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 2:00 p.m. ET
Wednesday, July 28, 2021

# CYBERSECURITY AND INFORMATION TECHNOLOGY

# Federal Agencies Need to Strengthen Efforts to Address High-Risk Areas

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

Accessible Version

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-105325

# GAO Highlights

Highlights of GAO-21-105325, a testimony before the Subcommittee on Government Operations, Committee on Oversight and Reform, House of Representatives

July 28, 2021

# CYBERSECURITY AND INFORMATION TECHNOLOGY

## Federal Agencies Need to Strengthen Efforts to Address High-Risk Areas

## Why GAO Did This Study

The nation's critical infrastructures and federal agencies are dependent on IT systems and electronic data to carry out operations and to process, maintain, and report essential information. Each year, the federal government spends more than $100 billion on cybersecurity and IT investments.

GAO has long stressed the continuing and urgent need for effective cybersecurity, as underscored by recent events that have illustrated persistent and evermore sophisticated cyber threats and incidents. Moreover, many IT investments have failed, performed poorly, or suffered from ineffective management. Accordingly, GAO has included information security on its high-risk list since 1997 and added improving the management of IT acquisitions and operations in 2015. In its March 2021 high-risk series update, GAO reported that significant attention was needed in both of these important areas.

GAO was asked to testify on federal agencies' efforts to address cybersecurity and the management of IT. For this testimony, GAO relied on selected products it previously issued.

## What GAO Recommends

Federal agencies have implemented about 73 percent of the approximately 5,100 recommendations that GAO has made since 2010 on cybersecurity and IT management. However, about 950 cybersecurity and approximately 300 IT recommendations have not been implemented. Actions are needed on these to successfully address the high-risk areas.

View GAO-21-105325. For more information, contact Carol C Harris at (202) 512-4456 or harriscc@gao.gov.

## What GAO Found

In March 2021, GAO issued its high-risk series update and emphasized that federal agencies' needed to implement numerous critical actions to strengthen the nation's cybersecurity and information technology (IT) management efforts. In the update, GAO reiterated the importance of agencies addressing four major cybersecurity challenges facing the nation: (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. Overall, the federal government has to move with a greater sense of urgency to fully address key cybersecurity challenges. In particular:

- **Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace**. In September 2020, GAO reported that the White House's national cyber strategy and associated implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources needed.
- **Mitigate global supply chain risks**. GAO reported in December 2020 that few of the 23 civilian federal agencies it reviewed implemented foundational practices for managing information and communication technology supply chain risks.
- **Address weaknesses in federal agencies information security programs.** GAO reported in July 2019 that 23 agencies almost always designated a risk executive, but had not fully incorporated other key risk management practices, such as establishing a process for assessing agency-wide cybersecurity risks.

In its March update, GAO also stressed the importance of the Office of Management and Budget (OMB) and federal agencies fully implementing critical actions recommended to improve the management of IT to better manage tens of billions of dollars in IT investments. GAO emphasized, for example, that

- OMB had demonstrated its leadership commitment to improving IT management, but sustaining this commitment was critically important;
- twenty-one of 24 federal agencies had not yet implemented recommendations to fully address the role of Chief Information Officers, including enhancing their authorities;
- OMB and agencies needed to address modernization challenges and workforce planning weaknesses; and
- agencies could take further action to reduce duplicative IT contracts and reduce the risk of wasteful spending.

Until OMB and federal agencies take critical actions to strengthen efforts to address these important high-risk areas, longstanding and pervasive weaknesses will likely continue to jeopardize the nation's cybersecurity and management of IT.

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

Thank you for the opportunity to contribute to today's discussion on cybersecurity and the federal government's management of information technology (IT). Our nation's critical infrastructures and agencies are reliant on IT systems to carry out operations and to process, maintain, and report essential information. Each year, the federal government spends more than $100 billion on investments related to cyber and IT.

