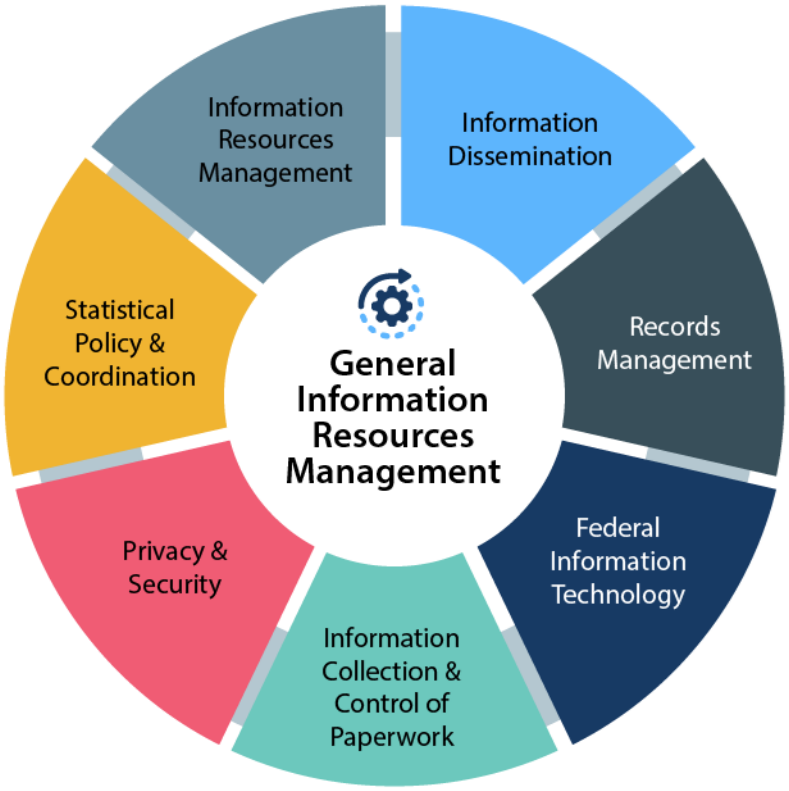
[30] 44 U.S.C. §3506(a)(2).

[31] P.L. 104-13, 109 Stat. 171-176.

[32] Note that Title 44, Section 3554(a)(3)(A), of the *U.S. Code* requires the agency CIO to further delegate responsibilities related to federal information security to a senior agency information security officer.

[33] 44 U.S.C. §3506. Note that Title 44, Section 3520, of the *U.S. Code* requires that a chief data officer carry out the requirements of the agency for IRM, information collection and control of paperwork, information dissemination, and records management.

Figure 1. Components of General Information Resources Management



Source: CRS analysis of 44 U.S.C. §3506.

The seven categories are components of the overall concept of general IRM, although the relative prominence of a single category may vary over time (see **Figure 1** above). A full enumeration of CIO responsibilities under Title 44, Section 3506, of the *U.S. Code* is located in the **Appendix** to this report.

IRM

The statute stipulates that the CIO's IRM activities include reducing information collection burdens on the public; increasing program efficiency and effectiveness; and improving the integrity, quality, and utility of information to all users within and outside the agency while also considering information protections for privacy and security.[34] In addition, the agency, acting through the CIO, is to develop and maintain a strategic IRM plan describing how IRM activities help accomplish agency missions.[35] Similarly, the CIO is to report agency policies and procedures for compliance with the Open, Public, Electronic, and Necessary (OPEN) Government Data Act and federal data catalogue, which has come to be known as data.gov.[36]

Finally, CIOs are required to ensure that IRM operations and decisions are "integrated with organizational planning, budget, financial management, human resources management, and

[34] 44 U.S.C. §3506(b)(1).

[35] 44 U.S.C. §3506(b)(2)(A).

[36] 44 U.S.C. §3506(b)(2)(B). For more information on the OPEN Government Data Act, see CRS In Focus IF12299, *The OPEN Government Data Act: A Primer*, by Meghan M. Stuessy.

program decisions" and consult with the OMB director and the Office of Personnel Management (OPM) director on formal training programs for agency program and management officials regarding IRM.[37]

Because the definition of *information resources* includes agency personnel, executive agency CIOs are responsible for assessing IRM workforce needs, of which the IT workforce comprises a subset, including strategies for hiring and training. These duties are restated in Title 40 of the *U.S. Code*, where CIOs must also annually assess the knowledge and skill requirements for the IRM workforce as well as the extent to which agency personnel met those knowledge and skill requirements.[38]

Information Collection and Control of Paperwork

Congress enacted the Paperwork Reduction Act of 1980 and reauthorized it in 1995 in part to address a concern that the federal government was requiring businesses, individuals, and other entities to spend too much time filling out paperwork at the behest of federal agencies.[39] The statute assigns certain responsibilities regarding collection of information and control of paperwork to the CIO.[40] This includes that the agency establish a process within the CIO's office to fairly evaluate and review information collections prior to submission to the OMB director for review in accordance with Section 3507 of Title 44 of the *U.S. Code* relating to public information collection activities,[41] providing public notice in the *Federal Register* and consulting with the public and affected agencies with regard to proposed information collections,[42] and certifying that information collections are not unnecessarily duplicative of other efforts, among other criteria.[43]

Information Dissemination

The CIO is to ensure that the public has timely and equitable access to public agency information, regularly solicit and consider public input on agency information dissemination, engage the public in using public data assets of the agency, and encourage collaboration, among other responsibilities.[44] Generally, public data assets are considered in law as a collection of data elements or datasets that has been publicly released or may be released under the Freedom of Information Act (FOIA).[45] The CIO's responsibilities here broadly relate to consulting with the

[37] 44 U.S.C. §3506(b)(3) and 44 U.S.C. §3506(b)(5).

