The Evolution of the Role of CIO in the U.S Federal Government

Full Report

March 2016

Julie M. Anderson
Principal
AG Strategy Group

Bethesda, MD, USA

The Evolution of the Role of CIO in U.S Federal Government
Full Report

In the U.S. federal government, Congress and Presidents have changed the role and responsibilities of the Chief Information Officer (CIO) multiple times over the past 20 years. Although a relatively recent addition to government agencies as compared with large corporations, the CIO is a vital position to help transform organizations as they deliver effective and efficient government services in the modern age.[1] Ultimately, the CIO role is intended to provide strategic leadership over information technology resources and advise the agency head to make good decisions about those resources. And the role has evolved from an operationally-oriented director of information resources management (IRM) position to one responsible for a strategic portfolio of investments that supports the mission of the government agency.

Congress has passed seven laws or sections of laws that direct the role and responsibilities of the CIO. The federal government includes two levels of CIO positions: a federal CIO at the President's Office of Management and Budget (OMB) who oversees all agencies, and an agency CIO at each cabinet-level department such as the U.S. Department of Treasury or smaller agency like the Small Business Administration. The statutes governing both types of CIO roles (with the exception of national security purposes) are listed in chronological order:

- Freedom of Information Act of 1946 (FOIA)
- The Privacy Act of 1974
- The Paperwork Reduction Act of 1995 (PRA)
- Clinger Cohen Act of 1996 (CCA)
- The E-Government Act of 2002
    - Federal Information Security Management Act section of The E-Government Act of 2002 (FISMA)
- Federal Information Technology Acquisition Reform Act of 2014 (FITARA)

Most notably, Congress shaped the federal and agency CIO roles through three of these laws: CCA, E-Government Act, and FITARA. And the other four laws discussed in this paper outline important responsibilities that each CIO must perform as part of his or her position. This report discusses the provisions in each law that contributed to the evolving role of the CIO over the past 20 years as well as suggested improvements to the CIO role in the future.

[1] http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/emergenceofcio/

Recommendations for Enhancing CIO Role Post-FITARA

Although Congress and Presidents have taken important steps to expand and clarify the roles of federal and agency CIO, they can do more to strengthen the position and improve agency decision making about information technology resources. Experts on government and technology have suggested various changes for the next round of reforms. Not all of these experts are in agreement about needed changes:

- Federal CIO
    - Centralize control of all infrastructure, applications, contracts, and enterprise licenses under one federal CIO position. In addition, create one government-wide organization for each technology function such as cyber security, which would be headed by a deputy CIO who reports to the federal CIO.
    - Integrate four of the primary statutes governing the role of the CIO into one framing statute that mirrors the structure OMB uses for its overarching information technology guidelines to all agencies – OMB Circular A-130. Those four laws are: Paperwork Reduction Act of 1995, Clinger – Cohen Act of 1996, FISMA, and FITARA.

- Agency CIO
    - Elevate the agency CIO role to be the strategic leader over all information resources including data and not only information technology. (FITARA defines CIO responsibilities over information technology.)
    - Change the CIO political leader position at each agency to integrate all information resources and manage deputy CIOs with specific responsibilities for certain functions such as IT, cyber, information policy.
    - Move the entire agency's IT budget under the agency CIO's decision making authority.
    - Clarify program ownership of IT programs so that the agency executive with mission responsibilities, e.g. Assistant Secretary for Policy, can be part of the process when CIO prioritizes list of IT investments across an agency
    - Address the downsides of the centralized acquisition of all technology resources through the agency CIO. That is, under FITARA the CIO will be responsible for all procurement decisions at the local level. This approach is neither efficient nor realistic. Instead, CIO at HQ should issue guidelines about acceptable parameters and encourage innovation at local levels.

Introduction

In the 1990s, Federal policymakers favored government reform and tangible results. They asserted government organizations should apply management lessons from business to more effectively and efficiently provide services and programs to constituents. Simultaneously, the U.S. economy was in a slump. The economic downturn, persistent

unemployment, and years of growing government expenditures caused voters politicians to demand that government do better.[2]

In this political environment, President William J. Clinton created a National Performance Review (later called the National for Partnership for Reinventing Government) intended to identify duplication and waste in government organizations and hold up exemplary models of efficient and effective government programs. It was the eleventh effort to reform the federal government in the 20th Century.

President Clinton cited the current economic downturn, low productivity, persistent unemployment, and years of growing government and declining investment in Americans' future as reason to reform government. The purpose of NPR was to create a government that works better and cost less. More specifically, "invent government that puts people first, by: serving its customers, empowering its employees, and fostering excellence." In order to achieve this, the objectives of the NPR were to "create a clear sense of mission; delegate authority and responsibility; replace regulations with incentives; develop budget-based outcomes; and measure [our] success by customer satisfaction."[2]

Congress acted on several legislative proposals stemming from the National Performance Review recommendations including the Federal Acquisition Reform Act of 1995. Notably, Congress also created the agency CIO role in the midst of this effort to improve government.

