The Current State of Federal Information Technology Acquisition Reform and Management

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

Updated February 3, 2020

Congressional Research Service
7-....
www.crs.gov
R44843

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The Government Accountability Office (GAO) has reported that the federal government budgets more than $90 billion each year on information technology (IT) investments. Historically, the projects supported by these investments have often incurred "multi-million dollar cost overruns and years-long schedule delays." In addition, GAO has reported that these projects may contribute little to mission-related outcomes and, in some cases, may fail altogether. These undesirable results, according to GAO, "can be traced to a lack of disciplined and effective management and inadequate executive-level oversight."

The Federal Information Technology Acquisition Reform Act (FITARA) was enacted on December 19, 2014, to establish a long-term framework through which federal IT investments could be tracked, assessed, and managed, to significantly reduce wasteful spending and improve project outcomes. These requirements of FITARA are carried out by the Federal Chief Information Officer (CIO). The position of the Federal CIO was created by the E-Government Act of 2002 as the "Administrator, Office of Electronic Government."

Congress and GAO have actively monitored the activities of the Federal CIO and the initiatives carried out by the office. Both have been especially attentive to the topics of data center use and cloud deployment as they relate to achieving the goals of FITARA. As of November 2019, GAO reported that federal agencies had fully implemented 61% of the 1,320 IT management-related recommendations that GAO has made to them since FY2010. Likewise, agencies had implemented 76% of the 3,323 security-related recommendations that GAO has made since FY2010.

The House Committee on Oversight and Reform has held two hearings on FITARA in the 116th Congress (June 26, 2019, and December 11, 2019). No legislation that would impact FITARA implementation has been introduced.

Contents

Introduction 1
FITARA Overview 1
Applicability of FITARA 3
FITARA Implementation 3
Modernizing Government Technology (MGT) Act 4
Oversight of Federal CIO Initiatives 4
Congressional Oversight, 116th Congress 4
Government Accountability Office Reports and Testimony, 2019 4
Recent Activity: FITARA Scorecard 9.0 6
CIO Responsibilities 6
CIO IT Acquisition Review 7
Consolidating Data Centers 8
Managing Software Licenses 8
Ensuring the Nation's Cybersecurity 8

Figures

Figure 1. Practices that Selected Agencies Used to Effectively Implement Key Provisions of FITARA 5
Figure 2. FITARA 9.0 Scorecard, December 2019 6

Contacts

Author Contact Information 8

Introduction

The federal government spends about $90 billion each year on information technology (IT) investments.[1] The Government Accountability Office (GAO) has found that, historically, the projects supported by these investments have often incurred "multi-million dollar cost overruns and years-long schedule delays." In addition, they may contribute little to mission-related outcomes and, in some cases, may fail altogether.[2] These undesirable results, according to GAO, "can be traced to a lack of disciplined and effective management and inadequate executive-level oversight."[3] The Federal Information Technology Acquisition Reform Act (FITARA) was enacted on December 19, 2014,[4] to address these issues[5] and codify existing initiatives managed by the Federal Chief Information Officer (CIO).[6]

FITARA Overview

FITARA outlined seven areas of reform that affect how federal agencies purchase and manage their information technology (IT) assets, including

[1] Testimony of Carol C. Harris, Director, Information Technology Acquisition Management Issues, before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, *Agencies and OMB Need to Continue Implementing Recommendations on Acquisitions, Operations, and Cybersecurity*, House of Representatives, December 11, 2019, https://oversight.house.gov/sites/democrats.oversight.house.gov/files/Harris%20Testimony.pdf.

[2] For example, the Department of Defense (DOD) canceled its Expeditionary Combat Support System in December 2012 after it had spent more than a billion dollars, but had not deployed the system within five years of initially obligating funds; the Department of Homeland Security's (DHS) Secure Border Initiative Network program was canceled in January 2011 after DHS had spent more than $1 billion because the program did not meet cost-effectiveness and viability standards; the Department of Veterans Affairs' (VA) Financial and Logistics Integrated Technology Enterprise program, which was intended to be delivered by 2014 at a total estimated cost of $609 million, was terminated in October 2011 due to challenges in managing the program; the Farm Service Agency's Modernize and Innovate the Delivery of Agricultural Systems program, which was to replace aging hardware and software applications that process benefits to farmers, was canceled after 10 years at a cost of at least $423 million, while delivering only about 20% of the functionality that was originally planned; and the Office of Personnel Management's Retirement System Modernization program was canceled in February 2011 after the agency had spent approximately $231 million on its third attempt to automate the processing of federal employee retirement claims. U.S. Government Accountability Office, *Additional Actions and Oversight Urgently Needed*, GAO-15-675T, June 10, 2015 (hereinafter *Additional Actions and Oversight Urgently Needed*, GAO).

