



January 2025

CYBERSECURITY WORKFORCE

Departments Need to Fully Implement Key Practices

GAO Highlights

Highlights of [GAO-25-106795](#), a report to congressional addressees

Why GAO Did This Study

Cybersecurity professionals are critical to developing, managing, and protecting the systems that support federal operations. The *Federal Information Security Modernization Act (FISMA) of 2014* includes a provision for GAO to periodically evaluate federal agencies' information security practices. GAO's specific objectives were to (1) determine the extent to which selected departments implemented cybersecurity workforce practices, and (2) describe the selected departments' cybersecurity workforce challenges and mitigation actions and the extent to which they evaluated the effectiveness of those actions. To do so, GAO identified the five federal non-military departments with the largest number of cybersecurity employees. GAO assessed the departments' cybersecurity workforce documentation against applicable leading practices. Further, GAO interviewed officials from the selected departments regarding workforce practices and challenges.

What GAO Recommends

GAO is making a total of 23 recommendations to the five departments--Commerce, Homeland Security, Health and Human Services, Treasury, and Veterans Affairs--to fully implement applicable practices and determine the effectiveness of mitigation actions. Three departments agreed with the recommendations, one agreed with two and partially agreed with three, and one department did not agree or disagree. GAO maintains that all of its recommendations are warranted.

View [GAO-25-106795](#). For more information, contact David Hinchman at (214) 777-5719 or hinchmand@gao.gov.

January 2025

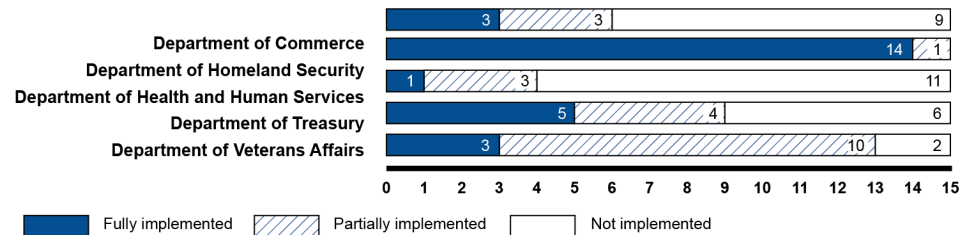
CYBERSECURITY WORKFORCE

Departments Need to Fully Implement Key Practices

What GAO Found

The Office of Personnel Management's (OPM) Workforce Planning Guide outlines a five-step process for workforce planning efforts: (1) setting the strategic direction, (2) conducting workforce analyses, (3) developing workforce action plans, (4) implementing and monitoring workforce planning, and (5) evaluating and revising these efforts. Within the five steps are 15 applicable practices that are central to effectively managing the cybersecurity workforce. Of the 15 applicable practices, the Department of Homeland Security fully implemented 14 of them. However, the other four selected departments were not as consistent in their implementation of the practices (see figure).

Extent to Which Selected Departments Implemented the 15 Applicable Practices for Workforce Planning



Fully implemented = selected departments documentation demonstrated all aspects of the applicable practice.

Partially implemented = selected departments documentation demonstrated some but not all aspects of the applicable practice.

Not implemented = selected departments did not provide any documentation or if documentation was provided it did not demonstrate any aspect of the applicable practice.

Source: GAO analysis of department documentation. | GAO-25-106795

Most of the selected departments reported that they had not fully implemented all 15 practices due, in part, to managing their cybersecurity workforces at the component level rather than the departmental level, as intended by OPM. Until the departments implement these practices, they will likely be challenged in having a cybersecurity workforce with the necessary skills to protect federal IT systems and enable the government's day-to-day functions.

Officials at the five selected departments cited three primary types of cybersecurity workforce management challenges: inadequate funding, difficulties with recruitment, and difficulties with retention. The departments described actions taken to mitigate these challenges. However, none of the departments had evaluated their actions taken to determine the extent to which they had been effective in addressing the challenges. Without evaluating the effectiveness of their mitigation actions, department officials will not know the extent to which their actions are addressing identified challenges and strengthening the cybersecurity workforce.

Contents

Letter		1
	Background	4
	Selected Departments Did Not Fully Implement Applicable Cybersecurity Workforce Management Practices	11
	Most Departments Took Steps to Mitigate Identified Workforce Challenges, but No Departments Evaluated Their Actions	23
	Conclusions	28
	Recommendations for Executive Action	28
	Agency Comments and Our Evaluation	31
Appendix I	Objectives, Scope, and Methodology	36
Appendix II	Comments from the Department of Homeland Security	39
Appendix III	Comments from the Department of Health & Human Services	42
Appendix IV	Comments from the Department of Veterans Affairs	45
Appendix V	Comments from the Department of Treasury	49
Appendix VI	GAO Contact and Staff Acknowledgments	50
Tables		
	Table 1: Office of Personnel Management's (OPM) Workforce Planning Guide Five-Step Process and the 15 Selected Applicable Practices for Cybersecurity Workforce Management	8
	Table 2: Assessment of Five Selected Departments' Implementation of Selected Applicable Practices for Step One: Set Strategic Direction	13

Table 3: Assessment of Five Selected Departments’ Implementation of Selected Applicable Practices for Step Two: Conduct Workforce Analyses	14
Table 4: Assessment of Five Selected Departments’ Implementation of Selected Applicable Practices for Step Three: Develop Workforce Action Plan	17
Table 5: Assessment of Five Selected Departments’ Implementation of Selected Applicable Practices for Step Four: Implement and Monitor the Workforce Action Plan	18
Table 6: Assessment of Five Selected Departments’ Implementation of Selected Applicable Practices for Step Five: Evaluate and Revise the Workforce Action Plan	20
Table 7: Selected Departments’ Reported Cybersecurity Workforce Challenges	23

Figure

Figure 1: Extent to Which Selected Departments Implemented the Practices Within Each of the Five Cybersecurity Workforce Management Steps	12
---	----

Abbreviations

CIO	chief information officer
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
HHS	Department of Health and Human Sciences
MCO	mission critical occupation
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



January 16, 2025

Congressional Addresses

A resilient, skilled, and dedicated cybersecurity workforce is essential to protecting federal IT systems as well as enabling the government’s day-to-day functions.¹ Building and maintaining the cybersecurity workforce is one of the federal government’s most important challenges as well as a national security priority.