We have long stressed the urgent need for effective cybersecurity, as underscored by increasingly sophisticated threats and frequent cyber incidents. Recent events, including the SolarWinds incident as well as the ransomware attack that led to a shutdown of a major U.S. fuel pipeline, have illustrated that the nation's critical infrastructure and federal agencies' IT systems continue to face growing cyber threats.[1] Further, the effective and efficient management of IT investments has been a longstanding challenge in the federal government. In our prior work, we have seen that many of these investments have performed poorly and frequently failed to deliver capabilities in a timely manner while contributing little to mission-related outcomes.

My remarks today will focus on what we have found in our prior work on federal agencies' efforts to address cybersecurity and improve IT management. This statement is based on the results of our work discussed in selected reports and testimonies issued between February 2015 and May 2021. 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.

[1]For more information regarding these recent events, see GAO, *Cybersecurity: Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks,* GAO-21-594T (Washington, D.C.: May 25, 2021). Ransomware is a type of malware used to deny access to IT systems or data and hold the systems or data hostage until a ransom is paid.

# Background

As discussed with this subcommittee in April 2021, cybersecurity and the federal government's management of IT are two areas identified as high-risk.[2] Specifically, we have designated information security as a government-wide high-risk area since 1997.[3] In 2003, we added the protection of critical infrastructure to the information security high-risk area, and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information.[4]

In our high-risk updates from September 2018 and March 2021, we emphasized the critical need for the federal government to take 10 specific actions to address four major cybersecurity challenges that the federal government and other entities face.[5] These 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. Figure 1 provides an overview of the critical actions needed to address the four major cybersecurity challenges.

[2]GAO, *Information Technology and Cybersecurity: Significant Attention Is Needed to Address High-Risk Areas,* GAO-21-422T (Washington, D.C.: Apr. 16, 2021).

[3]GAO, *High-Risk Series: Information Management and Technology*, HR-97-9 (Washington, D.C.: Feb. 1997) and *High-Risk Series: An Overview*, HR-97-1 (Washington, D.C.: Feb. 1997).

[4]GAO, *High-Risk Series: An Update,* GAO-15-290 (Washington, D.C.: Feb. 11, 2015) and *High-Risk Series: An Update,* GAO-03-119 (Washington, D.C.: Jan. 2003).

[5]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: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

**Figure 1: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges**

| Establishing a comprehensive cybersecurity strategy and performing effective oversight | Securing federal systems and information | Protecting cyber critical infrastructure | Protecting privacy and sensitive data |
|---|---|---|---|
| 1 Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace. | 5 Improve implementation of government-wide cybersecurity initiatives. | 8 Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks). | 9 Improve federal efforts to protect privacy and sensitive data. |
| 2 Mitigate global supply chain risks (e.g., installation of malicious software or hardware). | 6 Address weaknesses in federal agency information security programs. | | 10 Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent. |
| 3 Address cybersecurity workforce management challenges. | 7 Enhance the federal response to cyber incidents. | | |
| 4 Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things). | | | |

Source: GAO analysis; images: peshkov/stock.adobe.com; Gorodenkoff/stock.adobe.com; metamorworks/stock.adobe.com; Monster Ztudio/stock.adobe.com. | GAO-21-105325

**Text of Figure 1: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges**

- Establishing a comprehensive cybersecurity strategy and performing effective oversight
  - Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.

    - Mitigate global supply chain risks (e.g., installation of malicious software or hardware).
    - Address cybersecurity workforce management challenges.
    - Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).
- Securing federal systems and information
    - Improve implementation of government-wide cybersecurity initiatives.
    - Address weaknesses in federal agency information security programs.
    - Enhance the federal response to cyber incidents.
- Protecting cyber critical infrastructure
    - Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).
- Protecting privacy and sensitive data
    - Improve federal efforts to protect privacy and sensitive data.
    - Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Source: GAO analysis. | GAO-21-105325

Addressing cybersecurity challenges is important because threats to IT systems and networks supporting the federal government and the nation's critical infrastructure are increasing. These systems and networks are often interconnected with other internal and external systems and networks, including the internet. With this greater connectivity, threat actors are increasingly willing and capable of conducting a cyberattack on our nation's critical infrastructure and federal agencies' IT systems that could be disruptive and destructive.