[38] 40 U.S.C. §11315(c).

[39] For more information on the information collection and federal paperwork burden aspects of the Paperwork Reduction Act, see CRS In Focus IF11837, *The Paperwork Reduction Act and Federal Collections of Information: A Brief Overview*, by Maeve P. Carey and Natalie R. Ortiz.

[40] 44 U.S.C. §3506(c).

[41] 44 U.S.C. §3506(c)(1).

[42] 44 U.S.C. §3506(c)(2).

[43] 44 U.S.C. §3506(c)(3).

[44] 44 U.S.C. §3506(d).

[45] 44 U.S.C. §3502(22). For more information on the OPEN Government Data Act, which established these definitions, see CRS In Focus IF12299, *The OPEN Government Data Act: A Primer*, by Meghan M. Stuessy. For more information on FOIA, see CRS Report R46238, *The Freedom of Information Act (FOIA): A Legal Overview*, by Benjamin M. Barczewski.

public on agency information use, improving access to agency information, and publishing certain agency information in machine-readable formats.[46]

Statistical Policy and Coordination

CIOs are required to ensure the relevance, accuracy, timeliness, integrity, and objectivity of information collected or created for statistical purposes.[47] To these ends, CIOs must inform respondents fully and accurately about their agencies' statistical surveys and studies and protect respondents' privacy.[48] With regard to conducting statistical surveys, the CIO must ensure that the agency observes federal standards and practices for data collection, analysis, and dissemination. Under the related Information Quality Act, OMB issues guidance regarding how agencies are to ensure and maximize the quality, objectivity, utility, and integrity of information, including statistical information. OMB issued revised guidance in 2019 in OMB *Memorandum M-19-15*.[49]

Records Management

CIOs are to implement and enforce records management policies and procedures related to archiving electronic information, particularly in the planning, design, and operation of agency information systems.[50] Since the Presidential and Federal Records Act Amendments of 2014, materials to be assessed for records preservation include "all recorded information, regardless of form or characteristics, made or received by a Federal agency."[51]

Privacy and Security

CIOs are required to implement and enforce applicable policies, procedures, standards, and guidelines with respect to privacy, confidentiality, security, disclosure, and sharing of information collected or maintained by or for their agencies.[52] Additionally, CIOs assume responsibility and accountability for agency compliance and management of FOIA, the Privacy Act of 1974, and the Federal Information Security Management Act (FISMA).[53] Since 2014, Congress has further required an agency's FISMA responsibilities to be delegated to a senior agency information security officer designated by the CIO.[54]

---

[46] Title 44, Section 3502(18), of the *U.S. Code* defines *machine-readable data* as "data in a format that can be easily processed by a computer without human intervention while ensuring no semantic meaning is lost."

[47] 44 U.S.C. §3506(e).

[48] For more information on the federal statistical system, see CRS Insight IN12197, *The Federal Statistical System: A Primer*, by Taylor R. Knoedl.

[49] See 44 U.S.C. §3516 note, P.L. 106-554, 114 Stat. 2763A-153, and OMB, M-19-15, "Improving Implementation of the Information Quality Act," April 24, 2019, https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-15.pdf. The reprinted 2002 Information Quality Act guidance may be located at OMB, "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies; Republication," 67 *Federal Register* 8452-8460, February 22, 2002.

[50] 44 U.S.C. §3506(f).

[51] 44 U.S.C. §3301(a), P.L. 113-187, 128 Stat. 2009. For more information on federal records, see CRS In Focus IF11119, *Federal Records: Types and Treatments*, by Meghan M. Stuessy. For more information on presidential records, see CRS Report R46129, *The Presidential Records Act: An Overview*, by Meghan M. Stuessy.

[52] 44 U.S.C. §3506(g).

[53] For more information on the Privacy Act, see CRS Report R47863, *The Privacy Act of 1974: Overview and Issues for Congress*, by Meghan M. Stuessy. For more information about FISMA, see CRS Report R46926, *Federal Cybersecurity: Background and Issues for Congress*, by Chris Jaikaran.

[54] P.L. 113-283, 128 Stat. 3078. See also 44 U.S.C. §3554(a)(3)(A).

Federal IT

Acting on behalf of their agencies, CIOs are to implement and enforce government-wide and agency IT management policies; assume responsibility and accountability for IT investments; and propose legislative, regulation, and agency procedure changes to improve IT practices.[55] In addition, CIOs assume responsibility for "maximizing the value and assessing and managing the risks of major information systems initiatives."[56] Further IT duties assigned to the CIO have been expanded upon in Title 40 of the *U.S. Code*.