The Government Performance and Results Act of 1993

In this push to reform government, Congress passed the Government Performance and Results Act of 1993 (GPRA). The law focuses on improving performance management by requiring agencies to set goals, plan activities to achieve those goals, measure results, and report annual progress. More specifically, GPRA requires agencies to engage in the following three processes:

- Develop a five-year strategic plan based on the agency's mission statement and including results-oriented goals covering each of its major functions
- Prepare annual performance plans that set forth annual goals and plans to achieve these goals
- Prepare annual performance reports that measure organization's progress or failure in meeting its targeted performance goals

GPRA assigned responsibilities for implementation of the law to agency Chief Financial Officers and policy and planning officials. In addition, senior agency IT officials had to comply with the mandate to articulate goals and measure progress for all technology programs. GPRA's new requirements changed all senior executive roles in an agency -- including the senior IT official role -- to be more focused on producing specific results.

---

[2] http://govinfo.library.unt.edu/npr/library/papers/bkgrd/brief.html

For example, agencies developed metrics to measure results such as metric intended to measure the value of IT investments or percent of IT projects within 10% of budgeted cost. Another instance is a metric to measure the protection of federal IT assets and information or average percentage of IT assets subject to an automated inventory, configuration, or vulnerability management capability.

Congress passed the Government Performance and Results Modernization Act in 2010. This law was the first update in almost 20 years since the original GPRA passed. The GPRA Modernization Act put into place some lessons learned from agencies in setting goals and reporting performance. It focuses on setting priorities, cross-organizational collaborate to achieve shared goals, and the use of analysis of goals and measures to improve outcomes of federally funded programs.[3]

The Paperwork Reduction Act of 1995 (PRA)

During the 1990s era of government reform, Congress also passed a significant update to a 1980 law or The Paperwork Reduction Act of 1995 (PRA). The purpose of both statutes is to reduce the burden of paperwork the federal government places on people and businesses. The law outlines a required process for agencies to follow before they collect information from the public.[4]

- Determine a specific objective for collecting the information
- Seek public comment on proposed collections of information through "60-day notices" in the Federal Register;
- Certify to OMB that efforts have been made to reduce the burden of the collection on small businesses, local government and other small entities,
- Have in place a process for independent review of information collection requests prior to submission to OMB.

The 1980 PRA was the first law to put the information resources management (IRM) approach in place. The statute articulated the approach as "IRM combined IT with information management areas, including information collection, records management, and privacy.[5]"

PRA also established the Office of Information and Regulatory Affairs (OIRA) in OMB and assigned it the authority to administer all functions of the PRA. This process makes OIRA into a centralized clearinghouse for all government forms. Thus, it is able to assess the overall impact of the government bureaucracy on American citizens and businesses.

---

[3] http://www.samhsa.gov/grants/gpra-measurement-tools
[4]http://ocio.os.doc.gov/ITPolicyandPrograms/Information_Collection/dev01_003742

[5] http://www.gao.gov/assets/590/585305.pdf

Importantly, agency CIOs became responsible for managing and coordinating data requests across agencies after their new role was established in 1996. This responsibility was the first instance in which the senior IT leader in an agency had cross-cutting authority in an organization. In addition to the responsibilities above, the PRA identifies several other activities relating to the management of federal information resources, which is the other primary focus of the PRA. These include coordinating IRM policies and practices to improve the productivity, efficiency, and effectiveness of Government programs, and improve service delivery to the public, and providing for the dissemination of public information on a timely basis.

Analysis of The Clinger Cohen Act of 1996 (CCA)

One year after the enactment of PRA, Congress passed The Clinger Cohen Act of 1996 (CCA). The law added detailed requirements for IT capital planning and investments and instituted performance and results-based management consistent with the intent of GRPA. It also augmented the information technology provisions of PRA.

Notably, CCA created the position of an agency CIO to be filled by a political appointee. In the era of mainframe computers and long before the Internet, Congress viewed the newly established CIO role as one way to mitigate the large IT system failures plaguing government agencies. At that time, the federal government did not have a senior IT leader at the Chief level in agencies or at the White House.

CCA provides that the government information technology organization be operated as an efficient and profitable business would be operated. The acquisition, planning, and management functions of technology must be treated as a "capital investment." Congress' intent reflects the political environment of the 1990s when policymakers wanted government to act more like a private sector organization.

By passing the new legislation, Congress intended to shift the focus away from acquisition management to investment management for information technology resources. That is, begin treating IT spending as a capital investment, complete with a process to plan, analyze, track and evaluate results. The CIO plays a critical leadership role in driving reforms to: [4]

- Help control system development risks
- Better manage technology spending
- Succeed in achieving real, measurable improvements in agency performance

Congress assigned CIOs the authority and management responsibility necessary to advise agency heads on budget, program, and implementation issues concerning information technology. Among other responsibilities, CIOs oversee the design, development, and implementation of information systems. CIOs also monitor and evaluate system performance and advise agency heads whether to modify or terminate those systems. It also returned IT procurement authority to each agency.

