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 10:00 a.m. EST
Thursday, January 20, 2022

INFORMATION TECHNOLOGY

Biannual Scorecards Have Evolved and Served as Effective Oversight Tools

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

GAO-22-105659

GAO Highlights

Highlights of GAO-22-105659, a testimony before the Subcommittee on Government Operations, Committee on Oversight and Reform, House of Representatives

January 2022

INFORMATION TECHNOLOGY

Biannual Scorecards Have Evolved and Served as Effective Oversight Tools

Why GAO Did This Study

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.

To improve the management of IT, Congress and the President enacted FITARA in December 2014. The law better enables Congress to monitor covered agencies' progress in managing IT and hold them accountable. FITARA applies to the 24 agencies subject to the Chief Financial Officers Act of 1990, although not all FITARA provisions apply to the Department of Defense.

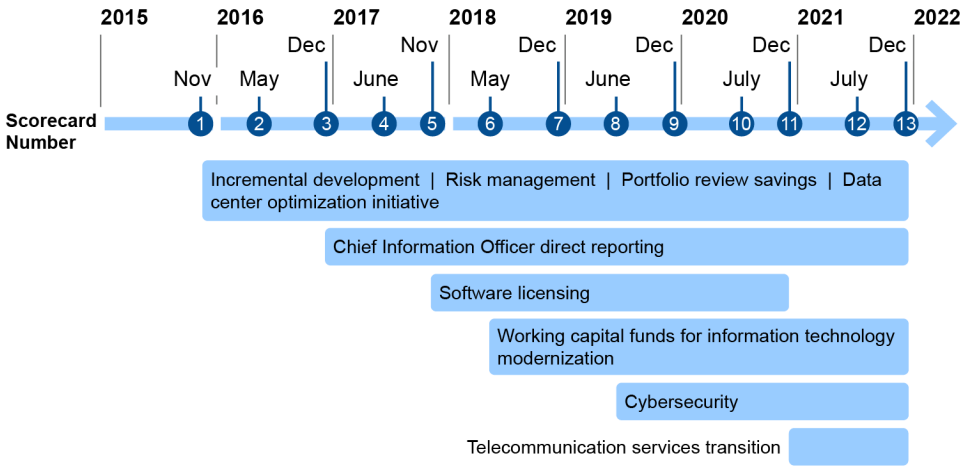
In November 2015, this Subcommittee began issuing biannual scorecards as an oversight tool to monitor agencies' progress toward implementing FITARA and subsequently, other IT-related issues. The scorecards rely on publicly available data to track and assign federal agencies letter grades (i.e., A, B, C, D, or F). As of January 2022, thirteen scorecards had been released.

GAO was asked to testify on the evolution and effectiveness of the biannual scorecards. For this testimony, GAO relied primarily on previously issued products.

What GAO Found

The Subcommittee's biannual scorecards initially focused on agencies' progress in implementing statutory provisions contained in the Federal Information Technology Acquisition Reform Act (FITARA) on topics such as incremental development and data center consolidation. The scorecard evolved over time to include additional IT-related components such as Chief Information Officer (CIO) direct reporting, software licensing, and cybersecurity (see figure).

Biannual Scorecards Release Timeline with Associated Components



Source: GAO analysis of scorecard releases and components. | GAO-22-105659

The biannual scorecards have served as effective tools for monitoring federal agencies' efforts in implementing statutory requirements and addressing other important IT issues. For example, the Subcommittee-assigned grades of agency performance have shown steady improvement. Specifically, from November 2015 through December 2021, agencies receiving C or higher grades increased from 29 to 100 percent (all agencies). For the most recent scorecard, 50 percent of agencies received an A or B. This escalation in grades reflects the notable improvements in components of the scorecard. For example:

- **Portfolio review savings.** The amount of cost savings and avoidances reported from annually reviewing IT portfolios increased from $3.4 billion to $23.5 billion.
- **CIO direct reporting.** The number of agency CIOs that report directly to the Secretary or Deputy increased from 12 to 16 of the 24 agencies.
- **Software licensing.** The number of agencies with comprehensive, regularly updated software licensing inventories went from 3 to all 24, resulting in the removal of this component from the scorecard.

