United States Government Accountability Office

Testimony

Before the Subcommittee on Government Operations, Committee on Oversight and Reform, House of Representatives

For Release on Delivery
Expected at 9:00 a.m. ET
Thursday, July 28, 2022

INFORMATION TECHNOLOGY AND CYBERSECURITY

Using Scorecards to Monitor Agencies' Implementation of Statutory Requirements

Statement of Carol C. Harris, Director, Information Technology and Cybersecurity

GAO-22-106105

July 28, 2022

INFORMATION TECHNOLOGY AND CYBERSECURITY

Using Scorecards to Monitor Agencies' Implementation of Statutory Requirements

GAO Highlights

Highlights of GAO-22-106105, a testimony before the Subcommittee on Government Operations, Committee on Oversight and Reform, House of Representatives

Why GAO Did This Study

Congress has long recognized that IT systems provide essential services critical to the health, economy, and defense of the nation. In support of these systems, the federal government annually spends more than $100 billion on IT and cyber-related investments.

However, many of these investments have suffered from ineffective management. Further, recent high profile cyber incidents have demonstrated the urgency of addressing cybersecurity weaknesses.

To improve the management of IT, Congress and the President enacted FITARA in December 2014. FITARA applies to the 24 agencies subject to the Chief Financial Officers Act of 1990, although with limited applicability to the Department of Defense.

GAO was asked to provide an overview of the scorecards released by this Subcommittee. The scorecards have been used for oversight of agencies' efforts to implement statutory provisions and other IT-related topics. For this testimony, GAO relied on its previously issued products.

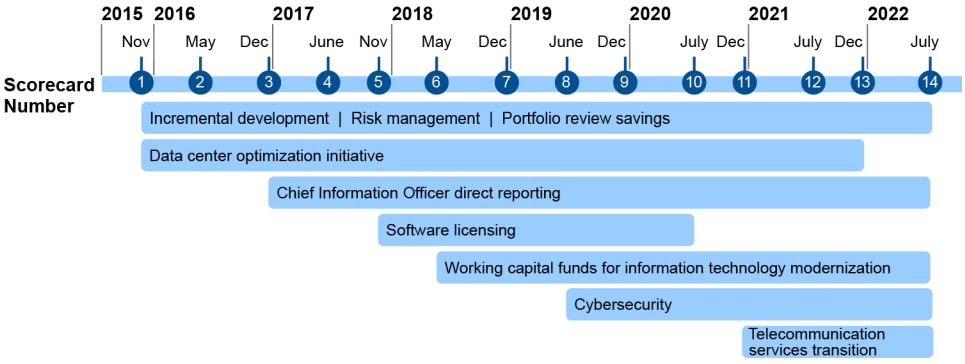
Since 2010, GAO has made approximately 5,300 recommendations to improve IT management and cybersecurity. As of June 2022, federal agencies have fully implemented about 77 percent of these. However, many critical recommendations have not been implemented—nearly 300 on IT management and more than 600 on cybersecurity.

View GAO-22-106105. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

Since November 2015, this Subcommittee has issued scorecards as an oversight tool to monitor agencies' progress in implementing various statutory IT provisions and addressing other key IT issues. The selected provisions are from laws such as the Federal Information Technology Acquisition Reform Act (commonly referred to as FITARA), Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016, the Modernizing Government Technology Act, and the Federal Information Security Modernization Act of 2014. The scorecards have assigned each covered agency a letter grade (i.e., A, B, C, D, or F) based on components derived from statutory requirements and additional IT-related topics. As of July 2022, fourteen scorecards had been released (see figure).

Scorecards Release Timeline with Associated Components



Source: GAO analysis of scorecard documents. | GAO-22-106105

As reflected above, additional important components have been added over time. Initial components were specific to FITARA provisions related to incremental development, risk management, cost savings and data centers. The scorecards then evolved to include additional statutory provisions and related IT topics, such as telecommunications.

The Subcommittee-assigned grades have shown steady improvement and resulted in the scorecards serving as effective oversight tools. For example, during 2020 and 2021, all 24 agencies received A grades for two components (software licensing and data center optimization initiative), resulting in removal of these components from the scorecard. Notwithstanding the improvements made through the use of the scorecard, the federal government's difficulties acquiring, developing, managing, and securing its IT investments remain.