IT Management: Title 40 *U.S. Code* Subtitle III

Statutory provisions that are associated with the Clinger-Cohen Act have been amended and codified into Title 40, Subtitle III, of the *U.S. Code* (40 U.S.C. §§11101-11704) and relate to multiple aspects of IT management and acquisition. FITARA further amended and supplemented provisions that were originally associated with Clinger-Cohen. FITARA's provisions relate more specifically to CIO authorities and, in addition, planning, risk management, and oversight of IT acquisition and investment management. The roles and responsibilities accorded to the CIO under this title may be categorized as follows:

- IT performance management,
- IT budgeting, and
- IT CPIC.

A full enumeration of CIO responsibilities under Title 40, Subtitle III, of the *U.S. Code* is located in **Table A-2** within the **Appendix** to this report.

IT Performance Management

Each executive agency CIO has responsibilities over IT performance management that include (1) establishing goals for improving agency operations through IT, (2) preparing an annual report on the progress in achieving the goals, (3) ensuring that performance measures are suited to the agency's IT, (4) benchmarking agency performance against other private and public sector organizations, and (5) revising agency processes before making IT investments.[57]

IT Budgeting

CIOs at certain agencies have explicit planning, programming, budgeting, and execution authorities. CFO Act agency CIOs, aside from the Department of Defense (DOD), must review and approve the agency IT budget requests before the agencies submit their requests for OMB review.[58] The DOD CIO must review and provide recommendations to the Secretary of Defense on the IT budget request.[59]

[55] 44 U.S.C. §3506(h).

[56] 44 U.S.C. §3506(h)(5) and 40 U.S.C. § 11312.

[57] 40 U.S.C. §11313.

[58] 40 U.S.C. §11319(b)(1)(B)(i).

[59] 40 U.S.C. §11319(b)(1)(B)(i).

IT Capital Planning and Investment Control (CPIC)

CFO Act agencies are required to use a CPIC process to acquire, use, maintain, and dispose of IT.[60] CPIC processes include all stages of the IT asset life cycle, including planning, budgeting, procurement, management, and assessment.[61] CIOs at these agencies are required to consult the OMB director on improving the management of agency IT through portfolio review.[62] As a part of the portfolio review process, CIOs must categorize IT investments according to risk and review those investments categorized as high risk.[63] OMB guidance instructs agency CIOs to give IT investments a risk rating of 1 through 5 (highest to lowest risk) based on six evaluation criteria: (1) risk management, (2) requirements management, (3) contractor overight, (4) historical performance, (5) human capital, and (6) other.[64] Furthermore, a CIO is required to monitor the performance of IT programs and advise the agency head on whether to continue, modify, or cancel a program.[65]

OMB *Circular No. A-130*

In addition to the CIO's statutory requirements, OMB requires agencies to comply with its guidance on IRM activities.[66] First issued in 1985 in response to the Paperwork Reduction Act of 1980 and last revised in 2016, OMB *Circular No. A-130: Managing Information as a Strategic Resource*, "establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services."[67] *Circular No. A-130*'s requirements apply to management activities "concerning all information resources in any medium," including paper and electronic information.[68] The circular also provides an overview of other agency officials and government-wide actors that interact within the government information policy space.[69]

Reflecting statute, OMB notes that agency heads are ultimately responsible for implementing the circular's requirements.[70] However, several information management and IT responsibilities are either shared with or delegated to the CIO. Other roles and responsibilities require the CIO to collaborate with other agency C-suite officials such as the CFO or the chief acquisition officer. Roles and responsibilities described within *Circular No. A-130* that involve agency CIOs include IT planning, budgeting, and acquisition; IT investments; information resources governance; information resources workforce planning; and privacy and information security.

---

[60] 40 U.S.C. §11302.

[61] CIO Council, "Policies and Priorities: Capital Planning and Investment Control (CPIC)," https://www.cio.gov/policies-and-priorities/cpic/.

[62] 40 U.S.C. §11319(d).

[63] 40 U.S.C. §11302(c).

[64] OMB, IT Dashboard, https://www.itdashboard.gov/faq.

[65] 40 U.S.C. §11315(c)(2).

[66] OMB, *Circular No. A-130*, p. 3. OMB defines *executive branch agency* in this circular as "any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency."

[67] OMB, *Circular No. A-130*, p. 2. OMB describes its authority to issue this circular as deriving from various statutes, several of which have been discussed in this report, including the Clinger-Cohen Act, the E-Government Act of 2002, the Paperwork Reduction Act (as amended), the Privacy Act of 1974, and FITARA. *Circular No. A-130* was originally issued on December 12, 1985, and this initial version is located at 50 *Federal Register* 247, December 24, 1985.

[68] OMB, *Circular No. A-130*, p. 3.

[69] OMB, *Circular No. A-130*, pp. 20-25.

[70] OMB, *Circular No. A-130*, p. 2.

CIO Institutional Relationships[71]

In general, statutorily established agency CIO positions operate within complex ecosystems of agency officials and organizations. These institutional relationships usually involve a need for collaboration and division of labor across agency functions and organizational levels, as well as potential tensions regarding who should exercise control or influence over decisions and priorities. In practice, the environments under which CIOs operate vary across agencies that have heterogeneous missions and contexts and specific individuals in key roles.[72]

Viewing the CIO position in a broader institutional context may help illuminate several kinds of issues, including, for example, how an agency is to effectively manage its information resources when pursuing its mission(s); how the CIO position may be designed; and where there may be opportunities, risks, and trade-offs in how Congress could structure the CIO's role.