Recent events involving a software supply chain compromise of SolarWinds Orion, a network management software suite, and the shutdown of a major U.S. fuel pipeline due to a cyberattack highlight the persistence and significance of these threats. In April and May 2021, we issued infographics regarding the SolarWinds cyberattack and response efforts as well as the basic components and vulnerabilities of a U.S.

pipeline system.[6] We have ongoing work examining federal agencies' responses to SolarWinds and any lessons that they have identified from the compromise. We plan to issue a report detailing our findings later this fall 2021.

Our prior work has also highlighted shortcomings in the federal government's management of IT. For fiscal year 2021, the federal government has projected that it will spend approximately $104 billion on IT investments. Notwithstanding the large amount of spending, these investments too frequently fail to deliver capabilities in a timely manner, incur cost overruns, and/or experiences schedule slippages while contributing little to mission-related outcomes.

In addition, we have pointed out that federal IT investments often suffer from a lack of disciplined and effective management. Specifically, in February 2015 we identified that the federal government's continued experience with failed and troubled IT projects was compounded by inconsistent implementation of numerous initiatives undertaken by the executive branch to better manage IT investments. Further, we stressed that the government would likely continue to produce disappointing results and miss opportunities to improve IT management, reduce costs, and improve services to the public, unless significant actions were taken to address the longstanding challenges.[7]

Consequently, in recognizing the severity of issues related to the government-wide management of IT, we added improving the management of IT acquisitions and operations to our high-risk list in February 2015.[8] In our March 2021 high-risk update, we reported that while progress had been made in addressing this high-risk area, significant actions were required by federal agencies to build on this progress.[9] For example, we emphasized that the Office of Management and Budget (OMB) and federal agencies needed to continue fully

[6]GAO, *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic),* (Washington, D.C.: May 18, 2021) and *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)*, (Washington, D.C.: Apr. 22, 2021).

[7]GAO-15-290.

[8]GAO-15-290.

[9]GAO-21-119SP.

implementing key statutory requirements aimed at reforming IT acquisitions.[10]

# Federal Agencies Need to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges

In our March 2021 high-risk update, we emphasized that federal agencies' ability to respond to cyber threats or attacks are limited without urgent actions to address four major cybersecurity challenges. These actions include (1) developing and executing a more comprehensive federal strategy for national cybersecurity and global cyberspace, (2) mitigate global supply chain risks, and (3) addressing weaknesses in information security programs.[11] Overall, since 2010 we have made about 3,700 recommendations related to our high-risk area focused on enhancing our nation's cybersecurity efforts.

## Develop and Execute a More Comprehensive Federal Strategy for National Cybersecurity and Global Cyberspace

For more than a decade, we have been reporting on the importance of a comprehensive strategy and clearly defined leadership to address national cybersecurity issues. For example, in July 2010 we reported that the government faced a number of challenges that impeded its ability to formulate and implement a coherent approach to addressing the global aspects of cybersecurity.[12]

[10]As part of its effort to reform the government-wide management of IT, Congress and the President enacted statutory provisions commonly known as the Federal Information Technology Acquisition Reform Act (FITARA), in December 2014. 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). The FITARA Enhancement Act of 2017, Pub. L. No 115-88, 131 Stat. 1278 (2017), as well as other legislation, eliminated or extended the sunset dates of certain FITARA provisions.

[11]GAO-21-288.

[12]GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance,* GAO-10-606 (Washington, D.C.: July 2, 2010).

More recently, in September 2020, we reported that the White House's 2018 National Cyber Strategy and related implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources needed.[13] Accordingly, we recommended that the National Security Council work with relevant federal entities to update cybersecurity strategy documents to include goals and resource information, among other things. The National Security Council staff neither agreed nor disagreed with our recommendation and has yet to address it.