GAO has long recognized the importance of addressing these difficulties by including improving the management of IT acquisitions and operations as well as ensuring the cybersecurity of the nation as areas on its high-risk list. Continued oversight by Congress to hold agencies accountable for implementing statutory provisions and addressing longstanding weaknesses is essential. Implementation of outstanding GAO recommendations can also be instrumental in delivering needed improvements.

Chairman Connolly, Ranking Member Hice, and Members of the Subcommittee:

Thank you for inviting me to discuss the biannual scorecards released by this Subcommittee. Since initial release in November 2015, the scorecards have been an effective oversight tool in monitoring federal agencies' implementation of the Federal Information Technology Acquisition Reform Act (commonly referred to as FITARA) and other IT-related statutory requirements.[1] Congressional oversight continues to be an important part of monitoring agencies' progress in better managing the large investment in IT and cybersecurity that the federal government continues to make.

As you know, the federal government annually spends more than $100 billion on IT and cyber-related investments; however, many of these investments have failed or performed poorly and have often suffered from ineffective management. Additionally, after a series of recent high-profile cyber incidents (e.g., SolarWinds and the Colonial Pipeline hacks), Congress and federal agencies need to move with renewed urgency to take actions that would improve the security of U.S. government IT systems.[2] As we have previously reported, there is more work to do to make these systems secure.[3]

At your request, my remarks provide an overview of the scorecards. This statement is based on previously issued reports and testimonies. More detailed information about our scope and methodology can be found in our reports and testimonies cited throughout this statement.

We conducted the work on which this statement is based in accordance with all sections of GAO's Quality Assurance Framework that are relevant

[1]Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014); Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016, Pub. L. No. 114-210, (2016); the Modernizing Government Technology Act, Pub. L. No. 115-91, (2017); and the Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, (2014).

[2]GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents,* GAO-22-104746 (Washington, D.C.: Jan. 13, 2022) and *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges,* GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

[3]GAO, *Cybersecurity: Preliminary Results Show That Agencies' Implementation of FISMA Requirements Was Inconsistent,* GAO-22-105637 (Washington, D.C.: Jan. 11, 2022).

to our objective. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions.

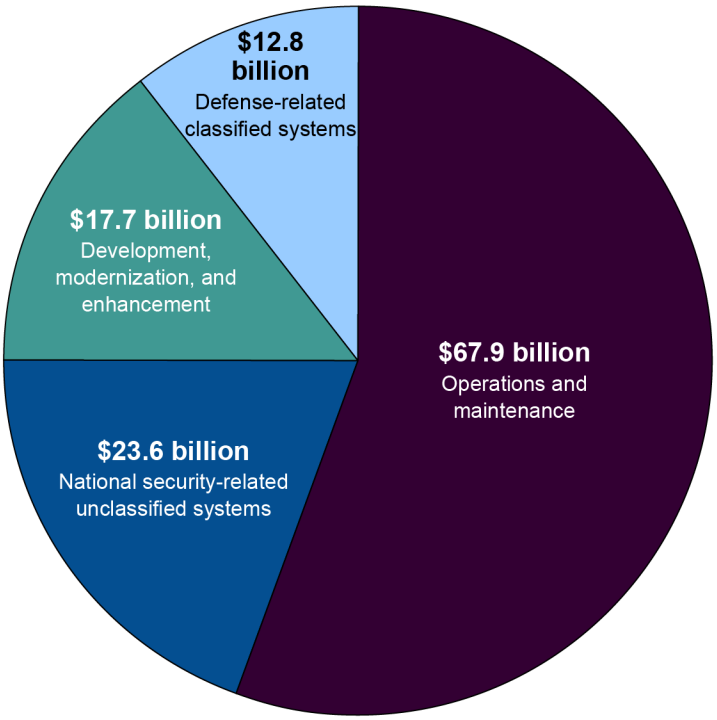
Background

Federal IT systems provide essential services that are critical to the health, economy, and defense of the nation. In fiscal year 2023, the federal government plans to spend approximately $122 billion on IT investments. A large majority of these investments are to support the operation and maintenance of existing IT systems—such as those that support tax filings, Census survey information, and veterans' health records. Additionally, these investments support system development, modernization, and enhancement activities including software upgrades, replacement of legacy IT, and new technologies.