CIOs and Information Ownership

Both in practice and by statute, IRM is embedded into virtually all aspects of how an agency operates. This includes activities within and among an agency's constituent organizations and programs, with other federal entities, and with nonfederal clients, partners, and stakeholders. Because of the pervasiveness of different aspects of IRM, organizations typically rely on extensive collaboration and some division of labor.

Within an agency, certain organizations and components can be considered part of *mission delivery*, where operating units or program offices run activities and programs associated with the agency's core mission, or *mission support*, where offices and functions provide specialized technical expertise in service to the agency head and the agency's major mission delivery organizations.[73]

For their part, statutorily established CIOs and the functions or offices they lead may be viewed as providing mission support for multiple aspects of IRM.[74] At the same time, many activities related to IRM are performed by programs and organizations that deliver aspects of an agency's core mission(s), complicating questions surrounding accountability for information stewardship. In practice, these mission delivery organizations often manage and control their own information (e.g., information collections, data assets, files, archives). The execution of IRM responsibilities may necessitate collaboration among many officials and organizations and may lead to tensions

[71] Clinton T. Brass, Specialist in Government Organization and Management, contributed to this section.

[72] The accompanying report to the legislation that redesignated the senior official as the agency CIO states, "The conferees anticipate that agencies may establish CIOs for major subcomponents or bureaus, and expect agency CIOs will possess knowledge of, and practical experience in, information and information technology management practices of business or government entities." See U.S. Congress, *National Defense Authorization Act for Fiscal Year 1996*, Conference Report, to accompany S. 1124, 104th Cong., 2nd sess., January 22, 1996, Report 104-450 (Washington: GPO, 1996), p. 977.

[73] With regard to mission support, IRM activities may require technical expertise in areas such as curation, access, systems, security, and privacy. At times, it may be economical to pool this capacity together and provide "shared services" to many of an agency's mission-delivering organizational units and programs rather than embed technical capacity in each agency component or program. However, centralization of mission support might make services less customized, responsive, or nimble in serving particular agency components, programs, and mission needs. With regard to mission delivery, these organizations focus on activities such as providing benefits to clients, protecting the environment, promoting safe air travel, conducting diplomacy, and fighting or deterring armed conflicts.

[74] For example, see National Academy of Public Administration, *Department of Energy: Managing at the Speed of Light, Improving Mission-Support Performance*, July 2009, https://napawash.org/uploads/Academy_Studies/09-03.pdf. Other examples of mission support functions include human resources, procurement, and financial management.

or even competition about who should exercise effective control or influence in key venues and processes. This mix of mission delivery and mission support responsibilities in IRM is reflected in statute by simultaneously vesting responsibility for IRM in the head of an agency,[75] requiring the designation of a statutorily established CIO to report directly to the agency head and carry out agency responsibilities,[76] and vesting responsibility and accountability in each agency program official for related information resources.[77]

Organizational Location of Agency CIOs

Another dynamic for statutorily established CIO positions relates to potential implications of their organizational location. Statute requires CIO positions be designated at the agency level, which is defined to include executive departments (e.g., the Department of Commerce) and establishments in the executive branch (e.g., the Environmental Protection Agency), among other, less common types of federal entities.[78] However, there is no general statutory requirement for a CIO position to be established or designated in suborganizations below the overall agency level.[79]

This variable structure can have implications for an agency CIO, because large federal agencies typically have multiple "component" organizations that perform most of the agencies' mission delivery activities.[80] In a large department, each major mission delivery component might be formally known as a bureau, administration, or service and have a distinct, corresponding mission or set of missions. Furthermore, each component may develop its own mission support function(s) related to IRM—or embed certain mission support capacity directly within program offices—in ways that are customized to the component's mission, environment, and history. Consequently, the CIO of a department, for example, might face challenges in attempting to exercise oversight and influence over the varied IRM activities of an agency's diverse and large components. If a component organization views the agency-level CIO function as being relatively distant from or ignorant of issues facing the component, the CIO may face further challenges in navigating the agency's ecosystem of officials and offices.

Collaboration Between CIOs and Other "CXO" Officials

A third potential dynamic for CIOs relates to collaboration with the heads of other agency mission support functions in support of the agency mission. These positions are sometimes referred to generically as "CXOs," where the *x* is a variable for other subjects such as human

[75] 44 U.S.C. §3506(a)(1).

[76] 44 U.S.C. §3506(a)(2) and (3).

[77] 44 U.S.C. §3506(a)(4).

[78] 44 U.S.C. §3502(1). See further discussion under "Practice 10.—Position a Chief Information Officer as a senior management partner," U.S. Congress, Senate Committee on Governmental Affairs, Paperwork Reduction Act of 1995, Report to accompany S. 244, 104th Cong., 1st sess., February 14, 1995, S.Rept. 104-8 (Washington: GPO, 1995), p. 101.

[79] In the conference agreement accompanying the legislation that formally established CIO positions, the conferees said they "anticipate that agencies may establish CIOs for major subcomponents or bureaus." U.S. Congress, Conference Committee, National Defense Authorization Act for Fiscal Year 1996, conference report to accompany S. 1124, 104th Cong., 2nd sess., H.Rept. 104-450, January 22, 1996, p. 977, https://www.congress.gov/104/crpt/hrpt450/CRPT-104hrpt450.pdf#page=980.