Going forward, it will be important for Congress to continue adapting oversight tools, such as the biannual scorecards, to meet the advancing federal IT landscape.

View GAO-22-105659. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

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

I am pleased to be here today to discuss the information technology related biannual scorecards released by this Subcommittee. 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. Congressional oversight, including the use of biannual scorecards, is an important aspect of monitoring agencies' progress in better managing the large investment in IT and cybersecurity that the federal government continues to make.

At your request, my remarks today will focus on ways the scorecards have evolved and the effectiveness of this oversight tool in monitoring federal agencies' efforts to implement statutory requirements and other IT-related issues. This statement is based primarily 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 to our objectives. 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.

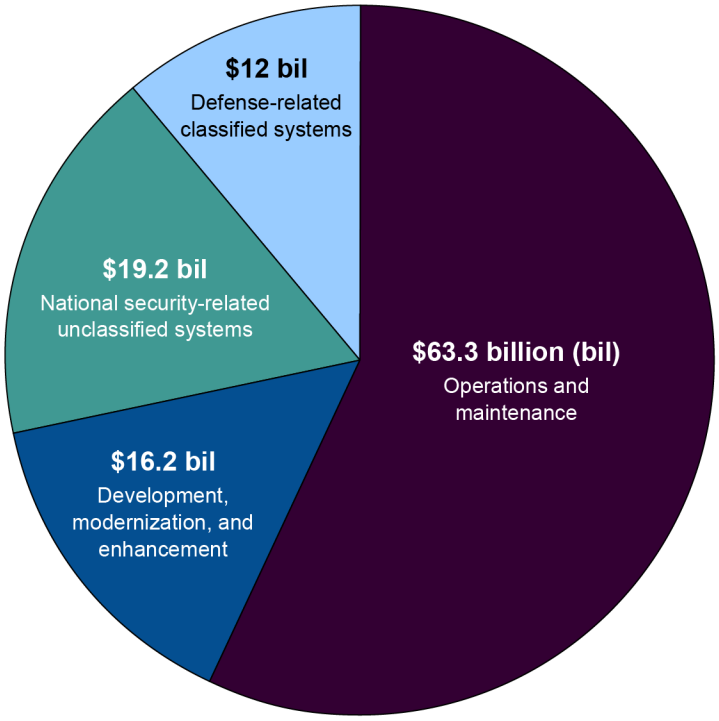
Background

Congress has long recognized that federal agencies accomplish their missions more quickly, effectively, and economically by using IT systems. These systems provide essential services that are critical to the health, economy, and defense of the nation. Toward this end, the federal government has projected that it will spend approximately $111 billion on IT investments in fiscal year 2022.

A large majority of these investments are intended 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 2022 spending also includes costs for defense-related classified systems

and national security-related unclassified systems, which support cybersecurity activities.[1] Figure 1 summarizes the planned fiscal year 2022 spending for IT investments.

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



Source: GAO analysis of Office of Management and Budget IT Dashboard reported data and Department of Defense IT and cyberspace activities budget overview fiscal year 2022. | GAO-22-105659

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 and governance. 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. For decades, our work has highlighted

[1]The overall totals of investment categories for defense-related classified systems and national security-related unclassified systems were included in the Department of Defense IT budget documentation for fiscal year 2022.

shortcomings in the federal government's management of IT investments.[2]

In addition, risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing. Risks include insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks.

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 nation as areas on our high-risk list.[3] 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.[4] 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]For example, see GAO, *Information Technology: IRS Needs to Address Operational Challenges and Opportunities to Improve Management*, GAO-21-178T (Washington, D.C.: Oct. 7, 2020); *DOD Business Transformation: Improved Management Oversight of Business System Modernization Efforts Needed*, GAO-11-53 (Washington, D.C.: Oct. 7, 2010); and *Information Technology: Actions Needed to Fully Establish Program Management Capability for VA's Financial and Logistics Initiative,* GAO-10-40 (Washington, D.C.: Oct. 26, 2009).

[3]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.: Jan. 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).

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

(2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.[5]

Since 2010, GAO has made approximately 5,200 recommendations in these two high-risk areas. As of January 2022, federal agencies had fully implemented about 75 percent of these recommendations.

