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 11:00 a.m. ET
Thursday, December 15, 2022

INFORMATION TECHNOLOGY AND CYBERSECURITY

Evolving the Scorecard Remains Important for Monitoring Agencies' Progress

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

and

Jennifer R. Franks, Director,
Information Technology and Cybersecurity

GAO-23-106414

GAO Highlights

Highlights of GAO-23-106414, a testimony before the Subcommittee on Government Operations, Committee on Oversight and Reform, House of Representatives

Why GAO Did This Study

Federal IT systems provide essential services that are critical to the health, economy, and defense of the nation. For fiscal year 2023, the federal government plans to spend over $122 billion on IT 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.

GAO has long recognized the importance of addressing these difficulties by including the management of IT acquisitions and operations as well as the cybersecurity of the nation as areas on its high-risk list.

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 and the importance of evolving the components. For this testimony, GAO relied on its previously issued products.

Since 2010, GAO has made approximately 5,400 recommendations to improve IT management and cybersecurity. As of December 2022, federal agencies have fully implemented about 76 percent of these. However, many critical recommendations have not been implemented—nearly 300 on IT management and more than 700 on cybersecurity.

View GAO-23-106414. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov or Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

December 15, 2022

INFORMATION TECHNOLOGY AND CYBERSECURITY

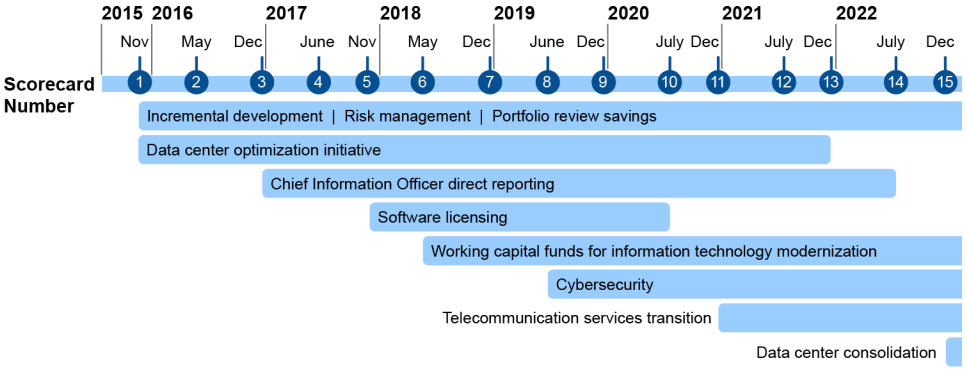
Evolving the Scorecard Remains Important for Monitoring Agencies' Progress

What GAO Found

Since November 2015, the scorecards issued by this Subcommittee have served as effective oversight tools for monitoring agencies' implementation of 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) 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 December 2022, fifteen scorecards had been released (see figure).

Scorecards Release Timeline with Associated Components



Source: GAO analysis of scorecard documents. | GAO-23-106414

The Subcommittee-assigned grades have shown steady improvement as demonstrated by the removal (or sunset) of components. For example, during 2020 and 2021, all 24 agencies received A grades for software licensing and data center optimization, resulting in removal of these components.

Notwithstanding the improvements made by using the scorecard, the federal government's difficulties acquiring, developing, managing, and securing its IT investments persist. Continued oversight by Congress to hold agencies accountable for implementing statutory provisions and addressing longstanding weaknesses is essential. Evolving the components of the scorecard to adapt to changes in the federal landscape also remains important.

Toward this end, GAO provided input to this Subcommittee regarding additional measures that could be added, including topics related to IT legacy system modernization and customer experience. GAO also provided input on ways to enhance the cybersecurity component.

Considering ways to evolve scorecard components is critical to increasing Congress' ability to monitor agencies' implementation of statutory IT provisions and address other key IT topics. Agency attention to implementing GAO recommendations can also be instrumental in delivering needed improvements.

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

Thank you for inviting us to discuss this Subcommittee's 15th biannual scorecard. The scorecards have been effective oversight tools in monitoring federal agencies' implementation of the statutory provisions commonly known as the Federal Information Technology Acquisition Reform Act (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.