[3] *Additional Actions and Oversight Urgently Needed*, GAO.

[4] Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, P.L. 113-291.

[5] Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, P.L. 113-291. See also H.Rept. 113-359. Not all federal agencies are subject to the requirements of FITARA. Generally, agencies identified in the Chief Financial Officers (CFO) Act of 1990, as well as their subordinate divisions and offices, are subject to the requirements of FITARA. The DOD, the intelligence community, and portions of other agencies that operate systems related to national security are subject to only certain portions of FITARA. Additionally, executive branch agencies not named in the CFO Act are encouraged, but not required, to follow FITARA guidelines.

[6] The position of the Federal CIO and the CIO Council were created within the Office of Management and Budget (OMB) by the E-Government Act of 2002. The role of the Federal CIO is to provide leadership and direction to the executive branch on IT implementation throughout the federal government. Specific responsibilities include directing the activities of the CIO Council, advising the Director of OMB on the performance of IT investments; and overseeing specific IT reform initiatives and activities. The CIO Council is the principal interagency forum on federal agency practices for IT management. Originally established by Executive Order 13011 (Federal Information Technology) and later codified by the E-Government Act of 2002, the CIO Council's mission is to help improve practices related to the design, acquisition, development, modernization, use, sharing, and performance of federal government information resources. CIO.gov is the website of the U.S. Chief Information Officer and the Federal CIO Council.

- enhancing the authority of agency CIOs;
- improving transparency and risk management of IT investments;
- setting forth a process for agency IT portfolio review;
- refocusing the Federal Data Center Consolidation Initiative (FDCCI) from only consolidation to optimization;
- expanding the training and use of "IT Cadres," as initially outlined in the "25 Point Implementation Plan to Reform Federal Information Management Technology";[7]
- maximizing the benefits of the Federal Strategic Sourcing Initiative (FSSI);[8] and
- creating a government-wide software purchasing program, in conjunction with the General Services Administration.

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

- refocus the Federal Data Center Consolidation Initiative (FDCCI) from consolidation to optimization, to include adoption of cloud services;[9]
- set forth a process for agency IT portfolio review and oversight;
- improve transparency and risk management of IT investments;
- identify and publish cost savings and optimization improvements;
- provide public updates on cumulative cost savings and optimization improvements; and
- review agencies' data center inventories and management strategies.

FITARA requires federal agencies to submit annual reports that include

- comprehensive data center inventories,
- multiyear strategies to consolidate and optimize data centers,
- performance metrics and a time line for agency action, and
- yearly calculations of investment and cost savings related to FITARA implementation.

[7] The "25-Point Implementation Plan to Reform Federal IT Management" was one of the original policy documents developed as part of a comprehensive effort to increase the operational efficiency of federal technology assets. "A 25-Point Implementation Plan to Reform Federal IT Management," Office of the U.S. Chief Information Officer, December 9, 2010, https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf.

[8] Strategic sourcing is "a method of managing procurement processes for an organization in which the procedures, methods, and sources are constantly re-evaluated to optimize value to the organization. Strategic sourcing, which is considered a key aspect of supply chain management, involves elements such as examination of purchasing budgets, the landscape of the supply market, negotiation with suppliers, and periodic assessments of supply transactions." BusinessDictionary.com, http://www.businessdictionary.com/definition/strategic-sourcing.html.

[9] For additional background on the FDCCI, see the "25-Point Implementation Plan to Reform Federal IT Management." This plan was one of the original policy documents developed as part of a comprehensive effort to increase the operational efficiency of federal technology assets. Office of the U.S. Chief Information Officer, "A 25-Point Implementation Plan to Reform Federal IT Management," December 9, 2010, https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf.

Applicability of FITARA

Generally, agencies identified in the Chief Financial Officers (CFO) Act of 1990,[10] as well as their subordinate divisions and offices, are subject to the requirements of FITARA. The DOD, the intelligence community, and portions of other agencies that operate systems related to national security are subject to only certain portions of FITARA. Additionally, executive branch agencies not named in the CFO Act are encouraged, but not required, to follow FITARA guidelines.