Congress' intent through CCA was to create a senior leader position with responsibility over the portfolio of IT programs in addition to advising the agency head on strategic decisions. However, the agencies' implementation of the new CIO authority was uneven because it depended on two factors. First, each Secretary, Deputy Secretary, and CFO had the discretion to cede as much authority to the CIO as they wanted to. Second, the individual skills of each CIO determined, in part, whether they executed their responsibilities effectively.

Prior to CAA, the senior IT leader at an agency was a career civil servant who did not have political authority. The career status limited their ability to affect decisions at the level of the political agency head. Similarly, the senior IT official at OMB was a career civil servant without political authority. But CCA created a downside when it changed the senior IT leader position from career civil servant to a CIO political appointee: the camaraderie among the career civil servants in each agency declined. The group of career civil servants had banded together and collaborated closely because they were more powerful as a group than as individuals. This positive dynamic was now lost with the addition of the political appointee role.

The law put into place many changes for the senior IT role at an agency. "The Clinger-Cohen Act establishes clear accountability for IRM activities by creating agency Chief Information Officers (CIOs) with the authority and management responsibility necessary to advise agency heads on budget, program, and implementation issues concerning information technology. Among other responsibilities, CIOs oversee the design, development, and implementation of information systems. CIOs also monitor and evaluate system performance and advise agency heads whether to modify or terminate those systems. The Clinger-Cohen Act directs agencies to work together towards the common goal of using information technology to improve the productivity, effectiveness, and efficiency of Federal programs and to promote an interoperable, secure, and shared government-wide information resources infrastructure.[6]"

The law also shifted day-to-day responsibilities for information technology from the General Services Agency (GSA) to OMB. Specifically, it grants the Director of OMB authority to oversee the acquisition, use, and disposal of information technology by the Federal government, so as to improve the productivity, efficiency, and effectiveness of Federal programs through these activities:

- Developing a process for analyzing, tracking, and evaluating the risks and results of major capital investments
- Directing executive agencies on establishing an effective, efficient IT capital planning and investment review process
- Enforcing accountability through the budget process[7]

---

[6] https://www.whitehouse.gov/omb/fedreg_a130notice

[7]http://ocio.os.doc.gov/ITPolicyandPrograms/Information_Collection/dev01_003742

"It supplements the information resources management (IRM) policies contained in the Paperwork Reduction Act (PRA) (44 U.S.C. Chapter 35) by establishing a comprehensive approach to improving the acquisition and management of agency information systems through work process redesign, and by linking planning and investment strategies to the budget process.[8]"

The most comprehensive guidance from OMB related to information technology is called OMB Circular No. A-130, "Management of Federal Information Resources." It contains the policy framework for the management of federal information resources. OMB revised Circular A-130 on February 20, 1996. To provide agencies with additional guidance on implementing the Clinger Cohen Act, and for other purposes, OMB on April 13, 2000 (65 FR 19933) requested public comment on a proposed revision to this Circular.

CCA also returned IT procurement authority to each agency. The law granted organizations such as the U.S. Departments of Homeland Security and Treasury the responsibilities to:

- Establish an IT capital planning and investment review process,
- Use performance measures to assess how well IT supports programs, and
- Justify continuation of systems that deviate from cost, performance, or schedule goals.

E-Government Act of 2002 Public Law 107-347

In the beginning of his administration, President George W. Bush sought to elevate the political authority of the White House over technology in the agencies. His administration created a political position at OMB focused on IT but without any statutory authority. The position was a Program Associate Director (PAD) for IT, which was consistent with the five other PAD roles over certain government agencies. But the PAD for IT position did not have the formal authority that the other PAD roles do.

Two years later, Congress passed The E-Government Act in 2002, which established a position similar to a federal CIO role within OMB. The purpose of the CIO role was to improve the management of electronic government processes and services across government agencies. Congress gave the new position the title, Administrator of E-Government and Information Technology, and created a new office in OMB with the same name. The new role was reserved for a political appointee. However, the law did not materially change the role of an agency CIO.

Unfortunately, the law created an unfunded position in OMB. As Roger Baker, former CIO at Department of Veterans Affairs under President Obama and former CIO at Department of

[8] https://www.whitehouse.gov/omb/fedreg_a130notice

Commerce under President Clinton stated, "OMB's authority remains the power of the purse, and the real authorities there lie with the cabinet secretaries, the director at OMB, and the appropriators in Congress. Departments could ignore the policies from the E-Government and Information Technology office with little to no consequence on their IT budget or operations."

The law also produced a bit of confusion about the distinction between the responsibilities of OIRA and E-Government and Information Technology Office within OMB. Rather than wait for Congressional action to address the confusion, the leaders of OIRA and E-Government Office worked together to clarify the responsibilities of each office. Going forward, OIRA would be responsible for information collection under PRA, information use, and reporting. And the E-Government office would direct IT management, as outlined by Clinger Cohen and FISMA; information use with privacy impact assessments; and information dissemination under the E-Government Act.