[80] OMB defines the term *component (of an agency)* to "describe major organizational units, such as a bureau, administration, or office, within a department or agency." OMB, *Circular No. A-11: Preparation, Submission, and Execution of the Budget*, August 2023, Section 200, p. 18, https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf.

capital, acquisition, and financial management.[81] Within the IRM field and adjacent to it, a variety of similar positions have been established by statute and practice to bring specialized attention to topics—for example, information stewardship (chief data officer),[82] information security (chief information security officer),[83] privacy (senior accountable official for privacy [SAOP]),[84] statistical uses of information for statistical purposes (agency "statistical official"),[85] and other aspects of IRM and information use (e.g., agency "evaluation officer").[86]

The working relationships among the CIO and these other CXO positions may be idiosyncratic to individual agencies. As with the relationship between mission delivery offices and mission support functions, issues of collaboration and division of labor may appear in these contexts as well.

CIO Council

CIOs also convene as the CIO Council. Originally established by Executive Order 13011 and later codified by the E-Government Act of 2002, the CIO Council is the "the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of Federal Government information resources."[87]

The council's members include three OMB officials, including the deputy director for management (DDM), the administrator of the Office of Electronic Government (E-Gov), the administrator of the Office of Information and Regulatory Affairs (OIRA). The council also includes CIOs of CFO Act agencies and selected other agencies and any other officer or employee of the United States as designated by the chair.[88] Although the DDM acts as the CIO Council chair, the E-Gov administrator is to lead the council's activities on behalf of the DDM.[89] A vice chair of the council is to be selected from among the council's members to serve for a term of one year.[90]

The CIO Council is first tasked with developing recommendations for the OMB director related to government IRM policies and requirements, among other responsibilities. These include that the CIO Council is to:

- share experiences, ideas, and best practices related to IRM;
- help identify and coordinate multiagency projects to improve government performance through IT; and

[81] For discussion, see CRS Report RL32388, *General Management Laws: Major Themes and Management Policy Options*, by Clinton T. Brass.

[82] 44 U.S.C. §3520.

[83] 44 U.S.C. §3554(a)(3)(A).

[84] OMB, *Memorandum No. M-16-24: Role and Designation of Senior Agency Officials for Privacy*, September 15, 2016, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m_16_24_0.pdf.

[85] 5 U.S.C. §314.

[86] 5 U.S.C. §313.

[87] 44 U.S.C. §3603(d). See also Executive Order 13011, "Federal Information Technology," 61 *Federal Register* 37658-37660, July 19, 1996; and P.L. 107-347, 116 Stat. 2905-2906.

[88] 44 U.S.C. §3603(b).

[89] 44 U.S.C. §3603(c)(1).

[90] 44 U.S.C. §3603(c)(2).

- promote the development and use of common performance measures for agency IRM.[91]

In addition, the CIO Council is expected to work with other agencies and departments, including (1) the National Institute of Standards and Technology within the Department of Commerce and the E-Gov administrator to develop recommendations on IT standards;[92] (2) OPM to assess and address the hiring, training, classification, and professional development needs;[93] and (3) the Archivist of the United States (the head of NARA) to assess how the Federal Records Act can be addressed through IRM activities.[94]

Given the CIO Council's orientation as an interagency forum to inform OMB's development of IRM policies as well as the number of OMB officials serving as members of the council, the council may prioritize or be influenced by OMB's perspective on IRM and IT issues.

OMB Roles and Responsibilities

In addition to agency-level interactions, certain agency missions are intertwined with the government-wide management of information. For example, (1) the Department of Commerce with respect to developing and issuing standards for information security and privacy, (2) the Department of Homeland Security with respect to its responsibilities under FISMA, (3) the General Services Administration with respect to providing a government-wide network services contracts and other shared services, (4) NARA with respect to administering the Federal Records Act and developing electronic records management regulations,[95] and (5) OPM with respect to analyzing the government's workforce needs related to IRM and IT.[96]

Statute authorizes the OMB director with the overall authority to develop, coordinate, and oversee the implementation of federal IRM policies, principles, standards, and guidelines. Specifically, statute requires the OMB director to provide direction and oversee six areas related to the CIO's roles and responsibilities, including:

1. Information collection and control of paperwork;
2. Information dissemination;
3. Statistical activities;
4. Records management;
5. Privacy, confidentiality, security, and sharing of information; and
6. Acquisition and use of IT.[97]

These areas also demonstrate the blending of responsibilities among different constituencies within OMB, including the administrator of OIRA, the chief statistician, and the administrator of

[91] 44 U.S.C. §3603(f). A schedule of CIO Council meetings is available at https://www.cio.gov/about/operations/.

[92] 44 U.S.C. §3603(f)(5).

[93] 44 U.S.C. §3603(f)(6).

[94] 44 U.S.C. §3603(f)(7).

[95] See also Executive Order 13526, "Classified National Security Information," 75 *Federal Register* 707-731, January 5, 2010, and Executive Order 13556, "Controlled Unclassified Information," 75 *Federal Register* 68675-68677, November 9, 2010, for NARA's role with respect to classified information.

[96] OMB, *Circular No. A-130,* pp. 20-25.

[97] 44 U.S.C. §3504(a).