The planned fiscal year 2023 spending also includes costs for defense-related classified systems and national security-related unclassified systems, both of which support cybersecurity activities.[4] Figure 1 summarizes the planned fiscal year 2023 spending for IT investments.

[4]The overall totals of investment categories for defense-related classified systems and national security-related unclassified systems were included in the Department of Defense's IT budget documentation for fiscal year 2023.

Figure 1: Summary of Planned Fiscal Year 2023 Spending on Information Technology Investments, as of June 2022 (Dollars in billions)



Source: GAO analysis of Office of Management and Budget IT Dashboard reported data for fiscal year 2023 and *Department of Defense Information Technology and Cyberspace Activities Budget Overview, Fiscal Year 2023 Budget Request.* | GAO-22-106105

Notwithstanding the billions of dollars spent annually, federal IT investments often suffer from a lack of disciplined and effective management in areas such as project planning, requirements definition, and program oversight. These investments too frequently fail to deliver capabilities in a timely manner, incur cost overruns, and/or experience schedule slippages while contributing little to mission-related outcomes. More than half of the fiscal year 2023 planned spending on IT investments ($122 billion) is dedicated toward the operations and maintenance of existing investments.[5]

[5]The $67.9 billion in total planned spending on operations and maintenance does not include the operations and maintenance spending for national security-related unclassified systems or defense-related classified systems.

Moreover, federal agencies rely on aging legacy systems that can be costly to maintain. We have long stressed the need for federal agencies to update their aging legacy IT systems.[6] These systems often use outdated programming languages, and unsupported hardware and software. In some cases, they may be operating with known security vulnerabilities.

For example, in 2016 we reported that some of the government's IT investments used hardware parts that were unsupported and relied on outdated software languages, such as the common business oriented language (COBOL).[7] In some cases, the lack of vendor support created security vulnerabilities and additional costs because known vulnerabilities were either technically difficult or prohibitively expensive to address.

Compounding these challenges, federal IT systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. The complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising federal systems and networks. Furthermore, federal systems and networks are often interconnected with other internal and external systems and networks, including the internet, thereby increasing risk and the number of avenues of attack.

As previously reported, without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks.[8] For fiscal year 2023, the planned spending on cybersecurity is $17.1 billion.

Given the importance of addressing IT management and cybersecurity weaknesses, we have included improving the management of IT acquisitions and operations as well as ensuring the cybersecurity of the

[6]GAO, *Information Technology: Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems,* GAO-21-524T (Washington, D.C.: Apr. 27, 2021); *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems,* GAO-19-471 (Washington, D.C.: June 11, 2019); and *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, GAO-16-468 (Washington, D.C.: May 25, 2016).

[7]GAO-16-468.

[8]GAO-22-105637.

nation as areas on our high-risk list.[9] In our March 2021 high-risk update, we emphasized the importance of federal agencies taking critical actions to better manage tens of billions of dollars in IT investments.[10]

We also reiterated the urgent need for the federal government to take specific actions to address four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.[11]

Since 2010, GAO has made approximately 5,300 recommendations in these two high-risk areas. As of June 2022, federal agencies had fully implemented about 77 percent of these recommendations; however, many critical recommendations have not been implemented—nearly 300 on IT management and more than 600 on cybersecurity.

[9]GAO designated information security as a high-risk area in 1997 and further expanded the area to include critical infrastructures and protecting the privacy of personally identifiable information in 2003 and 2015, respectively. Additionally, in 2015 improving the management of IT acquisitions and operations was included as a government wide high-risk area. GAO, *High-Risk Series: An Update,* GAO-15-290 (Washington, D.C.: Feb. 11, 2015); High-Risk Series: An Update, GAO-03-119 (Washington, D.C.: January 2003); *High-Risk Series: Information Management and Technology*, HR-97-9 (Washington, D.C.: February 1997); and *High-Risk Series: An Overview*, HR-97-1 (Washington, D.C.: February 1997).