Under President Obama, the first person to hold this role began using the title Federal Chief Information Officer. Regardless of the title, the role oversees federal technology spending, federal IT policy, and strategic planning of all Federal IT investments. The CIO is also charged with establishing a government-wide enterprise architecture that ensures system interoperability, information-sharing, and maintains effective information security and privacy controls across the Federal Government.

The responsibilities for the new position included:

- Providing effective leadership of federal Government efforts to develop and promote electronic Government services and processes by establishing an Administrator of a new Office of Electronic Government within the Office of Management and Budget
- Promoting use of the Internet and other information technologies to provide increased opportunities for citizen participation in Government
- Promoting inter-agency collaboration in providing electronic Government services, where this collaboration would improve the service to citizens by integrating related functions, and in the use of internal electronic Government processes, where this collaboration would improve the efficiency and effectiveness of the processes
- Improving the ability of the Government to achieve agency missions and program performance goals
- Promoting better informed decision making by policy makers
- Making the Federal Government more transparent and accountable

The E-Government Act also requires each agency issue Privacy Impact Assessment (PIA) for every technology system within the organization. More specifically, agencies are to evaluate how information about individuals is handled by information systems when collecting new data or developing or buying new systems. PIAs are to focus on individually identifiable information within each system.

Federal Information Security Management Act of 2002 (Title III of E-Government Act of 2002)

Although it was originally introduced as a stand-alone bill, the Federal Information Security Management Act of 2002 (FISMA) was enacted as part of The E-Government Act of 2002. The FISMA section of the E-Government Act may have garnered more attention than the other provisions of the law. "To help protect against threats to federal systems, FISMA 2002 set forth a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. This framework created a cycle of risk management activities necessary for an effective security program. It was also intended to provide a mechanism for improved oversight of federal agency information security programs. To ensure the implementation of this framework, FISMA 2002 assigned specific responsibilities to agencies, their inspectors general, OMB, and National Institutes for Technology (NIST)."[9]

FISMA laid down new, significant responsibilities for agency CIOs related to security of information technology, including:

- Monitoring their agency's implementation of IT standards including common standards for interconnectivity and interoperability, categorization of Federal Government electronic information, and computer system efficiency and security
- Conducting Privacy Impact Assessments for relevant IT systems
- Establishing and operating IT training programs
- Participating in the functions of the CIO Council. CIOs are expected to use their role on the Federal CIO Council to identify and leverage opportunities to partner with other agencies in carrying out FISMA requirements[10]

FISMA 2002 required each agency in the executive branch to develop, document, and implement an information security program that includes the following parts:

- Assessments of the risk that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each system
- Plans for providing adequate information security for networks, facilities, and systems or a group of information systems
- Security awareness training for personnel to teach the information security risks and of their responsibilities in complying with agency policies and procedures

[9] http://www.gao.gov/assets/680/672801.pdf
[10] https://www.whitehouse.gov/sites/default/files/omb/memoranda/m03-18.pdf

- Annual testing and evaluation of the effectiveness of information security policies, procedures, and practices
- Process for planning, implementing, evaluating, and documenting remedial action to address deficiencies in the information security policies, procedures, and practices of the agency
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures to ensure continuity of operations for information systems

Congress updated FISMA when it passed the Federal Information Security Modernization Act of 2014 (FISMA 2014). The law made several changes to the original statute from 2002. First, the law granted the authority to the Secretary of Homeland Security to assist OMB in implementation security practices for federal information systems across government. The Secretary can issue directives to an agency for the "purposes of safeguarding federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk."

Next, FISMA 2014 changed the type of information agencies must report to OMB. More specifically, agencies must now report specific information about threats, incidents, and actions taken to comply with security requirements. This is a change from primarily sharing policy and financial information, as was the case for many years.

Congress also added cyber breach notification requirements for government agencies when it passed FISMA 2014. The law also required OMB to update its overarching Circular A-130 to reflect the changes in statute.

In the years following the implementation of Clinger Cohen and The E-Government Act, multiple experts expressed concerns about the deficiencies of the then-current CIO role. For instance, the Government Accountability Office (GAO) conducted a study in 2011 to identify parts of Clinger Cohen that could be updated to enhance the CIO role. GAO is the independent research agency that evaluates government policies and programs. It found "CIOs do not consistently have responsibility for 13 major areas of IT and information management as defined by law or deemed as critical to effective IT management, but they have continued to focus more attention on IT management-related areas."[11]

The inconsistency among CIOs' responsibilities is illustrated by comparing the CIO role at Department of Commerce and at Department of Veterans Affairs. At that time, the CIO at Department of Commerce had control over a staff of 80 people and a small budget. The sub-agencies (or bureaus) such as the Census Bureau and National Oceanic and Atmospheric Administration controlled the majority of the IT budget and staff. None of the bureau CIOs reported to the department CIO. By contrast, the CIO at Department of Veterans Affairs had total authority and control over all IT staff, assets, and budget throughout the entire department.