FITARA Implementation

On June 10, 2015, OMB published guidance[11] to implement the requirements of FITARA and harmonize existing policy and guidance[12] with the new law. Among other goals, the requirements are intended to

- assist agencies in establishing management practices that align IT resources with agency missions, goals, programmatic priorities, and statutory requirements;
- establish government-wide IT management controls that will meet FITARA requirements while providing agencies with the flexibility to adapt to agency processes and unique mission requirements;
- establish universal roles, responsibilities, and authorities of the agency CIO and other senior agency officials;[13]
- strengthen the agency CIO's accountability for the agency's IT costs, schedules, performance, and security;
- strengthen the relationship between agency and bureau CIOs;
- establish consistent government-wide interpretation of FITARA terms and requirements; and
- provide appropriate visibility and involvement of the agency CIO in the management and oversight of IT resources to support the implementation of effective cybersecurity policies.[14]

In addition to implementing FITARA, the guidance also harmonized the requirements of FITARA with existing law, primarily the Clinger-Cohen Act of 1996 and the E-Government Act of 2002.[15] Those laws require OMB to issue management guidance for information technology and

[10] P.L. 101-576.

[11] U.S. Office of Management and Budget, *Management and Oversight of Federal Information Technology*, OMB-M-15-14, June 10, 2015, https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf (hereinafter "Management and Oversight of Federal Information Technology").

[12] In addition to implementing FITARA, OMB Memorandum M-15-14, "Management and Oversight of Federal Information Technology" also harmonizes the requirements of FITARA with existing law, primarily the Clinger-Cohen Act of 1996 and the E-Government Act of 2002. Those laws require OMB to issue management guidance for information technology and electronic government activities across the government, respectively. FITARA also contains provisions that required OMB interpretation before implementation.

[13] Senior Agency Officials, as referred to in OMB M-15-14, include positions, for example, chief financial officer, chief administrative officer, chief operating officer, and program manager.

[14] "Management and Oversight of Federal Information Technology" (OMB-M-15-14), OMB.

[15] P.L. 104-106 (40 U.S.C. 1401 et seq.) and P.L. 107-347 (43 U.S.C. 1601 et seq.), respectively. For information on federal acquisition generally, see CRS Report R42826, *The Federal Acquisition Regulation (FAR): Answers to Frequently Asked Questions*, coordinated by Erika K. Lunder.

electronic government activities across the government, respectively. FITARA also contains provisions that required OMB interpretation before implementation.

Modernizing Government Technology (MGT) Act

In December 2017, Congress enacted the Modernizing Government Technology (MGT) Act, which authorized agencies to set up IT-specific working capital funds. Thus far, only three agencies have taken the steps necessary to set up their fund, while five additional agencies have plans to set up an MGT working capital fund by the end of FY2020. The working capital funds authorized under the MGT Act allow agencies to fund IT modernization and reinvest savings for additional modernization projects. One reason given for this low adoption rate is that the law did not provide agencies the authority to transfer money into their working capital funds. Additional legislative actions to provide agencies with this authority may be needed.

The MGT Act also established a centralized Technology Modernization Fund (TMF) to fund large IT modernization projects. The MGT Act originally authorized $500 million for the TMF, but the fund has only received $125 million over the past two fiscal years, limiting the effectiveness of the TMF. While the Financial Services and General Government Fiscal Year 2020 Appropriation Act under consideration in the House would provide an additional $35 million for the fund, some believe more funding is needed to address the long list of agency IT modernization needs.

Oversight of Federal CIO Initiatives

Through hearings and GAO investigations, Congress has been active in monitoring the activities of the Federal CIO and the initiatives carried out by the office. Congress has been especially attentive to the topics of data center use and cloud adoption as they relate to achieving the goals of FITARA.

Congressional Oversight, 116th Congress

The 116th Congress has thus far not introduced any legislation directly related to FITARA. The House Committee on Oversight and Reform Subcommittee on Government Operations has held two hearings, "The Federal Information Technology Reform Act Scorecard 8.0,"[16] on June 26, 2019, and "The Federal Information Technology Reform Act Scorecard 9.0," on December 11, 2019.[17]

Government Accountability Office Reports and Testimony, 2019

The GAO has conducted numerous investigations into the initiatives being carried out under the auspices of the U.S. CIO. Most recently, GAO published testimony provided before the December 11, 2019, House Committee on Oversight and Reform Subcommittee on Government Operations, "Agencies and OMB Need to Continue Implementing Recommendations on Acquisitions, Operations, and Cybersecurity" (GAO-19-641T).[18]