[10]GAO-21-288 and GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[11]The critical actions are: (1) develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace, (2) mitigate global supply chain risks, (3) address cybersecurity workforce management challenges, (4) ensure the security of emerging technologies, (5) improve the implementation of government-wide cyber security initiatives, (6) address weaknesses in federal agency information security programs, (7) enhance the federal response to cyber incidents, (8) strengthen the federal role in protecting the cybersecurity of critical infrastructure, (9) improve federal efforts to protect privacy and sensitive data, and (10) appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Using Scorecards to Monitor Agencies' Implementation of Statutory Requirements

In December 2014, Congress and the President enacted FITARA provisions to improve covered agencies' acquisitions of IT and better enable Congress to monitor agencies' efforts and hold them accountable for reducing duplication and achieving cost savings.[12]

In November 2015, this Subcommittee began issuing scorecards as a tool for conducting oversight of FITARA implementation.[13] The scorecards have assigned each covered agency a letter grade (i.e., A, B, C, D, or F) based on components derived from statutory requirements and additional IT-related topics. Table 1 summarizes the components that have been included on the scorecards.

Table 1: Summary Descriptions of the Scorecard Components

Component	Description
Incremental development	Agency Chief Information Officers (CIO) are to certify that IT investments are adequately implementing incremental development.
Risk management	Agency CIOs are required to categorize their investments by level of risk and disclose these levels on the IT Dashboard.
Portfolio review savings	Agencies are to annually review IT investment portfolios in order to, among other things, increase efficiency and effectiveness and identify potential waste and duplication. Office of Management and Budget (OMB) is required to quarterly report associated cost savings to Congress.
Data center optimization initiative[a]	Agencies are to provide a strategy for consolidating and optimizing their data centers and issue quarterly updates on the progress made.
CIO direct reporting	Agencies are to institutionalize their respective CIO's ability to report directly to the head or deputy of the agency.
Software licensing[a]	Agencies are to establish a comprehensive regularly updated inventory of software licenses and analyze software usage to make cost-effective decisions, among other things.

[12]The provisions apply to the agencies covered by the Chief Financial Officers Act of 1990, 31 U.S.C. § 901(b). These agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development. Although FITARA has generally limited application to the Department of Defense.

[13]Two Subcommittees of the Committee on Oversight and Government Reform initially released the scorecard. For more information, see GAO, *Information Technology: Biannual Scorecards Have Evolved and Served as Effective Oversight Tools,* GAO-22-105659 (Washington, D.C.: Jan. 20, 2022) and *Information Technology and Cybersecurity: Significant Attention Is Needed to Address High-Risk Areas,* GAO-21-422T (Washington, D.C.: Apr. 16, 2021).

Component	Description
Incremental development	Agency Chief Information Officers (CIO) are to certify that IT investments are adequately implementing incremental development.
Working capital funds for IT modernization	Agencies are to establish a working capital fund, or equivalent, for use in transitioning from legacy IT systems, as well as for addressing evolving threats to information security. A working capital fund allows agencies to reinvest savings into modernization or cybersecurity initiatives.
Cybersecurity	Agencies are to use security tools to continuously monitor and diagnose the state of agencies' cybersecurity.
Telecommunication services transition	Agencies are required to transition their telecommunications services before their current contracts expire in May 2023.

Source: GAO analysis of scorecard documents. | GAO-22-106105

[a]Component was sunset and is no longer used as a basis for scorecard grades.