E-Gov. The chief statistician is the head of the statistical and science policy office of OIRA.[98] Within OMB, these three roles are divided among OIRA, which was established by the Paperwork Reduction Act of 1980, and E-Gov, which was established by the E-Government Act of 2002.[99] However, the offices themselves are intertwined: The E-Gov administrator is to work with the OIRA administrator to set strategic direction for implementing electronic government under relevant statutes, including Chapter 35 of Title 44 and Subtitle III of Title 40 of the *U.S. Code*.[100]

In practice, the overlap between these areas may further blur the delineation of responsibilities between these two offices within OMB. To suggest clarity and a division of labor among the offices supporting the OMB director's six roles and responsibilities, OMB has in recent years referred to the E-Gov administrator as the "Federal CIO."[101] Some have also suggested formalizing this position as the federal CIO and establishing responsibilities and authorities over government-wide IT management.[102] Such a change would not necessarily resolve or clarify questions surrounding the division of labor among the remaining areas of responsibility within OMB.[103]

Issues for Congress

In many ways, the development and redevelopment of the CIO position is indicative of Congress's evolving understanding of how information should be managed within agencies. Congress may continue to consider the effectiveness of the position in light of the growing expertise in areas such as information privacy and security, statistical information, and IT. Congress may examine whether information management responsibilities should be centralized within the CIO or divided among other agency officials and whether the CIO position should be standardized across heterogenous agency organizations and sizes.

CIO Structure Within an Agency

Recent legislative and executive branch efforts have created a confederation of agency officials involved in information management, and Congress may examine how these officials interact with one another in practice and as required to by law. While some agencies may have officials serving single roles, other agencies may have one official serving multiple roles. Centralizing

[98] OMB, "Statistical Programs and Standards," https://www.whitehouse.gov/omb/information-regulatory-affairs/statistical-programs-standards/.

[99] For more information on these offices, see CRS Report RS21665, *Office of Management and Budget (OMB): An Overview*, coordinated by Taylor N. Riccard.

[100] 44 U.S.C. §3602(d).

[101] See, for example The White House, Office of the Press Secretary, "Presidential Memorandum—Building a 21st Century Digital Government," press release, May 23, 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/05/23/presidential-memorandum-building-21st-century-digital-government; and The White House, "Office of the Federal Chief Information Officer," retrieved July 5, 2024, https://www.whitehouse.gov/omb/management/ofcio/.

[102] U.S. Government Accountability Office (GAO), *Chief Information Officers: Private Sector Practices Can Inform Government Roles*, GAO-22-104603, September 2022, p. 37, https://www.gao.gov/assets/d22104603.pdf.

[103] Similar issues may also arise in the context of agency CIOs and their roles and responsibilities. For example, a body of work from GAO has focused primarily on IT-related duties of agency CIOs, with a footnote acknowledgement that GAO "did not review the following CIO responsibilities relating to information management: information collection/paperwork reduction, information dissemination, information disclosure, statistical policy and coordination, records management, and privacy." See GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-93, August 2, 2018, p. 2, https://www.gao.gov/products/gao-18-93.

information management responsibilities within the CIO may streamline agency reporting structures but may also overtax the resources of the CIO office. Because information collection, curation, use, security, and disposal cut across many types of agency functions, an effectively functioning CIO position would appear to work in isolation only in rare situations, leading to challenges in determining how information management should be structured among agency officials. Nonetheless, OMB states that the agency CIO must still retain "accountability for the assigned role or responsibility and thus must ensure the overall suitability of selected officials."[104]

Conversely, other agencies may delegate information management activities to a variety of officials at the agency or component levels, as is consistent and appropriate with OMB guidance. In addition, Congress anticipated that agencies would delegate certain CIO responsibilities to its components when it passed Clinger-Cohen in 1996. Because information systems comprise integrated message, media, and storage layers, separating IRM into its component parts might superficially appear to simplify information management but may also streamline agency reporting structures. While this flexibility accomodates differing agency sizes and needs, the delegation of responsibilities could obfuscate accountability, particularly in the case of an operational failure. Similar to concerns that the CIO position may be customized to each agency's structure, preferencing certain CIO responsibilities (for example, IT or control of paperwork) may de-emphasize the others without clarifying roles or responsibilities among other agency stakeholders.

Congress may examine how agencies delegate CIO responsibilities and how differing patterns of delegation might impact agency operational outcomes. In addition, Congress might consider agency reporting hierarchy to the CIO and whether the CIO should behave as a convener of information management interests across the agency, or if the CIO should instead be seen as a peer official alongside the CDOs, SAOPs, and others.

Agency Size

Heterogeneity in agency sizes and missions may result in different aspects of IRM being emphasized or de-emphasized. For example, in an attempt to account for variability among agency resources, certain additional statutory responsibilities related to IT budgeting, capital planning, and investment control apply only to CIOs at larger agencies.

Given the increased importance of IT in supporting agency missions and facilitating interactions with the public, Congress may consider expanding certain IT statutory responsibilities to CIOs to additional agencies. In doing so, Congress may examine how this expansion of CIO responsibilities could be balanced against concerns that smaller agencies may lack the capacity to carry out additional activities.

[104] OMB, *Memorandum No. M-15-14*, p. 16.