Biannual Scorecards Have Evolved Beyond FITARA Implementation

Congress and the President enacted provisions commonly referred to as the Federal Information Technology Acquisition Reform Act (FITARA) in December 2014.[6] This legislation was enacted 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.[7]

As we previously reported, in November 2015 this Subcommittee began issuing biannual scorecards as an oversight tool for monitoring agencies' efforts toward implementing FITARA.[8] Biannual scorecards track and assign each agency a letter grade (i.e., A, B, C, D, or F). These grades

[5]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 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 limited the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

[6]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).

[7]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. However, FITARA has generally limited application to the Department of Defense.

[8]GAO, *Information Technology and Cybersecurity: Significant Attention Is Needed to Address High-Risk Areas,* GAO-21-422T (Washington, D.C.: Apr. 16, 2021). The scorecard was initially released by two subcommittees of the Committee on Oversight and Government Reform.

are comprised of several components. The initial four scorecard components, based on FITARA provisions, were:

- **Incremental development.** Agency Chief Information Officers (CIO) are required 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 Office of Management and Budget's (OMB) IT Dashboard.[9]
- **Portfolio review savings.** Agencies are to review IT investment portfolios annually in order to, among other things, increase efficiency and effectiveness and identify potential waste and duplication. OMB is required to quarterly report associated cost savings to Congress.
- **Data center consolidation/optimization initiative**.[10] Agencies are to provide a strategy for consolidating and optimizing their data centers and issue quarterly updates on the progress made.

Over time, the biannual scorecards evolved to include additional IT-related statutory requirements beyond FITARA. Specifically, the following components were added based on provisions from 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:[11]

[9]The IT Dashboard is a public website that discloses data on federal IT spending, including information on IT investments and data centers, among other things.

[10]In the initial scorecard, this component focused on data center consolidation; however, in June 2017, the Subcommittee expanded the component to include data center optimization.

[11]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).

- **Software licensing.** Agencies are to establish, among other things, a comprehensive, regularly updated inventory of software licenses and analyze software usage to make cost-effective decisions.[12]
- **Working capital funds for IT modernization**. Agencies are to establish a working capital fund for use in transitioning from legacy IT systems, as well as for addressing evolving threats to information security.[13]
- **Cybersecurity.** Agencies are to use security tools to continuously monitor and diagnose the state of agencies' cybersecurity.[14]

The scorecards further expanded to include the following government-wide components:

- **CIO direct reporting.** Agencies are to institutionalize their respective CIO's ability to report directly to the head or deputy of the agency.
- **Telecommunication services transition.** Agencies will need to transition their telecommunications services before their current contracts expire in May 2023.[15]

Figure 2 provides a timeline of the biannual scorecards release dates with the associated components.

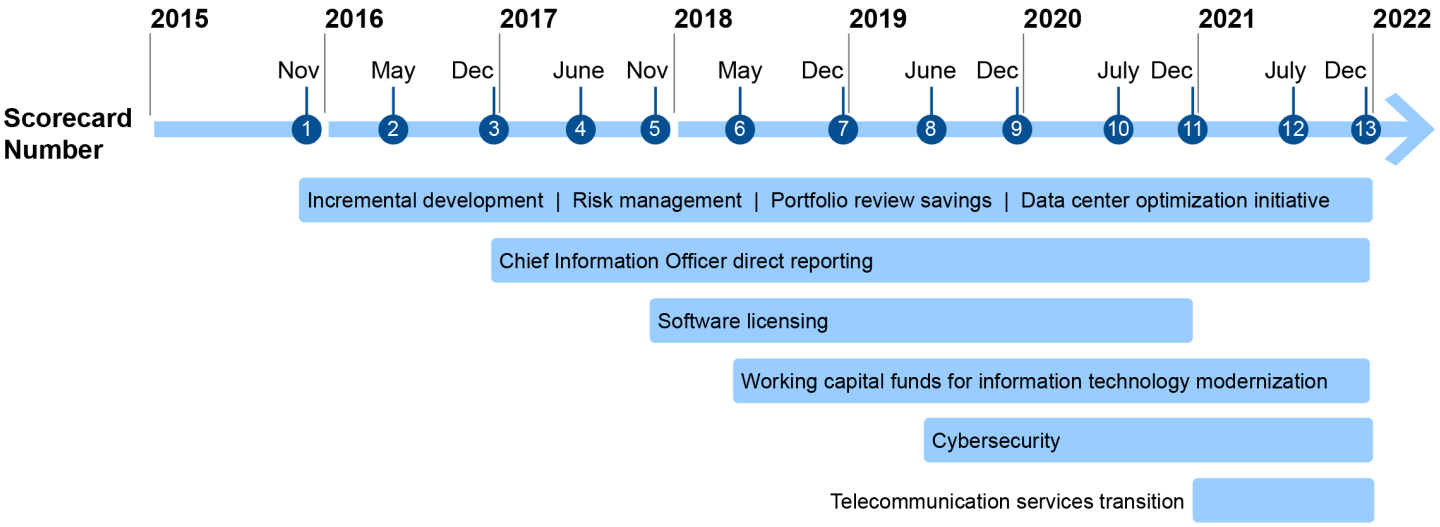
[12]The Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016, or the "MEGABYTE Act" further enhances CIOs' management of software licenses by requiring agency CIOs to establish an agency software licensing policy and a comprehensive software license inventory to track and maintain licenses, among other requirements. Pub. L. No. 114-210, 130 Stat. 824 (2016).