The federal government spends more than $100 billion annually 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]

At your request, our testimony provides an overview of the scorecards and the importance of continued efforts to evolve them as oversight tools. 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 (2014); the Modernizing Government Technology (MGT) Act provisions of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, div. A, title X, subtitle G (2017); Making Electronic Government Accountable by Yielding Tangible Efficiencies (MEGABYTE) Act of 2016, Pub. L. No. 114-210, (2016); and the Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, (2014), which largely superseded the Federal Information Security Management Act of 2002 (FISMA), Title III of Pub. L. No. 107-347, 116 Stat. 2899, 2946 (2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

[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).

to our objective. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objective 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.

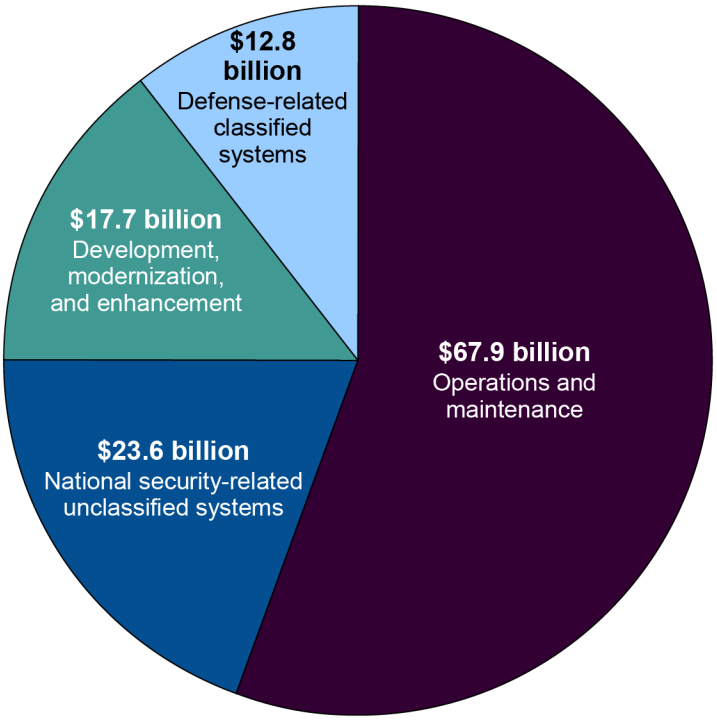
Background

Federal IT systems provide essential services that are critical to the health, economy, and defense of the nation. For fiscal year 2023, the federal government plans to spend about $122 billion on IT investments. These investments largely support the operation and maintenance of existing IT systems as well as system development, modernization, and enhancement activities. Costs for defense-related classified systems and national security-related unclassified systems are also included.[3]

Figure 1 summarizes the planned fiscal year 2023 spending for IT investments.

[3]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-23-106414

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 experience schedule slippages while contributing little to mission-related outcomes. 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.[4]

[4]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).

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 avenues of attack.

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.[5] 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. We also reiterated the urgent need for the federal government to engage in actions to address major cybersecurity challenges.[6]

Since 2010, GAO has made approximately 5,400 recommendations in these two high-risk areas. As of December 2022, federal agencies had fully implemented about 76 percent of these recommendations; however, many critical recommendations have not been implemented—nearly 300 on IT management and more than 700 on cybersecurity.

[5]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).

[6]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). These major cybersecurity challenges are (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.

Overview of the Biannual Scorecards

In December 2014, Congress and the President enacted the statute containing the FITARA provisions. A purpose of FITARA was 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] This Subcommittee began issuing biannual scorecards in November 2015 as a tool for conducting oversight of FITARA implementation.[8] 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.

Initially the scorecards focused on FITARA provisions such as incremental development, risk management, portfolio review savings, and data centers. Transitioning beyond FITARA, in 2017 through 2022, new components were added to the scorecard.[9] These components were software licensing, working capital funds for IT modernization, cybersecurity, telecommunications services transition, and data center consolidation.