Appendix. Enumeration of CIO Responsibilities

Table A-1. CIO Responsibilities Under 44 U.S.C. §3506

Agency Responsibilities with Respect to General Information Resources Management

Responsibility	Statutory Citation
Information Resources Management	
Manage information resources to (1) reduce information collection burdens on the public, (2) increase program efficiency and effectiveness, and (3) improve the integrity, quality, and utility of information to users within and outside the agency.	44 U.S.C. §3506(b)(1)
Develop an annually updated and publicly available strategic information resources plan in accordance with OMB director guidance that describes how information resources management activities help accomplish agency missions.	44 U.S.C. §3506(b)(2)(A) and (C)
Develop an open data plan to include processes and procedures related to data collection mechanisms in accordance with the Open, Public, Electronic, and Necessary Government Data Act (Title II of P.L. 115-435) and implements methods for analyzing data asset usage.	44 U.S.C. §3506(b)(2)(B) and (C)
Develop an ongoing process to ensure that information resources management opertions and decisions are integrated with organizational planning, budget, financial management, human resources management, and program decisions.	44 U.S.C. §3506(b)(3)(A)
Develop, in cooperation with the agency chief financial officer, a full and accurate accounting of IT expenditures related to expenses and results.	44 U.S.C. §3506(b)(3)(B)
Establish goals for improving information resources management's contribution to program productivity, efficiency, and effectiveness; methods for measuring progress; and clear roles and responsibilities for achieving those goals.	44 U.S.C. §3506(b)(3)(C)
Maintain a current and complete inventory of the agency's information resources in consultation with the OMB director, administrator of the General Services Administration, and the Archivist of the United States.	44 U.S.C. §3506(b)(4)
Conduct formal training programs to educate agency program and management officials about information resources management in consultation with the OMB director and the OPM director.	44 U.S.C. §3506(b)(5)
Make each data asset of the agency available in an open format and make each public data asset of the agency available under an open license in accordance with OMB guidance.	44 U.S.C. §3506(b)(6)
Information Collection and Control of Paperwork	
Establish a process within the CIO office to evaluate and review proposed collections of information prior to submission to the OMB director by considering the need for the information and estimating the paperwork burden.	44 U.S.C. §3506(c)(1)(A)
Establish a process within the CIO office to ensure that each information collection is inventoried, displays a control number, provides details on its use, and informs respondents of the reasons for the information collection.	44 U.S.C. §3506(c)(1)(B)
Establish a process within the CIO office to assess the information collection burden of proposed legislation affecting the agency.	44 U.S.C. §3506(c)(1)(C)
Provide 60-day notice in the *Federal Register* and consult with members of the public and affected agencies concerning proposed information collections and provide notice and comment for information collections in a proposed rule.	44 U.S.C. §3506(c)(2)(A) and (B)
Certify that each information collection submitted to the OMB director for review is necessary, does not duplicate other reasonably accessible information, and reduces to the extent practicable the burden on respondents.	44 U.S.C. §3506(c)(3)

Responsibility	Statutory Citation
Make efforts to reduce the information collection burden for small business concerns with fewer than 25 employees.	44 U.S.C. §3506(c)(4)
Establish one point of contact in the agency to act as a liaison between the agency and small business concerns.	44 U.S.C. §3506(i)
Information Dissemination	
Ensure that the public has timely and equitable access to the agency's public information and, in cases where the agency provides public information in an electronic format, provide access to the underlying data (in whole or in part).	44 U.S.C. §3506(d)(1)
Regularly solicit and consider public input on the agency's information dissemination activities and provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products.	44 U.S.C. §3506(d)(2) and (3)
Shall not establish an exclusive or restrictive arrangement that interferes with timely and equitable availability of public information, including any restriction or regulation for redissemination of public information.	44 U.S.C. §3506(d)(4)
Ensure that any public data asset of the agency is machine-readable.	44 U.S.C. §3506(d)(5)
Engage the public in using public agency data assets and encourage collaboration by publishing information on data assets on the agency's website and providing the public with the opportunity to request specific data assets to be disclosed.	44 U.S.C. §3506(d)(6)
Statistical Policy and Coordination	
Ensure the relevance, accuracy, timeliness, integrity, and objectivity of information collected or created for statistical purposes.	44 U.S.C. §3506(e)(1)
Inform respondents fully and accurately about the sponsors, purposes, and uses of statistical surveys and studies and protect respondents' privacy.	44 U.S.C. §3506(e)(1) and (2)
Observe federal standards and practices for data collection, analysis, documentation, sharing, and dissemination of information.	44 U.S.C. §3506(e)(4)
Ensure the timely publication of the results of statistical surveys and studies, including information about the quality and limitations of the surveys and studies.	44 U.S.C. §3506(e)(5)
Make data readily accessible to the public and available to statistical agencies.	44 U.S.C. §3506(e)(6)
Records Management	
Implement and enforce applicable policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design and operation of information systems.	44 U.S.C. §3506(f)
Privacy and Security	
Implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected or maintained by or for the agency.	44 U.S.C. §3506(g)(1)
Assume responsibility and accountability for compliance with and coordinated management of the Freedom of Information Act; the Privacy Act of 1974, 44 U.S.C. Chapter 35 Subchapter II, and related information management laws.	44 U.S.C. §3506(g)(2)
Federal Information Technology (IT)	
Implement and enforce applicable government-wide and agency IT management policies, principles, standards, and guidelines.	44 U.S.C. §3506(h)(1)
Assume responsibility and accountability for IT investments.	44 U.S.C. §3506(h)(2)