We have also stressed the urgency and necessity of clearly defining a central leadership role in order to coordinate the government's efforts to overcome the nation's cyber-related threats and challenges. In September 2020, we also reported that, in light of the elimination of the White House Cybersecurity Coordinator position in May 2018, it was unclear which official within the executive branch ultimately maintained responsibility for coordinating the execution of the National Cyber Strategy and related implementation plan. Accordingly, we suggested that Congress consider legislation to designate a position in the White House to lead such an effort. In January 2021, Congress enacted a statute that established the Office of the National Cyber Director within the Executive Office of the President.[14]

In June 2021, the Senate confirmed a Director to lead this new office. As a result, the federal government is in a better position to direct activities to overcome the nation's cyber threats and challenges, and to perform effective oversight. Although progress in establishing a central role has been made, our recommendation to update cybersecurity strategy documents to include goals and resource information, among other things, has still not yet been addressed and remains important to overcome the cyber challenges facing our nation.

[13]GAO, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*, GAO-20-629 (Washington, D.C.: Sept. 22, 2020).

[14]Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1752, 134 Stat. 3388, 4144 (2021). The National Cyber Director, a presidentially appointed, Senate-confirmed position will head the office.

## Mitigate Global Supply Chain Risks

In December 2020, we reported on 23 civilian agencies'[15] implementation of foundational practices for managing information and communication technology (ICT) supply chain risks.[16] In that report, we identified the seven practices from the National Institute of Standards and Technology's guidance that are foundational for an organization-wide approach to ICT supply chain risk management.[17] These practices include, among other things, establishing executive oversight of ICT activities, developing an agency-wide ICT strategy, and ensuring suppliers are adequately addressing risks associated with ICT products and services.

However, as we discussed in our report, none of the 23 agencies had fully implemented all of the supply chain risk management practices, and 14 of the 23 agencies had not implemented any of the practices. In a sensitive report issued in October 2020, we made 145 recommendations to the 23 agencies to fully implement the foundational practices in their organization-wide approaches to information and communication technology supply chain risk management.[18]

As of June 2021, we received updates from 22 of the 23 agencies regarding actions taken or planned to address our recommendations. However, none of the agencies had fully implemented all of their associated recommendations. Until they do so, agencies will be limited in their ability to effectively address supply chain risks across their organizations.

[15]We did not include the Department of Defense because the scope of our review focused on civilian agencies.

[16]GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, D.C.: Dec. 15, 2020).

[17]See National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, v. 1.1 (Apr. 16, 2018); *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, SP 800-161 (Gaithersburg, Md.: Apr. 2015); *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37, Rev. 2 (Gaithersburg, Md.: Dec. 2018); and *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: Mar. 2011).

[18]GAO, *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-164SU (Washington, D.C.: Oct. 27, 2020).

## Address Weaknesses in Federal Agencies' Information Security Programs

We have also reported that agencies need to address information security program weaknesses by, for example, fully establishing risk management programs. Specifically, in July 2019, we reported on key practices for establishing an agency-wide cybersecurity risk management program that include designating a cybersecurity risk executive, developing a risk management strategy and policies to facilitate risk-based decisions, assessing cyber risks to the agency, and establishing coordination with the agency's enterprise risk management program.[19]

Although the 23 agencies we reviewed almost always designated a risk executive, they had not fully incorporated other key practices in their programs, such as:

- establishing a cybersecurity risk management strategy to delineate boundaries for risk-based decisions;
- establishing agency- and system-level policies for assessing, responding to, and monitoring risk;
- establishing a process for assessing agency-wide cybersecurity risks; and
- establishing a process for coordinating between cybersecurity and enterprise risk management programs for managing all major risks.

We made 57 recommendations to the 23 agencies to address the challenges identified in our report. Although the agencies have taken steps to address these recommendations, as of July 2021, more than half of the recommendations had yet to be fully implemented. Until these challenges are addressed, agencies will face an increased risk of cyber-based incidents that threaten national security and personal privacy.