[11] http://www.gao.gov/assets/590/585305.pdf

The varied CIO responsibilities in these two agencies produced tangible differences: VA has one, single IT network controlled by the CIO for 330,000 agency employees. The Department of Commerce has about 400 separately controlled networks supporting almost 40,000 employees. These differences underscore the inefficiencies that can result from a weaker CIO position.

GAO stated, "Specifically, most CIOs are responsible for seven key IT management areas: capital planning and investment management; enterprise architecture; information security; IT strategic planning, "e- government" initiatives; systems acquisition, development, and integration; and IT workforce planning. By contrast, CIOs are less frequently responsible for information management duties such as records management and privacy requirements, which they commonly share with other offices or organizations within the agency. In this regard, CIOs report spending over two-thirds of their time on IT management responsibilities, and less than one-third of their time on information management responsibilities."[12]

GAO also concluded CIOs do not always have enough control over IT investments. They have limited influence over hiring and performance evaluations of sub-agency level CIOs. For example, the Department of Homeland Security CIO should have input into hiring the CIO for the Immigration and Citizenship Enforcement sub-agency. GAO recommended more consistent implementation of CIOs' authority could enhance their effectiveness in these areas if OMB established accountability measures to encourage the responsibilities are fully implemented.

Federal Information Technology Acquisition Reform Act (FITARA) of 2014

In 2013, Congress, the Obama Administration, and the American people grew frustrated with the cost overruns and delayed timelines of the healthcare.gov website, which was designed to enroll millions of uninsured Americans in health care insurance. Policymakers responded to the well-publicized failure by reforming the way government agencies contracted with technology companies to provide services and products. In addition, Congress wanted to update the role of CIO in the agencies to clarify their responsibilities in an attempt to avoid a repeat of the healthcare.gov debacle. Around the same time, the House and Senate staff looked to the strong Department of Veterans Affairs CIO role as a model for the position at other agencies.

At the White House, FITARA strengthened the role of The Office of Federal Chief Information Officer. As Karen Evans, former Administrator of the E-Government and Information Technology under President Bush said, "FITARA enhanced the responsibilities of the federal CIO and tied the role back to the E-Government Act and the responsibilities enumerated in it."

The Federal Information Technology Acquisition Reform Act of 2014 (FITARA) enhanced the authority of agency CIOs in numerous, important ways. These changes allow the CIO –

[12] http://www.gao.gov/assets/590/585305.pdf

for the first time – to have an agency-wide view of technology investments. The CIO duties in the planning and budgeting processes were enhanced through the explicit, joint responsibility with the agency CFO. More specifically, the CIO also has a stated role in planning the budget and program management for all technology programs within an agency. The CIO also approves budget requests for technology programs before the submission goes to OMB. The position has visibility into planned and actual expenditures on technology programs. CIOs have shared responsibility with the Chief Acquisition Officer (CAO) over acquisition and procurement including review and approval of acquisition plans and programs. Finally, the agency CIO reviews candidates for sub-agency CIOs and participates in their on-going evaluations. For example, the CIO at the Department of Homeland Security (DHS) would be involved in the hiring process for the CIO at the Customs and Border Protection directorate within DHS.

OMB published a table similar to the one below to guide the implementation of FITARA in the agencies. It lists the provisions of the FITARA statute next to the corresponding CIO responsibilities as interpreted by OMB:

Function	Summary of FITARA Text	CIO Role and Responsibilities
BUDGET FORMULATION AND PLANNING	The head of each covered agency…shall ensure that the CIO of the agency has a significant role in the decision processes for planning, programming, budgeting, and execution decisions.	**Visibility of IT resource plans/decisions to CIO.** CFO and CIO jointly shall define the level of detail with which IT resource levels are described distinctly from other resources throughout the planning, programming, and budgeting stages. This should serve as the primary input into the IT capital planning and investment control documents submitted with the budget.
		CIO role in pre-budget submission for programs that include IT and overall portfolio. The agency head shall ensure the agency-wide budget development process includes the CFO, CAO, and CIO in the planning, programming, and budgeting stages for programs that include IT resources (not just programs that are primarily IT oriented).
		CIO role in planning program management. CIO shall be included in the internal planning processes for how the agency uses IT resources to achieve its objectives. The CIO shall approve the IT components of any plans, through a process defined by the agency head that balances IT investments with other uses of agency funding. This includes CIO involvement with planning for IT resources at all points in their lifecycle, including operations and disposition or migration.
	OMB Director shall require in the annual information technology capital planning guidance that the CIO of each covered agency approve the information technology budget request of the covered agency.	**CIO reviews and approves major IT investment portion of budget request.** Agency budget justification materials in their initial budget submission to OMB shall include a statement that affirms: the CIO has reviewed and approves major IT investments in budget request; CFO and CIO jointly affirm that CIO had significant role in reviewing planned IT support for major program