Additionally, on April 29, 2019, GAO published, "Effective Practices Have Improved Agencies' FITARA Implementation (GAO-20-311T). In that report, GAO reviewed nine agencies and found 12 practices officials said helped them to effectively implement one or more of the FITARA

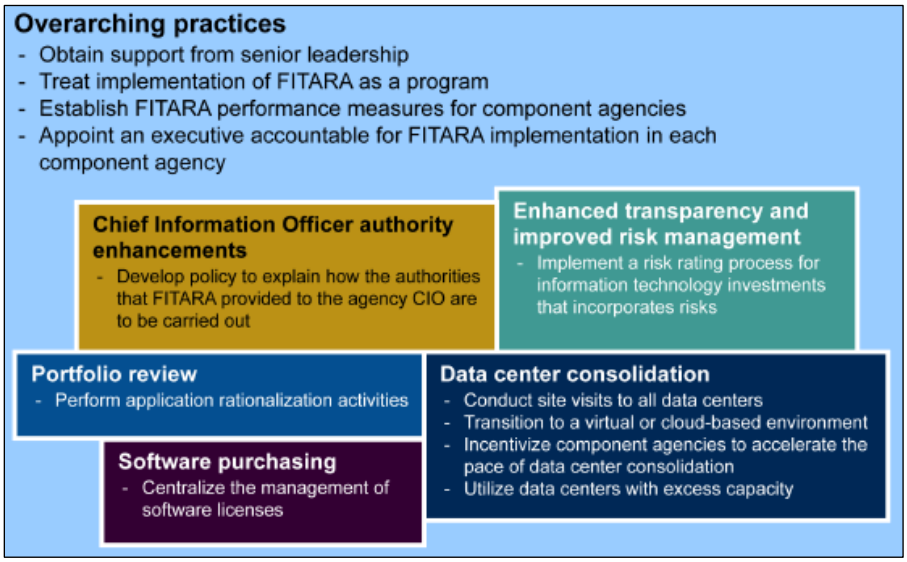
[16] https://oversight.house.gov/legislation/hearings/fitara-80.

[17] https://oversight.house.gov/legislation/hearings/fitara-90.

[18] https://www.gao.gov/products/GAO-20-311T.

provisions (**Figure 1**). For example, five of the agencies said that centralizing the management of software licenses was essential to meeting the software purchasing provision of the law. By doing so, agencies were able to make agency-wide purchasing decisions that saved them money.

Figure 1. Practices that Selected Agencies Used to Effectively Implement Key Provisions of FITARA



Source: "Effective Practices Have Improved Agencies' FITARA Implementation (GAO-19-131), April 29, 2019, https://www.gao.gov/products/GAO-19-131.

GAO also published reports on cloud adoption and data center optimization. In "Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked" (GAO-19-58), published April 4, 2019,[19] GAO noted that, each year, federal agencies spend $90 billion on IT. The agency found, though, that agencies don't consistently track cloud-related savings, making it hard for them to make informed decisions on whether to use cloud services. GAO recommended that agencies improve their savings tracking. In "Data Center Optimization: Additional Agency Actions Needed to Meet OMB Goals" (GAO-19-241), published April 11, 2019,[20] GAO noted that federal agencies that since 2010 have been required to close unneeded data center facilities and improve the performance of remaining facilities. Across the government, agencies have closed 6,250 centers to date and saved $2.7 billion. However, GAO stated that only two agencies in its review planned to meet September 2018 government-wide optimization goals that include, for example, a target for how much time data servers sit unused.