Nevertheless, the Office of Management and Budget (OMB) and our prior reports have stated that the federal government faces a persistent shortage of cybersecurity and IT professionals.² For example, in our 2024 High-Risk Series report, we identified four major cybersecurity challenges and 10 critical actions. One of these actions was to address cybersecurity workforce management challenges.³

The *Federal Information Security Modernization Act of 2014* (FISMA) requires federal agencies to develop, document, and implement an information security program to protect the information and systems that support the agencies’ operations and assets.⁴ The act includes a provision for GAO to periodically evaluate federal agencies’ information security policies and practices that are required by FISMA. A key portion

¹For the purposes of this report, we will refer to “cyber” and “cybersecurity” as “cybersecurity” unless otherwise stated.

²Office of Management and Budget, *Federal Cybersecurity Workforce Strategy*, Memorandum M-16-15 (July 12, 2016) and GAO, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, [GAO-19-144](#) (Washington, D.C.: Mar. 12, 2019); and *Cybersecurity Workforce: National Initiative Needs to Better Assess Its Performance*, [GAO-23-105945](#) (Washington, D.C.: Jul. 27, 2023).

³GAO, *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, [GAO-24-107231](#) (Washington, D.C.: Jun. 13, 2024).

⁴The *Federal Information Security Modernization Act of 2014* (FISMA) Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), Title III of Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

of these federal agency-wide cybersecurity programs include evaluating the agencies' cybersecurity workforce management policies.

Our specific objectives were to (1) determine the extent to which selected departments implemented applicable cybersecurity workforce management practices, and (2) describe the cybersecurity workforce management challenges and mitigation actions that selected departments have identified and determine the extent to which departments evaluated the effectiveness of those actions.

For both objectives, we identified the five federal non-military agencies with the largest number of cybersecurity employees based on the Office of Personnel Management's (OPM) Enterprise Human Resources Integration system for fiscal year 2021 data.⁵ Specifically, we identified the five federal agencies with the greatest number of cybersecurity employees assigned to OPM's General Schedule 1550 (Computer Science) and 2210 (Information Technology Management) occupational series codes. According to our prior work and OPM, these codes were the most frequently used for identifying federal cybersecurity professionals.⁶ The five federal non-military departments with the largest number of cybersecurity employees were the Departments of Commerce, Health and Human Services (HHS), Homeland Security (DHS), and Treasury, and Veterans Affairs (VA).

To address the first objective, we identified applicable workforce management practices based on our review of IT and cybersecurity workforce planning and management practices identified in OPM's Workforce Planning Guide and GAO's Key Principles for Effective

⁵The system is a collection of human resources payroll and training data, and the information in it is used to provide human resource and demographic information on each federal civilian employee. Executive Order 13197 empowers OPM to collect the personnel data in the system.

⁶The General Schedule classification and pay system covers the majority of civilian white-collar federal employees (about 1.5 million worldwide) in professional, technical, administrative, and clerical positions. General Schedule classification standards, qualifications, pay structure, and related human resources policies (e.g., general staffing and pay administration policies) are administered by OPM on a government-wide basis. Each agency classifies its General Schedule positions and appoints and pays its General Schedule employees filling those positions by following statutory and OPM guidelines. GAO, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, [GAO-19-144](#) (Washington, D.C.: Mar. 12, 2019).

Strategic Workforce Planning.⁷ OPM's Workforce Planning Guide outlines a continuous five-step process for (1) setting the strategic direction, (2) conducting a workforce analyses, (3) developing the workforce action plan, (4) implementing and monitoring the workforce action plan, and (5) evaluating and revising the workforce action plan. In addition, GAO's Key Principles for Effective Strategic Workforce Planning includes a framework for developing, communicating, and implementing strategic workforce planning.

We analyzed these documents and the five-step process, and selected 15 practices from both documents that can be categorized as supporting federal cybersecurity workforce management.⁸ We selected practices that were applicable to effective management of the workforce, including whether the selected departments had workforce strategic plans and action plans in place; conducted workforce analyses; and implemented, monitored, evaluated, and revised the workforce action plans.

We reviewed department-level cybersecurity workforce management documentation from the five selected departments, including workforce planning policies and procedures, strategic plans, cybersecurity workforce documents, and staffing performance metrics. We compared the documentation to the 15 selected applicable practices. We then determined whether the five selected departments had fully implemented, partially implemented, or not implemented each of the 15 applicable practices.⁹

To address the second objective, we conducted interviews with relevant officials from the five selected departments and asked department officials for documentation on their identified challenges with managing their cybersecurity workforce. We then compiled a list of cybersecurity

⁷Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: November 2022) and GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, [GAO-04-39](#) (Washington, D.C.: Dec. 11, 2003).

⁸We tailored OPM's Workforce Planning Guide applicable practices to be specific to our scope in reviewing the cybersecurity workforce.

⁹*Fully implemented* = selected departments' documentation demonstrated all aspects of the applicable practice; *partially implemented* = selected departments' documentation demonstrated some, but not all, aspects of the applicable practice; and *not implemented* = selected departments did not provide any documentation or if documentation was provided it did not demonstrate any aspect of the applicable practice.

workforce management challenges identified by the five selected departments and grouped them into three primary types of challenges.