		objectives; and IT Portfolio includes appropriate estimates of all IT resources included in budget request.
ACQUISITION AND BUDGET EXECUTION	The head of each covered agency…shall ensure that the agency CIO has a significant role in the decision processes for all annual and multi-year planning, programming, budgeting, and execution decisions…and the management, governance, and oversight processes related to IT The OMB Director shall require in annual information technology capital planning guidance that each agency CIO certify that IT investments are adequately implementing incremental development	**Ongoing CIO engagement with program managers.** CIO should establish and maintain a process to engage with program managers to evaluate IT resources supporting each agency strategic objective. It should be the CIO and program managers' shared responsibility to ensure that legacy and on-going IT investments are appropriately delivering customer value and meeting the business objectives of the program.
		Visibility of IT planned expenditure reporting to CIO. CFO, CAO, and CIO should define agency-wide policy for the level of detail of planned expenditure reporting for all transactions that include IT resources.
		CIO defines IT processes and policies. CIO defines the development processes, milestones, review gates, and the overall policies for all capital planning, enterprise architecture, and project management and reporting for IT resources. At a minimum, these processes shall ensure the CIO certifies that IT resources are adequately implementing incremental development. The CIO should ensure that such processes and policies address each category of IT resources appropriately.
		CIO role on program governance boards. In order to ensure early matching of appropriate IT with program objectives, the CIO shall be a member of governance boards that include IT resources, including bureau Investment Review Boards (IRB). CIO shall notify OMB of all government boards the CIO is a member of and at least annually update this notification.
		Shared acquisition and procurement responsibilities. CIO reviews all cost estimates of IT related costs and ensures all acquisition strategies and acquisition plans that include IT apply adequate incremental development principles.
	CIO monitors the performance of IT programs of the agency, evaluates the performance of those programs on the basis of performance measures, and advises the head of the agency regarding whether to continue, modify, or terminate a program or project.	**CIO role in recommending modification, termination, or pause of IT projects of initiatives.** CIO shall conduct reviews or use other performance measures to evaluate the use of IT resources of the agency. The CIO may recommend to the agency head the modification, pause, or termination of any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation.
	A covered agency other than the Department of Defense	**CIO review and approval of acquisition strategy and acquisition plan.** Agencies shall not approve

	may not enter into a contract or other legal agreement for IT or IT services unless the contract has been reviewed and approved by CIO.	an acquisition strategy or acquisition plan or interagency agreement that includes IT without review and approval by the agency CIO. For contract actions that contain IT without an approved acquisition strategy or acquisition plan, the CIO shall review and approve the action itself.
	A covered agency may not request the reprogramming of any funds made available for IT expenditures unless the request has been reviewed and approved by CIO.	**CIO approval of reprogramming.** CIO must approve any movement of funds for IT resources that requires Congressional notification.
ORGANIZATION AND WORKFORCE	CIO shall approve the appointment of any other employee with the title of CIO or who functions in the role of CIO for any component organization within the agency.	**CIO approves bureau CIOs.** CIO shall be involved in recruitment and shall approve the selection of any new bureau CIO. The title and responsibilities of current bureau CIOs may be designated or transferred to other agency personnel by the agency head or his or her designee, and such decisions make take into consideration recommendations from the agency CIO.
	CIO assesses the requirements established for agency personnel regarding knowledge and skill in information resources management and the adequacy of those requirements for helping meet performance goals.	**CIO role in ongoing bureau CIOs' evaluations.** CHCO and CIO shall jointly establish an agency-wide critical element included in all bureau CIOs performance evaluations. In cases where the bureau CIO is a member of the SES this critical element is an agency-specific performance requirement. The agency CIO must identify key bureau CIOs and provide input to the rating official for this critical element. The rating official will consider the input from the agency CIO when determining the initial summary rating.
		Bureau IT Leadership Directory. CIO and CHCO will conduct a survey of all bureau CIOs and jointly publish a dataset identifying all bureau officials with a title of CIO or duties of a CIO. This dataset shall be kept up-to-date.
		IT Workforce. CIO and CHCO will develop a set of competency requirements for IT staff, including IT leadership positions, and develop and maintain a current workforce planning process to ensure the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the IT talent needed to accomplish the mission.
	The head of each agency shall designate a CIO who shall report directly to such agency health to carry out the CIO responsibilities.	**CIO reports to agency head (or deputy/COO).** As required by the Clinger Cohen Act, and left in place by FITARA, the CIO "shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter."

However, FITARA did not clarify important distinctions among C-Suite roles for technology in government such as CIO, Chief Technology Officer, Chief Innovation Officer, and Chief Data Officer. The former senior executive at OMB and current Executive Director of the IBM Center for The Business of Government, Daniel Chenok, described FITARA as "solidifying the CIO's role of strategic leadership over IT. But the role should integrate all information and IT resources in a strategic framework that supports the agency's mission, which is an important distinction."

In addition, FITARA does not address program ownership within an agency. That is, the CIO has authority to prioritize IT projects within an agency, including their funding. But the business owner of the program or an Assistant Secretary responsible for the policy or programmatic purpose of the program, for example, no longer oversees the program even though they have the expertise.