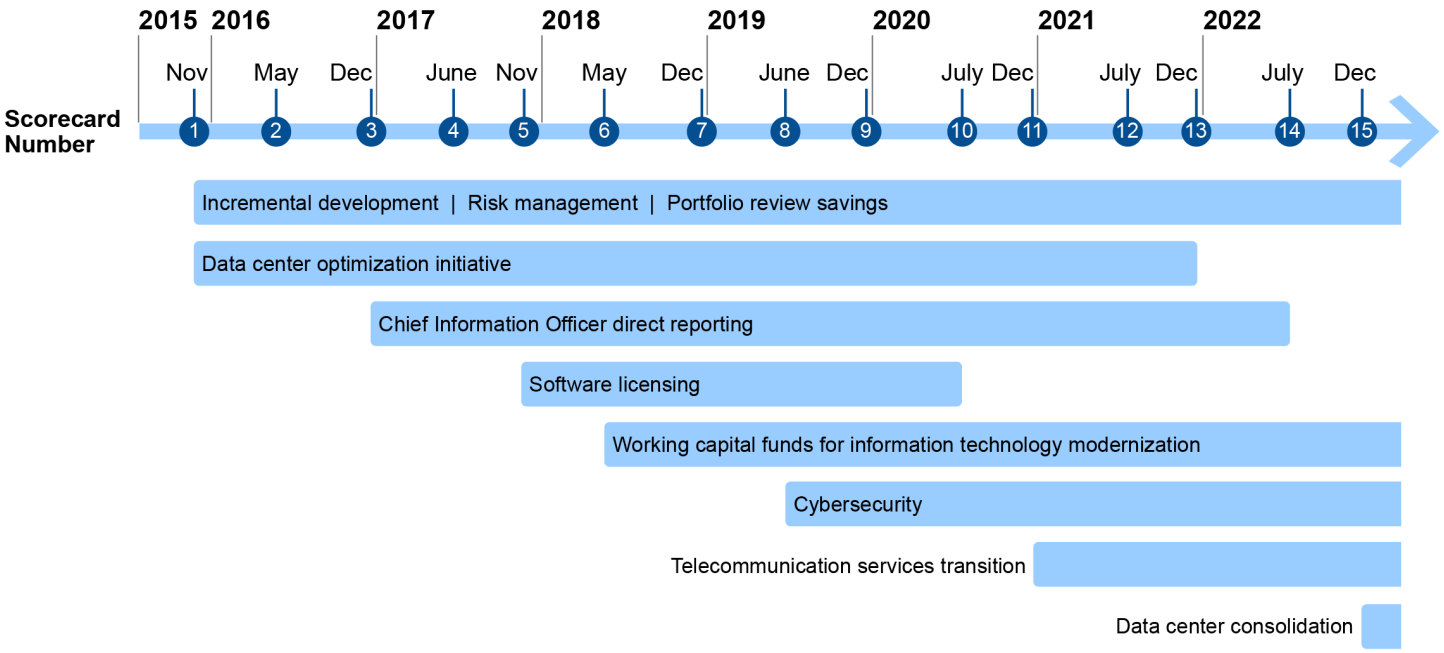
Figure 2 provides a timeline of the release dates for the scorecards and when the associated components were added or removed.

[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]Two Subcommittees of the Committee on Oversight and Government Reform initially released the scorecard. For more information, see GAO, *Information Technology and Cybersecurity: Significant Attention Is Needed to Address High-Risk Areas,* GAO-21-422T (Washington, D.C.: Apr. 16, 2021).

[9]These components were derived from provisions in the MGT Act, MEGABYTE Act of 2016, and FISMA.

Figure 2: Scorecards' Release Timeline with Associated Components



Source: GAO analysis of scorecard documents. | GAO-23-106414

Table 1 summarizes the components that have been included on the scorecards.

Table 1: Summary Descriptions of the Scorecard Components, as of December 2022

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 to, among other things, increase efficiency and effectiveness and identify potential waste and duplication.
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[a]	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.

Component	Description
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.
Data center consolidation	Agencies are to report on plans for completing their data center consolidation efforts.

Source: GAO analysis of scorecard documents. | GAO-23-106414

[a]Component was removed from the scorecard.