Further, we determined the extent to which the five selected departments had identified actions to mitigate their challenges through those interviews and document reviews. We then determined the extent to which the selected departments had evaluated the effectiveness of their mitigation actions by comparing them to practices identified in OPM's Workforce Planning Guide and GAO's prior work for measuring workforce performance.¹⁰ We supplemented our analyses with interviews of staff from the five selected departments who performed various IT, cybersecurity-related, and human capital functions. For more information on our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from April 2023 to January 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Congress has enacted various laws, and OPM and the National Institute of Standards and Technology (NIST) have issued guidance, that called for departments and agencies to implement workforce planning processes. These processes are essential for ensuring that federal departments and agencies have the talent, skills, and experience mix they need to execute their missions and program goals, including strengthening their departments' cybersecurity workforce. For example:

- The Clinger-Cohen Act of 1996 required agency chief information officers (CIO) to annually perform workforce-related tasks, such as develop strategies and specific plans for hiring, training, and professional development to address any workforce knowledge and skill gaps.¹¹
- The E-Government Act of 2002 required the Director of OPM, in consultation with the Director of OMB, the CIO Council, and the Administrator of General Services to, among other things, analyze the

¹⁰Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: November 2022) and [GAO-04-39](#).

¹¹Pub. L. No. 104-106, § 5125(c)(3) (Feb. 10, 1996), codified at 40 U.S.C. § 11315(c)(3).

personnel needs of the federal government related to IT and information resource management.¹²

- FISMA requires agencies to develop, document, and implement agency-wide information security programs to protect their IT systems.¹³ The act also requires agencies to submit reports on their information security programs to OMB, DHS, GAO, and Congress. As directed by OMB, these reports are to include the metrics that the agencies used to assess their progress toward outcomes intended to strengthen federal cybersecurity. FISMA also included provisions for GAO to periodically evaluate federal agencies' information security policies and practices. Additionally, GAO is to evaluate agencies' implementation of FISMA requirements, which include having sufficient personnel to carry out their responsibilities.
- The Federal Cybersecurity Workforce Assessment Act of 2015 required OPM, with support from the NIST, to establish a coding structure to be used in identifying all federal civilian and non-civilian positions that require the performance of IT, cybersecurity, or other cybersecurity-related functions.¹⁴ The act also required agencies, in consultation with OPM and NIST, to then use this coding structure to annually assess, among other things, the IT, cybersecurity, and other cybersecurity-related work roles of critical need in their workforce.¹⁵
- In November 2020, NIST released an updated version of its Workforce Framework for Cybersecurity.¹⁶ This guide included a common lexicon that categorizes and describes cybersecurity-related work roles and functions. The framework is intended to improve

¹²Pub. L. No. 107-347, § 209(b) (Dec. 17, 2002), 44 U.S.C. § 3501 note.

¹³The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 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 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

¹⁴Federal Cybersecurity Workforce Assessment Act of 2015, Pub. L. No. 114-113, Div. N, Title III (Dec. 18, 2015). 5 U.S.C. § 301 note.

¹⁵Fiscal year 2022 was the final year that OPM required agencies to submit these mission critical occupation documents.

¹⁶National Institute of Standards and Technology, *Workforce Framework for Cybersecurity, (NICE Framework)*, Special Publication 800-181 revision 1 (Gaithersburg, MD: November 2020). This version replaced an earlier version that was published in August 2017. See <https://csrc.nist.gov/pubs/sp/800/181/r1/final>.

communication about how to identify, recruit, develop, and retain cyber talent.

- In November 2022, OPM published a Workforce Planning Guide as a resource for federal agency leaders and employees to use for planning and analyzing their workforce, identifying gaps, as well as implementing workforce action planning efforts.¹⁷ Among other things, the Workforce Planning Guide detailed a continuous workforce process for identifying the size and composition of a workforce needed to achieve an organization's goals and objectives.
- In February 2024, OPM published a Workforce of the Future playbook to enunciate the specific actions agencies could take to provide the foundation for the workforce of the future.¹⁸ The Playbook was organized based on three pillars: inclusive, agile and engaged, and having the right skills. OPM, in partnership with its stakeholders, identified areas in the Playbook, that if strengthened, would enable federal agencies to adapt effectively to the rapidly evolving nature of work and to keep pace with other industries.

OPM Established a Cyber Workforce Dashboard

In addition to its Workforce Planning Guide and Workforce of the Future Playbook, OPM created the Cyber Workforce Dashboard to support departments in cybersecurity workforce planning efforts and in making data-driven decisions regarding current and future cybersecurity workforce requirements. Specifically, in April 2023, OPM launched its web-based Cyber Workforce Dashboard. The dashboard contained two viewing options: one for agency use and one for public use. OPM officials stated that the dashboard's data comes from OPM's Enterprise Human Resources Integration system and annual data calls made to the departments.¹⁹

¹⁷Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: November 2022).

¹⁸Office of Personnel Management, *Workforce of the Future: Playbook for Implementing Strategies to Enable a Federal Workforce that is Inclusive, Agile and Engaged, with the Right Skills to Enable Mission Delivery* (Washington, D.C.: February 2024).

¹⁹OPM's Enterprise Human Resources Integration system includes some legislative branch entities, the U.S. Tax Court, and most executive branch departments. It does not include the Board of Governors of the Federal Reserve System, Central Intelligence Agency, Defense Intelligence Agency, Foreign Service personnel at the State Department, National Geospatial-Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, Office of the Vice President, Postal Regulatory Commission, Tennessee Valley Authority, U.S. Postal Service, and White House Office.

According to officials from OPM's Office of Strategic Workforce Planning, the dashboard version for agencies displayed work roles, hiring trends, workforce demographics, staffing gaps, and mission critical occupations. In addition, agencies could use the dashboard to track work role metrics, such as separations, compare data to benchmarks and other agencies, and review demographic information and hiring targets specific to each agency. The dashboard for the public allowed the user to view data across the federal departments, such as demographic trends and comparisons, the top 10 cybersecurity occupations, retirement eligibility, and separations.

Selected Workforce Management Practices Are Key to Effective Cybersecurity Management

Workforce planning processes are essential for ensuring that federal agencies have the talent, skills, and experience mix they need to execute their missions and achieve program goals. OPM's Workforce Planning Guide outlines a continuous five-step process for (1) setting the strategic direction, (2) conducting workforce analyses, (3) developing the workforce action plan, (4) implementing and monitoring the workforce action plan, and (5) evaluating and revising the workforce action plan.²⁰ OPM officials stated that workforce planning is intended to be managed at the department level.