Privacy Act of 1974

Throughout the evolution of the CIO role, some responsibilities have remained the same across the decades. Notably, two long-standing statutes articulate CIO responsibilities over the privacy and public availability of information. First, The Privacy Act of 1974 established rules about how personally identifiable information can be collected, stored, used, and maintained in systems of records by federal government agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by a piece of information assigned to that individual. The law prohibits the disclosure of an individual record from a system of records without the explicit consent of the individual.[13]

The Freedom of Information Act of 1946

Second, The Freedom of Information Act of 1946 sets forth rules for making government information available to the public. Congress has amended the original law multiple times since its original passage. Notably, the Electronic Freedom of Information Act Amendments of 1996 stated that certain types of records be available electronically. Federal agencies are required to disclose any information requested under FOIA unless it meets one of the nine exemptions granted under the law such as national security or personal privacy. In addition, President Clinton issued executive orders that allowed previously classified national security documents to be covered under FOIA if they were older than 25 years and of historical interest.

Conclusion

Overall, the federal and agency CIO roles have evolved significantly in the past 20 years. Statutes, regulations, and policy guidance have added new responsibilities and clarify existing duties to create a more empowered executive roles responsible for all IT

[13] https://www.justice.gov/opcl/privacy-act-1974

investments in an agency and across government. Although policymakers have enacted important changes to the CIO role, they can do more to expand the authorities and responsibilities in the future. This paper will conclude with a summary of recommendations that experts have made to improve the CIO role going forward:

- Federal CIO
    - Centralize control of all infrastructure, applications, contracts, and enterprise licenses under one federal CIO position
    - Integrate the four primary statutes governing the role of the CIO into one framing statute that mirrors the structure OMB uses for its overarching information technology guidelines to all agencies – OMB Circular A-130

- Agency CIO
    - Elevate the agency CIO role to be the strategic leader over all information resources including data and not only information technology
    - Change the CIO political leader position at each agency to integrate all information resources and manage deputy CIOs with specific responsibilities for certain functions such as IT, cyber, information policy
    - Move the entire agency's IT budget under the agency CIO's decision making authority
    - Clarify program ownership of IT programs so that the agency executive with mission responsibilities
    - Address the downsides of the centralized acquisition of all technology resources through the agency CIO

Glossary of Terms

Adequate Incremental Development - for development of software or services, planned and actual delivery of new or modified technical functionality to users occurs at least every six months.

Agency - includes any department, independent establishment, commission, administration, authority, board or bureau of the United States or any corporation in which the United States has a proprietary interest, unless the context shows that such term was intended to be used in a more limited sense.

Agency CIO - the Chief Information Officer at the headquarters level of a department or establishment of the government as defined in Section 20 of OMB Circular A-11 (contrast with 'bureau CIO').

Agency Head - the secretary or deputy secretary of a cabinet-level department such as the Department of Transportation; the administrator or deputy administrator of an agency such as the Environmental Protection Agency

Assistant Secretary – an executive official with sub-cabinet rank at a department.

Bureau CIO - official with the title or role of Chief Information Officer within a principal subordinate organizational unit of the agency, as defined in Section 20 of OMB Circular A-11, or any component organization of the agency (contrast with 'agency CIO').

Career Civil Servant – any agency employee hired on the basis of merit and competence. These employees are not linked to a particular presidential administration and can serve beyond changes in political leadership.

Contract - a mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include (but are not limited to) awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modifications. Contracts do not include grants and cooperative agreements covered by 31 U.S.C. § 6301, et seq.

Covered Agency – a department or agency subject to federal statutes governing the agency CIO roles. The Department of Defense is exempt from this list. A Covered Agency also matches the list of agencies required to have a Chief Financial Officer position, as prescribed by The Chief Financial Officers Act of 1990.

Chief Acquisition Officer (CAO) – the senior procurement executive responsible for all procurement processes at a department or agency.

Chief Financial Officer (CFO) – the senior financial executive responsible for all financial management at a department or agency. The Chief Financial Officers Act of 1990 established the political appointee position at 24 departments or agencies. The Clinger Cohen Act established CIOs at the same 24 departments or agencies.

Chief Human Capital Officer (CHCO) – the senior executive position responsible for human resources policies, workforce development and training programs, and organizational culture. The Chief Human Capital Officers Act of 2002 established the position at 24 departments or agencies.

Chief Information Officer (CIO) – the senior executive position responsible for information technology and technology investments in an agency. The Clinger Cohen Act of 1996 established the position at 24 departments or agencies.

Clinger – Cohen Act of 1996 (CCA) – a federal law intended to guide how the government acquires, uses, and disposes of information technology. The statute created the Chief Information Officer position at 24 departments or agencies, which matches the Chief Financial Officers Act of 1990.

Circular A-130 – the official guidance document for all federal information technology assets and data issued by the Office of Management and Budget. First issued in 1985 to implement sections of The Paperwork Reduction Act of 1980, the document has been revised several times in the past 30 years. The circular is the most comprehensive guidance document about technology. It requires all agencies to put into place and maintain emergency response capabilities, security awareness training to all government users of technology, and security plans for all federal information systems.