[13]A working capital fund allows agencies to reinvest savings into modernization or cybersecurity initiatives. The Modernizing Government Technology Act, Pub. L. No. 115-91, (2017) and the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1283, 1586 (2017).

[14]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).

[15]Delays in the previous telecommunication contract transition resulted in hundreds of millions of dollars in missed savings. Also see GAO, *Telecommunications: Agencies Should Fully Implement Established Transition Planning Practices to Help Reduce Risk of Costly Delays,* GAO-20-155 (Washington, D.C.: Apr. 7, 2020) and *Telecommunications: GSA Needs to Share and Prioritize Lessons Learned to Avoid Future Transition Delays,* GAO-14-63 (Washington, D.C.: Dec. 5, 2013).

Figure 2: Biannual Scorecards Release Timeline with Associated Components



Source: GAO analysis of scorecard releases and components. | GAO-22-105659

The data used for grading federal agencies have largely been publicly available and regularly updated. For instance, data to support measuring five components are from OMB's IT Dashboard. Table 1 provides a summary of the latest scorecard components and data sources.

Table 1: Scorecard Components and Data Sources, as of December 2021

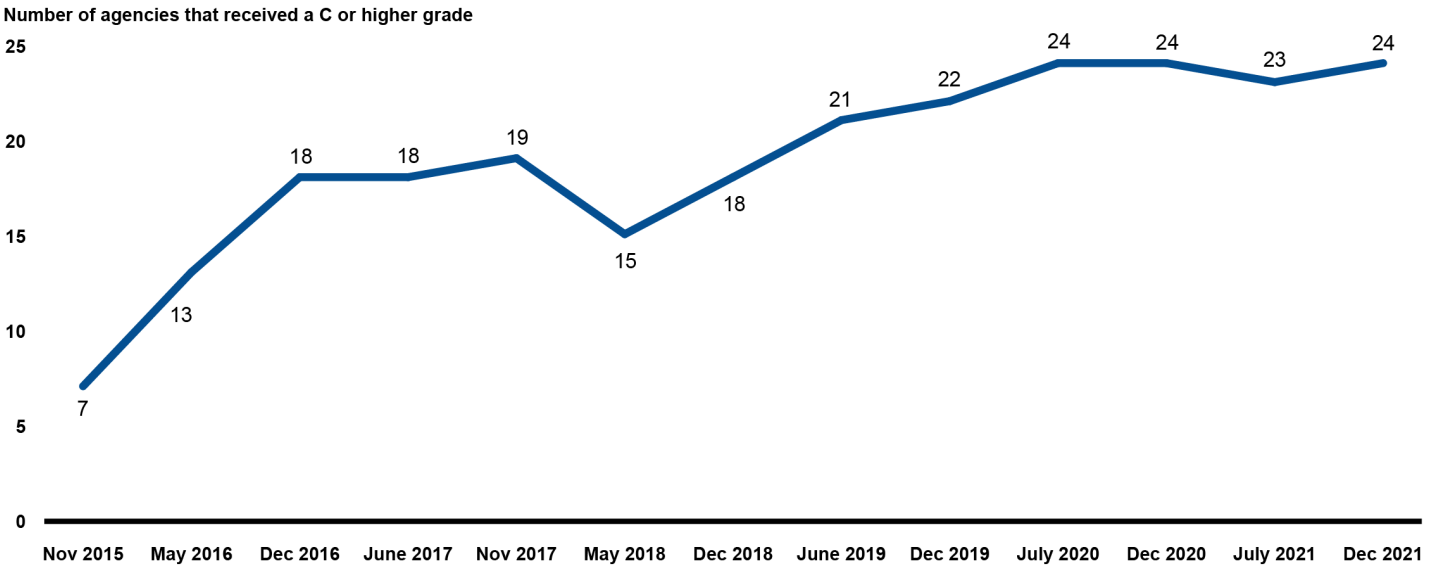
Component	Source
Incremental development	Office of Management and Budget's (OMB) Information Technology Dashboard investment project and activities data feeds
Risk management	OMB IT Dashboard business case data feed
Portfolio review savings	OMB IT Dashboard portfolio and cost savings data feeds
Data center optimization initiative	OMB IT Dashboard data center statistics report
Working capital funds for IT modernization	Agencies' written responses to working capital fund questions
Cybersecurity	OMB's Annual Federal Information Security Modernization Act (FISMA) Report to Congress and IT Dashboard FISMA performance data report
CIO direct reporting	Agencies' organization charts
Telecommunication services transition	General Services Administration's Enterprise Infrastructure Solutions Transition Progress Tracking Report Dashboard