In addition, GAO's Key Principles for Effective Strategic Workforce Planning includes a framework for developing, communicating, and implementing strategic workforce planning.²¹ Within the five primary steps are 15 selected applicable practices from OPM's Workforce Planning Guide that are central to effectively managing the cybersecurity workforce.²² GAO's workforce planning guidance further supports and complements these practices.²³ Table 1 describes the 15 selected applicable practices for the cybersecurity workforce.

²⁰Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: November 2022).

²¹[GAO-04-39](#).

²²Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: November 2022).

²³[GAO-04-39](#).

Table 1: Office of Personnel Management’s (OPM) Workforce Planning Guide Five-Step Process and the 15 Selected Applicable Practices for Cybersecurity Workforce Management

Cybersecurity workforce management step	Description	Selected applicable practices
Step 1: Set Strategic Direction	Understanding the agency’s cybersecurity strategy and related performance plans, and involving top management, employees, and other stakeholders in workforce planning.	<p>1.1 Develop a strategy that describes the agency’s cybersecurity goals and mission and identifies anticipated changes in the cybersecurity landscape over the next 3-5 years.</p> <p>1.2 Establish a governance process that involves top management, employees, and other stakeholders in developing, communicating, and implementing the strategic workforce plan.</p>
Step 2: Conduct Workforce Analyses	Analyzing the agency’s cybersecurity workforce, identifying skill gaps, and conducting workforce analyses.	<p>2.1 Conduct workforce analyses to forecast demand, and identify the skills and competencies needed to meet future organizational demands.</p> <p>2.2 Conduct workforce analyses to forecast supply including current staffing levels, skills, and competencies; and anticipated recruitments, attrition, retirements, and separations.</p> <p>2.3 Identify the cybersecurity mission critical occupations to help ensure that the agency has the resources and talent it needs to function successfully.</p> <p>2.4 Conduct cybersecurity gap and risk analyses that evaluate the gap between supply and demand and analyze current and future workforce risks.</p>
Step 3: Develop Workforce Action Plan	Identifying strategies to close workforce gaps, implementing those strategies, and assessing progress.	<p>3.1 Develop a cybersecurity workforce plan that identifies current and future human capital needs, skills, and competencies.</p> <p>3.2 Develop a cybersecurity workforce plan that includes strategies to close the cybersecurity gaps, such as recruiting, training, retraining, restructuring, use of contractors, succession planning, and technological enhancements.</p> <p>3.3 Develop a cybersecurity workforce action plan with metrics to evaluate success and achievement of desired results.</p>
Step 4: Implement and Monitor Workforce Action Plan	Ensuring human and fiscal resources are in place, roles are understood, and the necessary communication, education, change management, and coordination are occurring; and monitoring progress against milestones.	<p>4.1 Communicate the cybersecurity workforce action plan to the agency’s leadership; and plan and implement a communication strategy that defines roles, resources, and achievement of strategic objectives.</p> <p>4.2 Develop a plan that describes how implementation will occur, including information on key deliverables, timelines, responsibilities, and needed resources.</p>

Cybersecurity workforce management step	Description	Selected applicable practices
Step 5: Evaluate and Revise Workforce Action Plan	Assessing continuous improvement, adjusting the cybersecurity workforce action plan to make course corrections, and addressing new workforce issues.	<p data-bbox="1003 491 1500 621">4.3 Implement and monitor the cybersecurity workforce action plan, including tracking information on the milestones, metrics, and targets from the cybersecurity workforce action plan.</p> <p data-bbox="1003 636 1500 741">5.1 Assess the effectiveness and efficiency of the cybersecurity workforce action plan and the progress made against its targets, baselines, outcomes, and performance measures.</p> <p data-bbox="1003 751 1500 856">5.2 Record actions taken, review lessons learned from the cybersecurity workforce action plan, and update or adjust metrics and targets as necessary.</p> <p data-bbox="1003 867 1500 947">5.3 Conduct an analysis of the extent to which cybersecurity workforce strategic objectives are being achieved.</p>

Source: GAO analysis of cybersecurity workforce management practices identified in OPM's Workforce Planning Guide and GAO's Key Principles for Effective Strategic Workforce Planning. | GAO-25-106795.

GAO Has Previously Reported on Challenges to Effective Federal IT Workforce Planning

We have previously reported on federal workforce planning.

- In October 2019, we reported that federal agencies varied widely in their efforts to implement key IT workforce planning activities that were critical to ensuring that agencies have the staff they need to support their missions.²⁴ We noted that while agencies took important steps towards identifying their workforces, most agencies had not fully implemented the key IT workforce activities. Agencies limited implementation of the IT workforce planning activities was due, in part, to not making IT workforce planning a priority.

Accordingly, we made 18 recommendations directing 18 of the 24 federal agencies to fully implement the eight key IT workforce planning activities. As of January 2025, agencies have fully implemented 16 of the recommendations and partially implemented two.

- In July 2022, we reported on workforce recruitment and retention processes, leading practices, and challenges at the Department of

²⁴GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, [GAO-20-129](#) (Washington, D.C.: Oct. 30, 2019).

State.²⁵ Specifically, we evaluated 15 recruitment and retention practices and determined that State fully implemented one, partially implemented 11, and did not implement three. For example, we reported that State had collected training performance data, but did not recruit continuously year-round for most of its IT positions or regularly assessed staffing needs. We also identified challenges related to State recruiting and retaining its IT workforce, including (1) low entry-level pay and no recruiting incentives, (2) long hiring and security clearance process, (3) inaccurate position descriptions that did not accurately reflect actual IT job responsibilities, and (4) limited promotions.

We noted that State addressed some of its IT workforce challenges, but the department had not monitored and evaluated those actions to determine whether they have been effective in addressing the recruitment and retention challenges. Accordingly, we made 16 recommendations to improve State's IT workforce management. As of January 2025, one of the recommendations has been implemented.