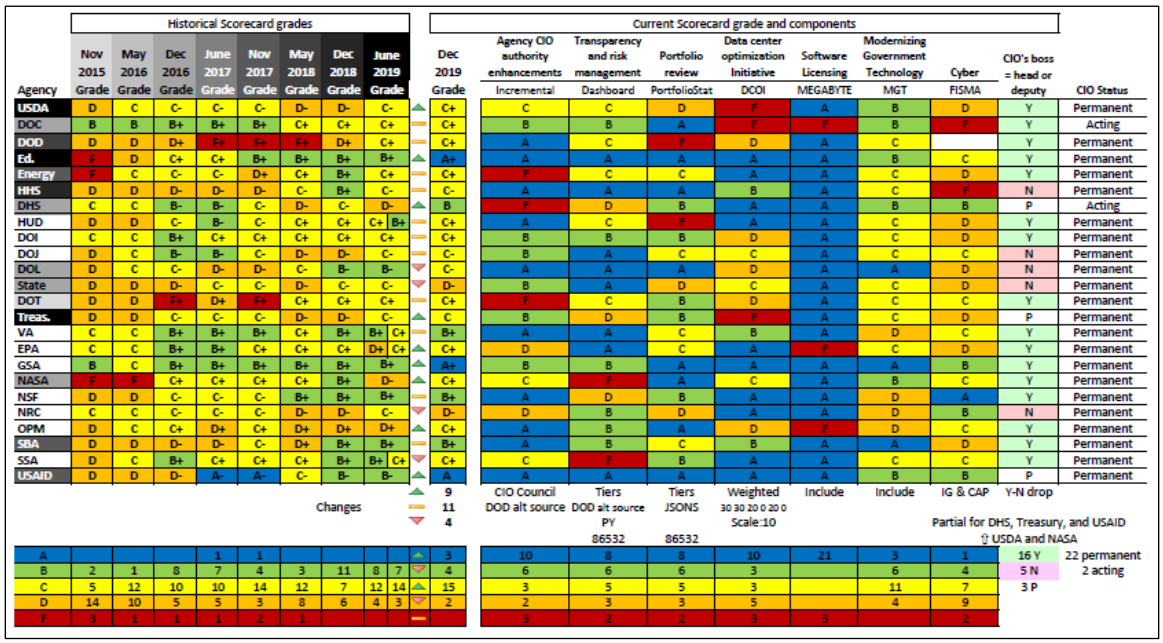
[19] https://www.gao.gov/products/GAO-19-58.

[20] https://www.gao.gov/products/GAO-19-241.

Recent Activity: FITARA Scorecard 9.0

The "FITARA Scorecard 9.0"[21] was issued at a December 11, 2019, hearing of the Committee on Oversight and Reform Subcommittee on Government Operations, "The Federal Information Technology Reform Act Scorecard 9.0,"[22] (**Figure 2**).

Figure 2. FITARA 9.0 Scorecard, December 2019



	Historical Scorecard grades									Current Scorecard grade and components								
Agency	Nov 2015 Grade	May 2016 Grade	Dec 2016 Grade	June 2017 Grade	Nov 2017 Grade	May 2018 Grade	Dec 2018 Grade	June 2019 Grade	Dec 2019 Grade	Agency CIO authority enhancements Incremental	Transparency and risk management Dashboard	Portfolio review PortfolioStat	Data center optimization Initiative DCOI	Software Licensing MEGABYTE	Modernizing Government Technology MGT	Cyber FISMA	CIO's boss = head or deputy	CIO Status
USDA	D	C	C-	C-	C-	D-	D-	C-	C+	C	C	D	F	A	B	D	Y	Permanent
DOC	B	B	B+	B+	B+	C+	C+	C+	C+	B	B	A	F	F	B	F	Y	Acting
DOD	D	D	D+	F+	F+	F+	D+	C+	C+	A	C	F	D	A	C		Y	Permanent
Ed.	F	D	C+	C+	B+	B+	B+	B+	A+	A	A	A	A	A	B	C	Y	Permanent
Energy	F	C	C-	C-	D+	C+	B+	C+	C+	F	C	C	A	A	C	D	Y	Permanent
HHS	D	D	D-	D-	D-	C-	B+	C-	C-	A	A	A	B	A	C	F	N	Permanent
DHS	C	C	B-	B-	C-	D-	C-	D-	B	F	D	B	A	A	B	B	P	Acting
HUD	D	D	C-	B-	C-	C+	C+	C+ B+	C+	A	C	F	A	A	C	D	Y	Permanent
DOI	C	C	B+	C+	C+	C+	C+	C+	C+	B	B	B	D	A	C	D	Y	Permanent
DOJ	D	C	B-	B-	C-	D-	D-	C-	C-	B	A	C	C	A	C	C	N	Permanent
DOL	D	C	C-	D-	D-	C-	B-	B-	C-	A	A	A	D	A	A	D	N	Permanent
State	D	D	D-	C-	C-	D-	C-	C-	D-	B	A	D	C	A	C	D	N	Permanent
DOT	D	D	F+	D+	F+	C+	C+	C+	C+	F	C	B	D	A	C	C	Y	Permanent
Treas.	D	D	C-	C-	C-	D-	D-	C-	C	B	D	B	F	A	C	D	P	Permanent
VA	C	C	B+	B+	B+	C+	B+	B+ C+	B+	A	A	C	B	A	D	C	Y	Permanent
EPA	C	C	B+	B+	C+	C+	C+	D+ C+	C+	D	A	C	A	F	C	D	Y	Permanent
GSA	B	C	B+	B+	B+	B+	B+	B+	A+	B	B	A	A	A	A	B	Y	Permanent
NASA	F	F	C+	C+	C+	C+	B+	D-	C+	C	F	A	C	A	B	C	Y	Permanent
NSF	D	D	C-	C-	C-	B+	B+	B+	B+	A	D	B	A	A	D	A	Y	Permanent
NRC	C	C	C-	C-	C-	D-	D-	C-	D-	D	B	D	A	A	D	B	N	Permanent
OPM	D	C	C+	D+	C+	D+	D+	D+	C+	A	B	A	D	F	D	C	Y	Permanent
SBA	D	D	D-	D-	C-	D+	B+	B+	B+	A	B	C	B	A	A	D	Y	Permanent
SSA	D	C	B+	C+	C+	C+	B+	B+ C+	C+	C	F	B	A	A	C	C	Y	Permanent
USAID	D	D	D-	A-	A-	C-	B-	B-	A	A	A	A	A	A	B	B	P	Permanent
									9	CIO Council	Tiers	Tiers	Weighted	Include	Include	IG & CAP	Y-N drop	
								Changes	11	DOD alt source	DOD alt source	JSONS	30 30 20 0 20 0					
									4		PY		Scale:10					
											86532	86532					Partial for DHS, Treasury, and USAID	
																	⇧ USDA and NASA	
A				1	1				3	10	8	8	10	21	3	1	16 Y	22 permanent
B	2	1	8	7	4	3	11	8 7	4	6	6	6	3		6	4	5 N	2 acting
C	5	12	10	10	14	12	7	12 14	15	3	5	5	3		11	7	3 P	
D	14	10	5	5	3	8	6	4 3	2	2	3	3	5		4	9		
F	3	1	1	1	2	1			2	3	2	2	3	3		2		