Evolving the Scorecard Remains Important for Continued Monitoring of Agencies' Progress

The biannual scorecards have served as effective oversight tools for monitoring agencies' implementation of statutory requirements and additional IT-related topics.[10] Specifically, from November 2015 through December 2022, 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.

Furthermore, the Subcommittee-assigned grades have shown steady improvement as demonstrated by the removal (or sunset) of scorecard components. For example, when software licensing was first introduced, three of the 24 agencies had established comprehensive, regularly updated inventories. By December 2020, all 24 agencies had established 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.

Notwithstanding the improvements made by using the scorecard, the federal government's difficulties acquiring, developing, managing, and securing its IT investments persist. Evolving the components of the scorecard to adapt to changes in the federal landscape and address long-standing weaknesses in federal IT and cybersecurity remains important. Such tools enable Congress to monitor progress toward implementing statutory requirements and hold agencies accountable for improvements.

[10]GAO, *Information Technology and Cybersecurity: Using Scorecards to Monitor Agencies' Implementation of Statutory Requirements,* GAO-22-106105 (Washington, D.C.: July 28, 2022) and *Information Technology: Biannual Scorecards Have Evolved and Served as Effective Oversight Tools,* GAO-22-105659 (Washington, D.C.: Jan. 20, 2022).

To support continued efforts to adapt the scorecard, we have identified areas for measuring agency actions. In March 2022, we provided input to this Subcommittee regarding additional measurements that could be added to the scorecard, including topics related to IT legacy system modernization, investment cost and schedule, IT workforce planning, customer experience, and cybersecurity. For example:

- Federal IT legacy systems are becoming increasingly obsolete and can be more costly to maintain, more exposed to cybersecurity risks, and less effective in meeting their intended purposes. As we have reported in the past, specific attributes determine if systems are obsolete and need modernization.[11] These attributes include the use of legacy programing languages, criticality to mission success, and risk. It would be helpful to devise a metric that tracks progress toward updating or eliminating the most critical legacy systems. One way to do this would be through assessing agencies' modernization plans.
- For an issue as complex and dynamic as cybersecurity, additional measures could provide a more detailed and comprehensive view into an agency's overall posture. The cybersecurity grade relies on inspector general assessments of agency cybersecurity programs as reported in the Office of Management and Budget's Annual FISMA Report to Congress.[12] These assessments reflect a portion of the agency's program and a snapshot in time. A different approach could be to grade agencies using a risk-based approach that reflects current trends in cybersecurity and government-wide initiatives. Furthermore, continuously reported metrics could also help to achieve better insight into agencies implementation of effective cybersecurity programs.

We recognize that there may be limited data currently available for the topics we proposed including on future scorecards; however, we continue to see value in pursuing data in order to adapt the scorecard. Another way to evolve the scorecard methodology could be to monitor progress based on metrics that take into account an agency's size and mission. By identifying, collecting, and publicly releasing consistent data for many of these topics, the ability to evolve the scorecard could increase. This in turn could enhance Congress' ability to monitor agencies' progress in better managing and protecting their IT investments.

[11]GAO-19-471.

[12]Prior to July 2022, the cybersecurity grade also included the results of agencies' FISMA performance data. The performance data was based cross-agency priority goals that were discontinued in 2021.

In summary, adapting the scorecard to changes in the federal IT landscape remains important for monitoring agencies' progress in implementing statutory requirements. Continued oversight by Congress to hold agencies accountable for addressing long-standing weaknesses in IT management and cybersecurity is essential.

GAO has long recognized the importance of improving the management of IT acquisitions and operations as well as ensuring the cybersecurity of the nation. Moreover, agency attention to implementing recommendations we have made—nearly 300 on IT management and more than 600 on cybersecurity—can be instrumental in delivering needed improvements in acquiring, developing, managing, and securing federal IT investment.

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

GAO Contacts and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov or Jennifer R. Franks at (404) 679-1831 or franksj@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), Cassaundra Pham (Analyst-in-Charge), Alex Anderegg, Donny Baca, Lauri Barnes, Christopher Businsky, Donna Epler, Nicole Jarvis, Keith Kim, Scott Pettis, Meredith Raymond, Kevin Smith, Jonathan Wall, and Haley Weller.

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