- In September 2022, we reported on the Coast Guard's implementation of workforce management leading practices.²⁶ Of the 12 selected recruitment, retention, and training leading practices, the Coast Guard fully implemented seven, partially implemented three, and did not implement two. For example, it leveraged available hiring incentives such as recruiting bonuses, relocation expenses, and student loan repayments. However, it had not developed a strategic workforce plan for its cyberspace workforce. Accordingly, we made six recommendations to the Coast Guard, including to determine the cyberspace staff needed to meet its mission demands and fully implement five recruitment and retention leading practices, such as establishing a strategic workforce plan for its cyberspace workforce. Coast Guard concurred with these recommendations. Coast Guard stated it is actively working to address each recommendation and has provided us updates. However, as of January 2025, we have not received evidence to close the recommendations.
- In our June 2024 high-risk update report, we stated that it was critical for the federal government to address cybersecurity workforce management challenges to help ensure it has a highly-skilled

²⁵GAO, *State Department: Additional Actions Needed to Address IT Workforce Challenges*, [GAO-22-105932](#) (Washington, D.C.: July 12, 2022).

²⁶GAO, *Coast Guard: Workforce Planning Action Needed to Address Growing Cyberspace Mission Demands*, [GAO-22-105208](#) (Washington, D.C.: Sept. 27, 2022).

workforce, which is essential to a functioning government.²⁷ For example, we reported that federal agencies could strengthen cybersecurity by establishing and effectively implementing a comprehensive national cyber strategy and a government-wide cyber workforce plan. We also reported that while federal agencies had made progress in improving their cybersecurity workforce practices, they needed to take additional action to address challenges in hiring, training, and retaining their cybersecurity workforces.

**Selected
Departments Did Not
Fully Implement
Applicable
Cybersecurity
Workforce
Management
Practices**

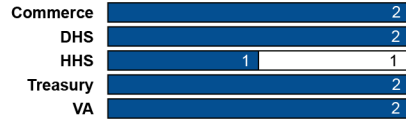
Of the 15 applicable practices, DHS fully implemented 14 of them. However, the other four departments were not as consistent in their implementation of the practices.

Figure 1 summarizes the extent to which the five selected departments implemented the practices within each of the five steps.

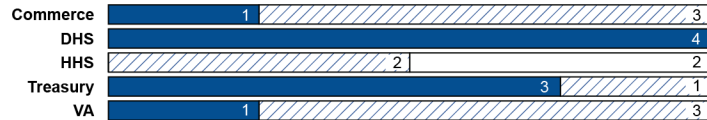
²⁷GAO, *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, [GAO-24-107231](#) (Washington, D.C.: Jun. 13, 2024).

Figure 1: Extent to Which Selected Departments Implemented the Practices Within Each of the Five Cybersecurity Workforce Management Steps

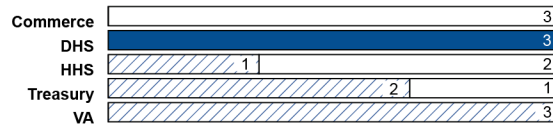
Step 1 - Set the strategic direction for the cyber workforce



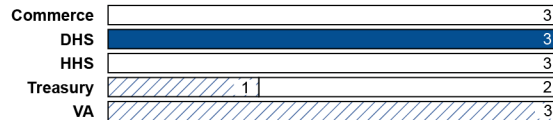
Step 2 - Analyze the cyber workforce, identify skill gaps, and conduct analysis



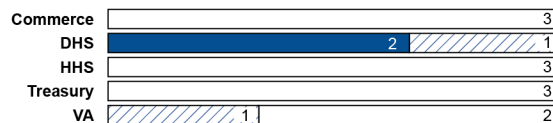
Step 3 - Develop the cyber workforce action plan



Step 4 - Implement and monitor the cyber workforce action plan



Step 5 - Evaluate and revise the cyber workforce action plan



Fully implemented = selected departments documentation demonstrated all aspects of the applicable practice.
 Partially implemented = selected departments documentation demonstrated some but not all aspects of the applicable practice.

Not implemented = selected departments did not provide any documentation or if documentation was provided it did not demonstrate any aspect of the applicable practice.

Commerce = Department of Commerce, DHS = Department of Homeland Security, HHS = Department of Health and Human Services, Treasury = Department of the Treasury, VA = Department of Veterans Affairs

Source: GAO analysis of department documentation. | GAO-25-106795

Departments Largely Set the Strategic Direction

Almost all of the selected departments provided documentation that set the stage for the strategic direction of their cybersecurity workforces.

Table 2 provides a detailed assessment of the completeness of departments' efforts to set the strategic direction for their cybersecurity workforces.

Table 2: Assessment of Five Selected Departments' Implementation of Selected Applicable Practices for Step One: Set Strategic Direction

Department	Rating	GAO assessment
Practice 1.1: Develop a strategy that describes the agency's cybersecurity goals and mission and identifies anticipated changes in the cybersecurity landscape over the next 3-5 years.		
Commerce	●	Commerce provided a 5-year strategic plan, a 3-year cybersecurity strategy, and a technical statement of direction that described the department's cybersecurity goals and mission. The plan also identified anticipated changes to the department's cybersecurity landscape.
Department of Homeland Security (DHS)	●	DHS provided a 5-year department level IT strategic plan that described the department's cybersecurity goals and mission. The plan also identified anticipated changes to the department's cybersecurity landscape.
Department of Health and Human Services (HHS)	●	HHS provided a 5-year department level strategic plan and a 3-year IT strategic plan that addressed the department's cybersecurity activities and described its goals and mission. The plan also identified anticipated changes to the department's cybersecurity landscape.
Treasury	●	Treasury provided a 5-year department level strategic plan and a 5-year human capital operating plan that described the department's cybersecurity goals and mission. The plan also identified anticipated changes to the department's cybersecurity landscape.
Department of Veterans Affairs (VA)	●	VA provided a 5-year IT workforce plan that described the department's cybersecurity goals and mission. The plan also identified anticipated changes to the department's cybersecurity landscape.
Practice 1.2: Establish a governance process that involves top management, employees, and other stakeholders in developing, communicating, and implementing the strategic workforce plan.		
Commerce	●	Commerce provided a cybersecurity workforce strategy and a technical statement of direction that described the department's governance process that involved top management, employees, and other stakeholders in developing, communicating, and implementing the strategic workforce plan.
DHS	●	DHS provided a department-level cybersecurity workforce strategy and a department-level cybersecurity implementation plan that described the department's governance process that involved top management, employees, and other stakeholders in developing, communicating, and implementing the strategic workforce plan.
HHS	○	While HHS provided an IT strategic plan and a department level strategic plan, the documentation did not describe the department's governance process nor described how it involved top management, employees, and other stakeholders in developing, communicating, and implementing the strategic workforce plan.
Treasury	●	Treasury provided a human capital operating plan, a strategic workforce planning policy, and a strategic workforce planning guide that described the department's governance process that involved top management, employees, and other stakeholders in developing, communicating, and implementing the strategic workforce plan.
VA	●	VA provided workforce charters and directives that described the department's governance process that involved top management, employees, and other stakeholders in developing, communicating, and implementing the strategic workforce plan.