# Improving the Management of IT Acquisitions Requires Action by OMB and Federal Agencies

In our March 2021 high-risk update, we stressed the importance of the Office of Management and Budget (OMB) and other federal agencies fully implementing critical actions we recommended to better manage tens of

[19]GAO, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges,* GAO-19-384 (Washington, D.C.: July 25, 2019).

billions of dollars in IT investments.[20] We also emphasized that sustained leadership, among other things, can improve IT management.

Further, our high-risk update highlighted how OMB and other federal agencies could improve IT management efforts by taking action to, among other things, align practices with federal law and guidance in order to ensure the Chief Information Officer (CIO) is adequately involved in the acquisition process. For this high-risk area, since 2010 we have made nearly 1,400 recommendations focused on improving government-wide management of IT acquisitions and operations.

## Sustained Leadership Can Improve Agencies' IT Modernization and Workforce Challenges

As noted in our high-risk update, OMB has continued to demonstrate its leadership commitment through actions taken to provide guidance and government-wide strategies for key issues, including federal data centers and cloud computing. However, maintaining this current level of leadership with the new administration is important for ensuring that agencies succeed. To ensure progress in addressing long-standing IT management challenges, sustained executive branch leadership continues to be essential.

Our update to the IT acquisition and operations high-risk area also emphasized federal agencies' IT modernization efforts. We highlighted, in particular, the Technology Modernization Fund established in December 2017 to assist agencies with funding to replace aging IT systems.[21]

In December 2019, we reported that Congress had appropriated $125 million to the Technology Modernization Fund but that challenges with covering the cost of operating the fund had resulted in fewer funds being available than anticipated for the new projects.[22] Our work identified the need for OMB to (1) develop a plan to address the challenges with operating the fund and (2) clarify guidance for agencies' cost estimates associated with the awarded projects. However, as of July 2021, OMB

[20]GAO-21-422T.

[21]*National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1283, 1586 (2017).

[22]GAO, *Technology Modernization Fund: OMB and GSA Need to Improve Fee Collection and Clarify Cost Estimating Guidance for Awarded Projects,* GAO-20-3 (Washington, D.C.: Dec. 12, 2019).

had not yet taken the necessary steps to address our findings. Until OMB clarifies the requirement that agencies follow cost estimating processes, agencies are at risk of continuing to provide unreliable cost information in their proposals.

The recent increase in appropriations to the Technology Modernization Fund further highlights the importance of addressing challenges we identified in 2019. On March 11, 2021, Congress and the President enacted legislation that appropriated an additional $1 billion to be available until September 30, 2025 to carry out the purposes of the fund.[23] According to the fund's website, as of June 2021, approximately $89 million had been awarded to 11 projects across seven federal agencies and new proposals are reviewed on a rolling basis.[24] We have ongoing work evaluating the Technology Modernization Fund cost estimating practices and plan to issue a report detailing our findings by the end of 2021.

We have also previously reported that effective workforce planning is key to addressing the federal government's IT challenges and ensuring that agencies have staff with the necessary knowledge, skills, and abilities to execute a range of management functions that support agencies' missions and goals. In this regard, we have stressed that implementing workforce planning activities can facilitate the success of major IT acquisitions.[25]

In August 2018, we reported on critical actions needed to address shortcomings and challenges in implementing CIO responsibilities, including the role of the CIO in assessing agency IT workforce needs.[26] Specifically, we found that agencies had not modified their practices to fully address the role of the CIO, consistent with federal laws and OMB's guidance. The guidance covers, among other things, enhancing the authority of federal CIOs and ensuring that program staff have the

[23]*American Rescue Plan Act of 2021*, H.R. 1319, Pub. L. No: 117-2, Title IV, § 4011, 135 Stat. 4, 79 (2021).

[24]The $89 million awarded was part of the initial $125 million appropriated.