Source: GAO analysis of scorecard documents. | GAO-22-105659

Biannual Scorecards Have Served As Effective Oversight Tools

Biannual scorecards have served as effective oversight tools for monitoring federal agencies' efforts in implementing statutory requirements and addressing other important IT issues. For example, the Subcommittee-assigned grades of agency performance have shown steady improvement. Specifically, from November 2015 through December 2021, agencies receiving C or higher grades increased from 29 (seven agencies) to 100 percent (all 24 agencies). For the most recent scorecard, 50 percent of agencies received an A or B. Figure 3 summarizes the distribution of agency biannual scorecard grades from November 2015 through December 2021.

Figure 3: Number of Federal Agencies that Received a C or Higher Grade on the Biannual Scorecards, November 2015 through December 2021



Source: GAO analysis of scorecard documents. | GAO-22-105659

The escalation in grades reflects the notable improvements in components of the scorecards. For example, when software licensing was first introduced, three of 24 agencies had established comprehensive, regularly updated inventories. In December 2020, all 24 agencies had comprehensive inventories and analyzed software usage to make cost-effective decisions. As a result, the software licensing component was removed from the scorecard. While the removal of this component is evidence of improvement, agencies' continued efforts over managing software licenses remains important.

Federal agencies' improvements in the following components between November 2015 and December 2021 also exemplify the effectiveness of the biannual scorecards:

- **Incremental development.** The portion of agencies' projects that reported plans to deliver functionality every six months increased from 58 percent to 81 percent.
- **Risk management.** The percentage of federal IT dollars identified as needing additional CIO attention increased from 24 percent to 61 percent.

- **CIO direct reporting.** The number of agency CIOs that report directly to the Secretary or Deputy increased from 12 to 16.
- **Portfolio review savings.** The amount of cost savings and avoidances reported from annually reviewing IT portfolios increased from $3.4 billion to $23.5 billion. This includes about $1 billion related to software license management and approximately $7 billion connected to data center consolidation and optimization.

In summary, the biannual scorecards have steadily evolved while serving as effective oversight tools for monitoring agencies' implementation of FITARA and other IT-related statutory requirements. Going forward, it will be important for Congress to continue adapting oversight tools, such as the biannual scorecards, to address changes in the federal landscape and hold agencies accountable for improving IT management.

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), Hannah Brookhart (Analyst-in-Charge), Jordan Adrian, Christopher Businsky, Donna Epler, Scott Pettis, and Kevin Walsh.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548