Legend: ● Fully implemented = departments' documentation demonstrated all aspects of the selected applicable practices;

- Partially implemented = departments' documentation demonstrated some, but not all, aspects of the selected applicable practices;
- Not implemented = departments did not provide any documentation, or if documentation was provided, it did not demonstrate any aspect of the selected applicable practices.

Source: GAO analysis of department IT workforce planning policies and documentation. | GAO-25-106795

Most Departments Partially Conducted Workforce Analyses

DHS fully implemented all four applicable practices, but the other four departments did not. Specifically:

- Treasury fully implemented three practices,
- Commerce fully implemented one practice,
- VA fully implemented one practice, and
- HHS partially implemented two practices.

Table 3 provides a detailed assessment of the completeness of departments' efforts to conduct workforce analyses.

Table 3: Assessment of Five Selected Departments' Implementation of Selected Applicable Practices for Step Two: Conduct Workforce Analyses

Department	Rating	GAO assessment
Practice 2.1: Conduct workforce analyses to forecast demand, identify the skills and competencies needed to meet future organizational demands.		
Commerce	●	Commerce provided some documentation on workforce analysis to forecast demand, including identification of some skills and competencies needed. However, this documentation did not detail what the department's current cybersecurity workforce looked like, nor its optimal workforce capability to meet its future workforce demands.
Department of Homeland Security (DHS)	●	DHS provided documentation of a cybersecurity workforce analysis to forecast its demand, specifically for the department's cybersecurity work roles of critical need, including the skills and competencies needed to meet the department's future organizational demands.
Department of Health and Human Services (HHS)	○	HHS did not provide documentation of a workforce analysis to forecast demand.
Treasury	●	Treasury provided a workforce demand analysis to forecast the department's future workforce needs based on the Office of Personnel Management occupational codes. However, the analysis did not identify specific skills and competencies needed to meet the department's future organizational demands.
Department of Veterans Affairs (VA)	●	VA provided documentation including VA's Office of Information Technology strategic workforce plan, that included an analysis to forecast its demand. It also included information related to the skills and competencies needed to meet the department's future organizational demands.

Department	Rating	GAO assessment
------------	--------	----------------

Practice 2.2: Conduct workforce analyses to forecast supply including current staffing levels, skills, and competencies; and anticipated recruitments, attrition, retirements, and separations.

Commerce	⦿	Commerce provided some documentation of a cybersecurity workforce analysis to forecast the department's workforce supply including the full-time equivalent shortages for its roles of critical need, specifically the type and numbers of employees. However, this documentation did not describe the department's current cybersecurity supply including current staffing levels, skills, and competencies, anticipated recruitments, attrition, retirements, and separations. Commerce officials stated succession planning assessments were conducted to review high-risk leadership positions and to identify potential employees to ensure the department had a pipeline of candidates to backfill IT and cybersecurity positions. While Commerce officials stated the department had a succession planning strategy and assessment that identified critical positions, talent pipeline, workforce strengths, weakness, and future needed competencies, the strategy was in draft.
DHS	●	DHS provided documentation of a cybersecurity workforce analysis to forecast the department's workforce supply, including current staffing levels, skills, and competencies; and anticipated recruitments, attrition, retirements, and separations, specifically for its cybersecurity work roles of critical need.
HHS	⦿	HHS provided some documentation of a cybersecurity workforce analysis to forecast the department's workforce supply including mission critical occupations and 2210 occupational series. While this presentation included specific metrics such as retirement eligibility and new hire, retention, and attrition rates, it did not include details on the department's current cybersecurity workforce including staffing levels, skills, and competencies. It also did not include information about the department's recruitments and separations.
Treasury	●	Treasury provided evidence of conducting a cybersecurity workforce analysis to forecast the department's supply, including anticipated recruitments, retirements, and current staffing levels. Treasury officials provided an analysis of the department's current cybersecurity occupational series staffing levels, skills distribution, and attrition rates, as well as a report that discussed the department's 2210 occupational series retirements.
VA	⦿	VA provided the department's Office of Information and Technology strategic workforce plan, which identified the current staffing levels, anticipated supply, and impacts to anticipated supply for its mission critical occupations. However, this plan did not contain any discussion of the department's current workforce skills and competencies.

Practice 2.3: Identify the cybersecurity mission critical occupations to help ensure that the agency has the resources and talent it needs to function successfully.

Commerce	●	Commerce provided documentation regarding the department's cybersecurity work roles of critical need for mission critical occupations to help ensure that it has the resources and talent it needs to function successfully. This documentation included progress metrics using fiscal year 2018 as a baseline to target the number of fiscal years 2019 to 2023 resources.
DHS	●	DHS provided documentation that identified its cybersecurity mission critical occupations to help ensure the department had the resources and talent it needed to function successfully.
HHS	⦿	HHS provided some documentation regarding its cybersecurity mission critical occupations, including metrics for its 2210 occupational series. However, this documentation lacked a discussion of the department's cybersecurity resources and talent needed to function successfully.
Treasury	●	Treasury provided a human capital operating plan for fiscal years 2022 to 2026 that identified mission critical occupations to help ensure that the department has the resources and talent it needs to function successfully.
VA	⦿	VA provided a human capital operating plan and the department's Office of Information and Technology strategic workforce plan, which identified some, but not complete information regarding its cybersecurity mission critical occupations projections, such as type, number, and location of employees.