Responsibility	Statutory Citation
Promote agency use of IT to improve the productivity, efficiency, and effectiveness of agency programs; reduce information collection burdens on the public; and improve dissemination of information.	44 U.S.C. §3506(h)(3)
Propose changes in legislation, regulations, and agency procedures to improve IT practices, including changes that improve the ability of the agency to use technology to reduce burden.	44 U.S.C. §3506(h)(4)
Assume responsibility for maximizing the value and assessing and managing the risks of major information systems initiatives through a process that is integrated with budgetary and program management decisions.	44 U.S.C. §3506(h)(5)

Source: CRS analysis of the *U.S. Code*.

Notes: 44 U.S.C. §3506(a)(2) requires the head of each agency to designate a CIO who shall report directly to the agency head to carry out the responsibilities of the agency under 44 U.S.C. Chapter 35 Subchapter I. Some of these areas of responsibility have additional explanations and requirements under other areas of Chapter 35.

Table A-2. Selected CIO Responsibilities Under 40 *U.S. Code* Subtitle III

Agency Responsibilities with Respect to Information Technology Management

Responsibility	Statutory Citation	Definition of Agency
Information Technology (IT) Accountability		
Report to the agency head or deputy on matters of information policy.	44 U.S.C. §3506(a)(2)(A)	Executive Agencies
Assume responsibility and accountability for IT investments.	44 U.S.C. §3506(h)(2) and 40 U.S.C. §11312	Executive Agencies
Approve the appointment of CIOs at agency components.	40 U.S.C. §11319(b)(2)	CFO Act Agencies
Assess performance of agency officials with information management responsibilities.	40 U.S.C. §11315(c)(3)(B)	Executive Agencies
IT Performance Management		
Establish goals for improving agency operations through IT.	40 U.S.C. §11313(1)	Executive Agencies
Prepare an annual report on the progress in achieving the goals.	40 U.S.C. §11313(2)	Executive Agencies
Ensure that performance measures are suited to the agency's IT.	40 U.S.C. §11313(3)	Executive Agencies
Benchmark agency performance against other private and public sector organizations.	40 U.S.C. §11313(4)	Executive Agencies
Revise agency processes before making IT investments.	40 U.S.C. §11313(5)	Executive Agencies
IRM Workforce		
Assess annually the requirements for agency personnel regarding information resources management.	40 U.S.C. §11315(c)(3)(A)	Executive Agencies
Assess annually the extent to which agency personnel meet information resource management knowledge and skill requirements.	40 U.S.C. §11315(c)(3)(B)	Executive Agencies
Develop strategies annually for hiring and training.	40 U.S.C. §11315(c)(3)(C)	Executive Agencies

Responsibility	Statutory Citation	Definition of Agency
Report annually to the head of the agency on improvements in information resources management capabilities.	40 U.S.C. §11315(c)(3)(D)	Executive Agencies
IT Budgeting		
Has a significant role in IT planning, programming, and budgeting decisions.	40 U.S.C. §11319(b)(1)(A)	CFO Act Agencies
Approves agency IT budget request.	40 U.S.C. §11319(b)(1)(B)(i)	CFO Act Agencies
Approve reprogramming of funds made available for IT programs.	40 U.S.C. §11319(b)(1)(C)(i)(II)	CFO Act Agencies
Be responsible for system for selecting IT investments.	44 U.S.C. §3506(h)(5)(B)	Executive Agencies
IT Capital Planning and Investment Control		
Has a significant role in IT planning, programming, and budgeting decisions.	40 U.S.C. §11319(b)(1)(A)	CFO Act Agencies
Consult the OMB director on improving the management of agency IT through portfolio review.	40 U.S.C. §11319(d)(1) and (2)	CFO Act Agencies
Categorize IT investments according to risk.	40 U.S.C. §11302(c)(3)(C)	CFO Act Agencies
Review high-risk IT investments.	40 U.S.C. §11302(c)(4)	CFO Act Agencies
Certify that IT investments are implementing incremental development as defined by OMB capital planning guidance.	40 U.S.C §11319(b)(1)(B)(ii)	CFO Act Agencies
Monitor the performance of IT programs and advise agency head on whether to continue, modify, or cancel a program.	40 U.S.C. §11315(c)(2)	CFO Act Agencies
Coordinate with agency head and agency chief financial officer or other comparable official to ensure that financial management systems are effective.	40 U.S.C. §11316	Executive Agencies
Approve IT contracts or acquisition plans.	40 U.S.C. §11319(b)(1)(C)(i)(I)	CFO Act Agencies
Responsible for system for selecting IT investments.	44 U.S.C. §3506(h)(5)(B) and 40 U.S.C. §§11312 & 11313	Executive Agencies

Source: CRS analysis of the *U.S. Code*.

Notes: 40 U.S.C. §11315(b) requires the head of each agency to designate a CIO who shall report directly to the agency head to carry out the responsibilities of the agency under Subtitle III of Title 40.

Author Information

Meghan M. Stuessy
Analyst in Government Organization and Management

Dominick A. Fiorentino
Analyst in Government Organization and Management

Disclaimer