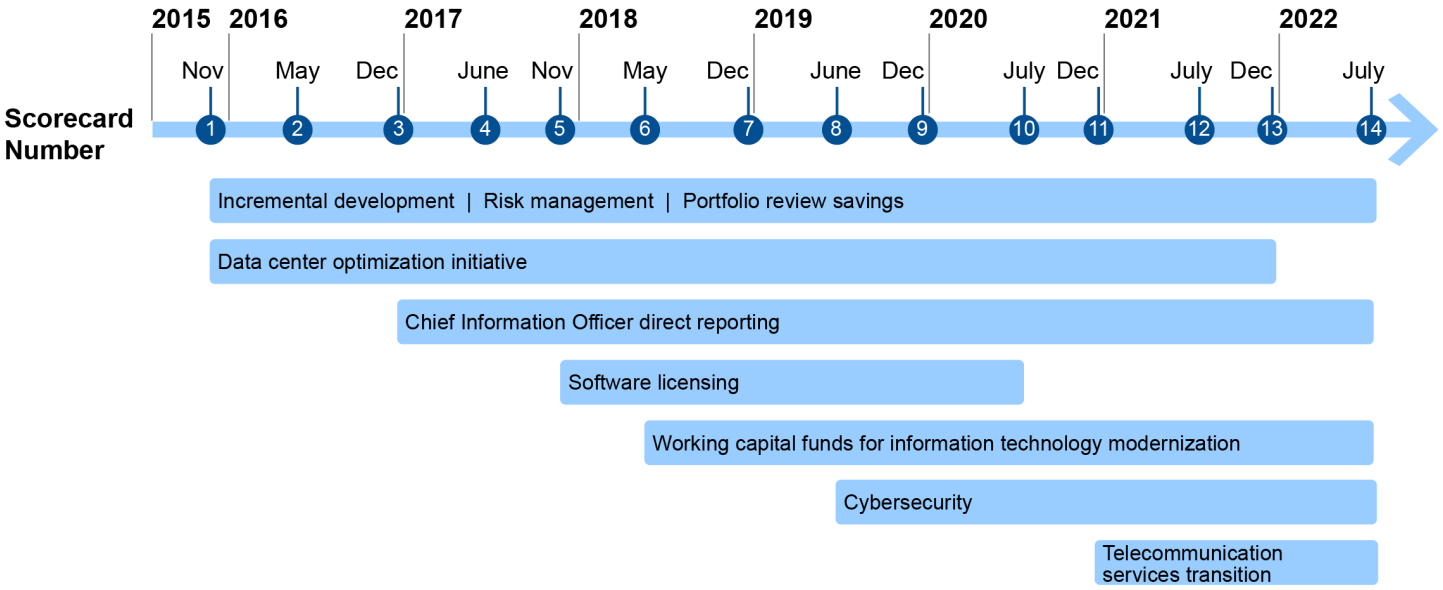
The scorecards evolved over time to include additional IT-related statutory requirements beyond FITARA. Initial components were specific to FITARA provisions on incremental development, risk management, portfolio review savings, and data centers.

Starting in 2017 and continuing through 2019, new components derived from provisions in the Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016, the Modernizing Government Technology Act, and the Federal Information Security Modernization Act of 2014 were added to the scorecard.[14] The scorecard further expanded in 2020 to include a government-wide component, telecommunications services transition.

As of July 2022, fourteen scorecards had been released. Figure 2 provides a timeline of the release dates for the scorecards and the associated components that were added.

[14]Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016, Pub. L. No. 114-210, 130 Stat. 824 (2016). Also known as the "MEGABYTE Act," the statute further enhances CIOs' management of software licenses by requiring agency CIOs to establish an agency software licensing policy and a comprehensive software license inventory to track and maintain licenses, among other requirements. The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128. Stat. 3073 (2014). FISMA 2014 largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (2002). The provisions known as the Modernizing Government Technology Act ("MGT Act"), Subtitle G of Title X, Div. A of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283, 1586 (2017) established new funding mechanisms for technology modernization.

Figure 2: Scorecards' Release Timeline with Associated Components



Source: GAO analysis of scorecard documents. | GAO-22-106105

As we previously testified, Subcommittee-assigned grades of agency performance have shown steady improvement and resulted in the scorecards serving as effective oversight tools.[15] For example, when software licensing was first introduced, three of 24 agencies had established comprehensive, regularly updated inventories. By December 2020, all 24 agencies had comprehensive inventories and analyzed software usage to make cost-effective decisions.

Additionally, for the December 2021 scorecard, all 24 agencies received A grades for the data center optimization initiative. This is notable progress compared to the initial November 2015 scorecard when 15 agencies received failing grades.

As a result, these components were removed (or sunset) from the scorecard grading. While the removal of these components is evidence of improvement, agencies' continued efforts in managing software licenses and data centers remains important.

[15]GAO-22-105659.

In summary, the federal government faces persistent difficulties acquiring, developing, managing, and providing adequate security over its IT investments. To address longstanding weaknesses and changes in the federal landscape, it will be essential for Congress to continue effective oversight and hold agencies accountable for improving IT management and cybersecurity. Tools such as the biannual scorecards can be essential in driving improvements. Moreover, implementation of outstanding GAO recommendations can be instrumental in delivering needed improvements.

Chairman Connolly, Ranking Member Hice, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Carol C. Harris, Director of Information Technology and Cybersecurity, at (202) 512-4456 or harriscc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Teresa M. Yost (Assistant Director), Jacqueline Mai (Analyst-in-Charge), Lauri Barnes, Christopher Businsky, Donna Epler, Valerie Hopkins, Cassaundra Pham, Scott Pettis, Sukhjoot Singh, and Haley Weller.