Department	Rating	GAO assessment
Practice 2.4: Conduct cybersecurity gap and risk analyses that evaluate the gap between supply and demand and analyze current and future workforce risks.		
Commerce	⦿	Commerce provided documentation describing the department's full-time equivalent shortages based on roles of critical need, specifically the type and numbers of employees. However, this documentation did not describe the department's current cybersecurity workforces' skills, competencies, or gaps in workforce supply and demand. The documentation also lacked an analysis of current and future workforce risks.
DHS	●	DHS conducted a cybersecurity gap and risk analyses that evaluated the gap between supply and demand and analyzed current and future workforce risks.
HHS	○	HHS did not provide documentation of a cybersecurity gap and risk analysis, a discussion of the gaps between the department's current workforce supply and projected demand, nor current and future workforce risks.
Treasury	●	Treasury conducted a cybersecurity gap and risk analyses that evaluated the gap between supply and demand and analyzed current and future workforce risks.
VA	⦿	VA provided an Office of Information and Technology strategic workforce plan that provided some information related to the department's gaps in current and projected workforce needs, as well as current and future workforce risks. However, VA's demand and supply analyses were incomplete, including the department's analysis of workforce gaps.

Legend: ● Fully implemented = departments' documentation demonstrated all aspects of the selected applicable practices;
 ⦿ Partially implemented = departments' documentation demonstrated some, but not all, aspects of the selected applicable practices;
 ○ Not implemented = departments did not provide any documentation, or if documentation was provided, it did not demonstrate any aspect of the selected applicable practices.

Source: GAO analysis of department IT workforce planning policies and documentation. | GAO-25-106795

Most Departments Did Not Fully Develop Workforce Action Plans

DHS implemented all three applicable practices, but the other four departments did not. Specifically:

- VA partially implemented three practices,
- Treasury partially implemented two practices,
- HHS partially implemented one practice, and
- Commerce did not implement any practices.

Table 4 provides a detailed assessment of the completeness of departments' efforts to develop their workforce action plans.

Table 4: Assessment of Five Selected Departments’ Implementation of Selected Applicable Practices for Step Three: Develop Workforce Action Plan

Department	Rating	GAO assessment
Practice 3.1: Develop a cybersecurity workforce plan that identifies current and future human capital needs, skills, and competencies.		
Commerce	○	Commerce did not provide a cybersecurity workforce plan that identified the department’s current and future human capital needs, skills, and competencies. Commerce provided documentation that described the department’s shortages in roles of critical need, specifically, the type and numbers of employees; however, this analysis was incomplete in that it did not comprehensively identify the department’s current and future human capital needs, skills, and competencies.
Department of Homeland Security (DHS)	●	DHS provided a cybersecurity workforce action plan that identified the department’s current and future human capital needs, skills, and competencies. In addition, DHS provided an implementation plan supporting its cybersecurity workforce action plan, as well as DHS’s cyber workforce strategy that was shared with Congress.
Department of Health and Human Services (HHS)	○	HHS did not provide a cybersecurity workforce plan that identified the department’s current and future human capital needs, skills, and competencies.
Treasury	◐	Treasury provided some information regarding the department’s current and future human capital needs as it related to its IT and cybersecurity mission critical occupations. The information was limited to the department’s current and future skills and competencies.
Department of Veterans Affairs (VA)	◐	VA provided the VA Office of Information Technology Strategic Workforce Plan, for fiscal years 2024 to 2028. However, the department’s analysis was incomplete in that it did not comprehensively identify VA’s current and future human capital needs, skills, and competencies.
Practice 3.2: Develop a cybersecurity workforce plan that includes strategies to close the cybersecurity gaps, such as recruiting, training, retraining, restructuring, use of contractors, succession planning, and technological enhancements.		
Commerce	○	Commerce did not provide a cybersecurity workforce action plan that included strategies to close cybersecurity gaps, such as recruiting, training, retraining, restructuring, use of contractors, succession planning, and technological enhancements.
DHS	●	DHS provided a cybersecurity workforce implementation plan and an annual report on cybersecurity work roles of critical need, including strategies to close cybersecurity gaps, such as recruiting, training, and retention incentives.
HHS	◐	HHS provided some documentation of recruiting and retention incentive strategies intended to address cybersecurity workforce gaps, such as using hiring flexibilities and student loan repayment. However, HHS did not provide a cybersecurity workforce action plan that included strategies to close cybersecurity gaps, such as recruiting, training, retraining, restructuring, use of contractors, succession planning, and technological enhancements.
Treasury	○	Treasury did not provide a cybersecurity workforce action plan that included strategies to close cybersecurity gaps, such as recruiting, training, retraining, restructuring, use of contractors, succession planning, and technological enhancements.
VA	◐	VA provided its Office of Information and Technology strategic workforce plan that mentioned strategies to close cybersecurity gaps such as the use of special salary rate, ⁹ a succession planning program, and an apprenticeship program. The plan also referenced participation in the Cyber NextGen Development Program. However, the plan did not include details regarding the strategies listed.
Practice 3.3: Develop a cybersecurity workforce action plan with metrics to evaluate success and achievement of desired results.		
Commerce	○	Commerce did not have a cybersecurity action plan with metrics to evaluate success and achievement of desired results.

Department	Rating	GAO assessment
DHS	●	DHS provided a cybersecurity workforce implementation plan and an annual report on cyber work roles of critical need with workforce metrics to evaluate success and achievement of desired results.
HHS	○	HHS did not have a cybersecurity action plan with metrics to evaluate success and achievement of desired results.
Treasury	◐	Treasury provided some cybersecurity workforce metrics to evaluate success, such as baseline and target attrition rates and average time to hire. The documentation was not specifically dedicated to Treasury's cybersecurity workforce; it targeted mission critical occupations, which included IT and cybersecurity-related occupational series. However, these metrics were only projected for 1 year (fiscal year 2024).
VA	◐	VA provided documentation that included some cybersecurity metrics to evaluate success and achievement of desired results such as time to hire, executive fill rates, and retention rates. VA used milestones to monitor its achievement of workforce goals; however, the department did not provide any other workforce metrics.