[25]GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps,* GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

[26]GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities,* GAO-18-93 (Washington, D.C.: Aug. 2, 2018).

necessary knowledge and skills to effectively acquire IT. Accordingly, we reported that the majority of agencies' policies minimally addressed or did not address the role of their CIOs with respect to the IT workforce and made related recommendations. As of July 2021, 21 of the 24 major federal agencies had not yet implemented our recommendations.

We also identified the need for OMB to address CIO responsibilities not included in existing guidance—in particular, roles related to IT workforce matters. As we stressed in our August 2018 report, until OMB updates its guidance to address these responsibilities, CIOs may not have the personnel needed to effectively acquire, maintain, and secure their IT systems. As of July 2021, OMB had not yet taken action to fully address our recommendation.

In October 2019, our report on major agencies' implementation of IT workforce planning strategies noted that 23 of 24 agencies had at least partially implemented three of eight key workforce planning activities, including identifying staffing needs and assessing gaps.[27] However, most of the agencies had minimally implemented or had not implemented five other workforce planning activities, including developing strategies to address those gaps. The agencies provided various reasons for their limited progress in implementing workforce planning activities, including competing priorities and limited resources.

We made a recommendation to 18 of the 24 agencies to fully implement the eight key IT workforce planning activities. Thirteen agencies agreed with the recommendation, while the other five expressed a range of views. Although, as of July 2021, none of the agencies had fully addressed the recommendation, a number of agencies had made progress toward implementation.

## Greater Cost Savings Could be Achieved by Addressing IT Acquisition Shortcomings

A key component of improving the management of IT is the involvement of the agency CIO in the acquisition process. Toward this end, several agencies had made progress in identifying IT contracts and ensuring that acquisition offices were involved in the process. For example, as of July 2021, 19 of the 20 agencies included in our review had implemented our

[27]GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities,* GAO-20-129 (Washington, D.C.: Oct. 30, 2019).

recommendation to ensure that their acquisition office was involved in the process of identifying IT acquisitions. To their credit, all 20 agencies had issued specific guidance to direct the identification of IT acquisitions. However, as of July 2021, nine agencies had not yet ensured that their CIOs reviewed and approved IT acquisition plans or strategies in accordance with OMB guidance.

Further, as we highlighted in our November 2017 report, CIO involvement in the certification of incremental development also continues to be a focus. For instance, 13 of 17 agencies that lacked adequate incremental development approaches involving their CIOs fully implemented our 2017 recommendations to improve reporting accuracy and update or establish policies.[28] Nonetheless, our work in 2020 found that selected federal agencies could take further action to reduce duplicative IT contracts and reduce the risk of wasteful spending.[29] Until such actions are implemented, agencies could miss opportunities to identify and realize savings of potentially hundreds of millions of dollars.

In summary, longstanding and pervasive weaknesses continue to jeopardize the security and effectiveness of federal agencies' IT and electronic data and the safety of our nation's critical infrastructures. Federal agencies and OMB have taken some important actions; nevertheless, further actions are needed. As of July 2021, federal agencies had fully implemented about 73 percent of the approximately 5,100 recommendations that GAO has made since 2010 in these two high-risk areas. However, about 950 cybersecurity and approximately 300 IT recommendations have not been implemented. Actions are needed on these to successfully address the high-risk areas.

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.

[28]GAO, *Information Technology Reform: Agencies Need to Improve Certification of Incremental Development,* GAO-18-148 (Washington, D.C.: Nov. 7, 2017).

[29]GAO, *Information Technology: Selected Federal Agencies Need to Take Additional Actions to Reduce Contract Duplication,* GAO-20-567 (Washington, D.C.: Sept. 30, 2020).

# 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), Thomas Murphy (Analyst-in-Charge), Chris Businsky, Quintin Dorsey, Donna Epler, Kaelin Kuhn, and Sukhjoot Singh.

## 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/fraudnet/fraudnet.htm

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

## Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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, Acting Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548