Source: U.S. House of Representatives, Committee on Oversight and Reform, available at https://oversight.house.gov/sites/democrats.oversight.house.gov/files/12.11.19_FITARA%20Scorecard%209.0.pdf.

At the hearing, Carol Harris, Director of Information Technology Management Issues at GAO, cited five areas where significant actions remain to be completed: CIO responsibilities, CIO IT acquisition review, consolidating data centers, managing software licenses, and ensuring the nation's cybersecurity.

CIO Responsibilities

Laws such as FITARA and related guidance assigned 35 key IT management responsibilities to CIOs to help address longstanding challenges. In August 2018, GAO reported that none of the 24 selected agencies had established policies that fully addressed the role of their CIO. GAO recommended that OMB and each of the 24 agencies take actions to improve the effectiveness of CIOs' implementation of their responsibilities. Although most agencies agreed or did not comment, none of the 27 recommendations have yet been implemented.

[21] https://oversight.house.gov/sites/democrats.oversight.house.gov/files/Scorecard%208.0.pdf.

[22] https://oversight.house.gov/legislation/hearings/fitara-80.

CIO IT Acquisition Review

According to FITARA, covered agencies' CIOs are required to review and approve IT contracts. However, in January 2018, GAO reported that most of the CIOs at 22 covered agencies were not

adequately involved in reviewing billions of dollars of IT acquisitions. Consequently, GAO made 39 recommendations to improve CIO oversight for these acquisitions. Since then, 23 of the recommendations had not been implemented.

Consolidating Data Centers

OMB launched an initiative in 2010 to reduce the number of data centers. In August 2018, 22 agencies reported that they had achieved $1.94 billion in cost savings for fiscal years 2016 through 2018, while 2 agencies reported that they had not achieved any savings. GAO has made 196 recommendations to OMB and agencies to improve the reporting of related cost savings and to achieve optimization targets. As of November 2019, 121 of the recommendations have been implemented.

Managing Software Licenses

Effective management of software licenses can help avoid purchasing too many licenses that result in unused software. In May 2014, GAO reported that better management of licenses was needed to achieve savings, and made 135 recommendations to improve such management. As of November 2019, all but 19 of the recommendations had been implemented.

Ensuring the Nation's Cybersecurity

GAO has consistently identified shortcomings in the federal government's approach to cybersecurity and made 3,323 recommendations to agencies since 2010. These recommendations have identified actions for agencies to take to fully implement their information security programs and strengthen technical security controls over their computer networks and systems. As of November 2019, 76% of the recommendations had been implemented.

Author Contact Information

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy
/redacted/@crs.loc.gov,7-....