Department – the cabinet-level agency headed by a cabinet secretary such as the Department of State.

Deputy Secretary – the chief operating officer or second-in-command of a department; position reports to a cabinet secretary.

The E-Government Act of 2002 – a federal law to improve the management of electronic government services. It established a position similar to the federal Chief Information Officer and a new Office of E-Government and Information Technology within the president's Office of Management and Budget.

Federal Chief Information Officer – the executive position at OMB filled by a political appointee. The role is responsible for coordinating all information technology policies and investments across government agencies. The E-Government Act of 2002 established a position named Administrator, which is practically called the federal CIO at OMB as of 2009.

Federal Information Security Management Act section of The E-Government Act of 2002 (FISMA) – a federal law that brought cybersecurity to the government's attention.

The statutes requires each federal agency to develop, document, and implement a program to provide information security for all information assets and data that are managed by the agency directly or provided by a contractor to the agency.

Federal Information Security Modernization Act of 2014 – a federal law that updates the original FISMA statute enacted in 2002. The law gave the Department of Homeland Security the authority to assist the Office of Management and Budget (OMB) in ensuring information security throughout government agencies. The statute also changed the type of reporting that agencies submit to OMB from process updates to data about risks and threats to federal IT assets.

Federal Information Technology Acquisition Reform Act of 2014 (FITARA) – a section of the National Defense Authorization Act of 2015 that increased the authority and responsibilities of agency Chief Information Officers (CIOs). After enactment, CIOs now had the authority to approve all budget and acquisition requests for any technology investment in an agency.

Freedom of Information Act of 1946 and 1995 (FOIA) – a federal law that permits the full or partial disclosure of information and documents controlled by the federal government. The original statute has been updated multiple times. The law specifies which agency records are subject to disclosure and grants exemption requirements.

General Services Agency (GSA) – federal agency responsible for support services such as travel, real estate, and acquisition provided to other agencies.

Government Accountability Office (GAO) – a federal agency that conducts research studies, program evaluations, and investigations for Congress.

Government Performance and Results Act of 1993 (GPRA) – a federal law intended to improve the performance of government organizations. The statute requires agencies to set goals, measure results, and report progress to OMB, Congress, and the public.

GPRA Modernization Act of 2010 (GPRA Modernization) – a federal law that updated GPRA by refining strategic planning and performance management frameworks.

Information Resources Management (IRM) - process of managing information resources to accomplish mission and improve performance of the organization.

Information Technology - any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where such services or equipment are 'used by an agency' if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product. The term "information technology" includes

computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

IT Resources - all agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of information technology; acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but does not include grants to third parties which establish or support information technology not operated directly by the Federal Government.

Major IT Investment - an IT investment requiring special management attention because of its importance to the mission or function to the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; unusual funding mechanism; or definition as major by the agency's capital planning and investment control process. Agencies should also include all "major automated information system" as defined in 10 U.S.C. 2445 and all "major acquisitions" as defined in the OMB Circular A-11 Capital Programming Guide consisting of information resources. OMB may work with the agency to declare IT investments as major IT investments. Agencies must consult with assigned OMB desk officers and resource management offices (RMOs) regarding which investments are considered "major." Investments not considered "major" are "non-major."

Office of Information and Regulatory Affairs (OIRA) – the office is the central authority of all regulations, information collection under The Paperwork Reduction Act, statistical practices, and coordination of privacy policy for the entire federal government. The Paperwork Reduction Act of 1980 established OIRA as part of the Office of Management and Budget within the Executive Office of the President.

Office of Management and Budget (OMB) – the office within the White House Executive Office of the President that oversees all federal government operations and implementing the President's agenda government-wide. OMB is responsible for carrying out the president's vision by creating the president's budget proposals, aligning regulations, and monitoring and measuring agency programs. OMB staff includes political appointees and career civil servants.

The Paperwork Reduction Act of 1995 (PRA) – a federal law enacted in 1980 and updated substantially in 1995 designed to reduce the total burden of paperwork the federal government imposes on private businesses and citizens. The statute established the Office of Information and Regulatory Affairs (OIRA) within the Office of Management

and Budget. OIRA became responsible for coordinating the collection of information from the public across all agencies.

Political Appointee – any agency employee appointed by the president, vice president, or agency head. These employees typically serve during a particular presidential administration and not beyond.

The Privacy Act of 1974 – a federal law that regulates the collection, use, and dissemination of personally identified information about individuals that is stored in systems of records by federal agencies. An agency controls a system of records from which data are retrieved by the name of the individual or another individual identifier.

Privacy Impact Assessment (PIA) – the E-Government Act of 2002 required agencies to evaluate privacy protections for all information technology systems that contain any personally identifiable information.

Program Associate Director (PAD) – the position filled by political appointees within the Office of Management and Budget who oversees the budget and programs within a particular resource area such as health care. OMB employs a total of five PAD positions.

Reprogramming - any movement of funds for IT resources that requires Congressional notification.

Secretary – a member of the President's cabinet who leads a cabinet-level department such as the Department of Treasury.