Legend: ● Fully implemented = departments' documentation demonstrated all aspects of the selected applicable practices;

◐ Partially implemented = departments' documentation demonstrated some, but not all, aspects of the selected applicable practices;

○ Not implemented = departments did not provide any documentation, or if documentation was provided, it did not demonstrate any aspect of the selected applicable practices.

Source: GAO analysis of department IT workforce planning policies and documentation. | GAO-25-106795

^aThe Special Salary Rate is paid to VA employees in General Schedule (GS) positions at grades GS-5 to GS-15 across the 2210, 1550, and 0854 occupational series, unless an employee is entitled to receive a higher GS locality rate of pay.

Most Departments Did Not Fully Implement and Monitor Action Plans

DHS implemented all three applicable practices, but the other four departments did not. Specifically:

- VA partially implemented three practices;
- Treasury partially implemented once practice; and
- Commerce and HHS did not implement any practices.

Table 5 provides a detailed assessment of the completeness of departments' efforts to implement and monitor their workforce action plans.

Table 5: Assessment of Five Selected Departments' Implementation of Selected Applicable Practices for Step Four: Implement and Monitor the Workforce Action Plan

Department	Rating	GAO assessment
Practice 4.1: Communicate the cybersecurity workforce action plan to the agency's leadership; plan and implement a communication strategy that defines roles, resources, and achievement of strategic objectives.		
Commerce	○	Commerce did not provide documentation of communicating a cybersecurity workforce action plan to the department's leadership. Commerce officials also did not provide a plan and implement a communication strategy that defined roles, resources, and achievement of strategic objectives.

Department	Rating	GAO assessment
Department of Homeland Security (DHS)	●	DHS communicated the cybersecurity workforce action plan to the department's leadership; and planned and implemented a communication strategy that defined roles, resources, and achievement of strategic objectives.
Department of Health and Human Services (HHS)	○	HHS did not provide documentation of communicating a cybersecurity workforce action plan to the department's leadership. HHS officials also did not provide a plan and implement a communication strategy that defined roles, resources, and achievement of strategic objectives.
Treasury	●	Treasury provided some documentation of communicating cybersecurity workforce planning to the department's leadership. Specifically, Treasury provided a human capital operating plan that included some evidence of communicating and coordinating roles including those for the department's mission critical occupations such as IT and cybersecurity-related occupational series. Treasury did not provide a plan and implement a communication strategy that defined roles, resources, and achievement of strategic objectives.
Department of Veterans Affairs (VA)	●	VA provided some documentation of communicating cybersecurity workforce action planning to the department's leadership. Specifically, VA provided an Office of Information and Technology strategic workforce plan that included documentation regarding workforce communication. VA did not provide a plan and implement a communication strategy that defined roles, resources, and achievement of strategic objectives.
Practice 4.2: Develop a plan that describes how implementation will occur, including information on key deliverables, timelines, responsibilities, and needed resources.		
Commerce	○	Commerce did not develop a plan that described how implementation will occur, including information on key deliverables, timelines, responsibilities, and needed resources.
DHS	●	DHS provided a cybersecurity workforce implementation plan and described how implementation will occur, including information on key deliverables, timelines, responsibilities, and needed resources.
HHS	○	HHS did not develop a plan that described how implementation will occur, including information on key deliverables, timelines, responsibilities, and needed resources.
Treasury	○	Treasury did not develop a plan that described how implementation will occur, including information on key deliverables, timelines, responsibilities, and needed resources.
VA	●	VA provided documentation that discussed implementation of the agency's workforce activities; however, this documentation did not describe how VA would implement its cybersecurity workforce action plan, including key deliverables, timelines, responsibilities, and needed resources.
Practice 4.3: Implement and monitor the cybersecurity workforce action plan, including discussing the plan at the department dashboards and includes information on how the milestones, metrics, and targets from the cybersecurity workforce action plan are being tracked.		
Commerce	○	Commerce did not implement and monitor the cybersecurity workforce action plan, including discussing the plan at the department dashboards nor included information on how the milestones, metrics, and targets from the cybersecurity workforce action plan were being tracked.
DHS	●	DHS implemented and monitored the cybersecurity workforce action plan, including discussing the plan at the department dashboards and included information on how the milestones, metrics, and targets from the cybersecurity workforce action plan were being tracked.
HHS	○	HHS did not implement and monitor the cybersecurity workforce action plan, including discussing the plan at the department dashboards nor included information on how the milestones, metrics, and targets from the cybersecurity workforce action plan were being tracked.
Treasury	○	Treasury did not implement and monitor the cybersecurity workforce action plan, including discussing the plan at the department dashboards nor included information on how the milestones, metrics, and targets from the cybersecurity workforce action plan were being tracked.

Department	Rating	GAO assessment
VA	●	VA provided documentation that discussed the workforce status at the department's dashboards. The information included discussions on milestones, metrics, and targets for the workforce. However, the department did not provide evidence of it implementing and monitoring the cybersecurity workforce action plan.

Legend: ● Fully implemented = departments' documentation demonstrated all aspects of the applicable practice;
 ● Partially implemented = departments' documentation demonstrated some, but not all, aspects of the applicable practice;
 ○ Not implemented = departments did not provide any documentation, or if documentation was provided, it did not demonstrate any aspect of the applicable practice.

Source: GAO analysis of department IT workforce planning policies and documentation. | GAO-25-106795

Departments Did Not Fully Evaluate and Revise Action Plans

None of the five selected departments fully evaluated and revised their cybersecurity workforce action plans. Specifically, of the three applicable practices:

- DHS fully implemented two practices;
- VA partially implemented one practice; and
- Commerce, HHS, and Treasury did not fully implement any practices.

Table 6 provides a detailed assessment of the completeness of departments' efforts to evaluate and revise their workforce action plans.

Table 6: Assessment of Five Selected Departments' Implementation of Selected Applicable Practices for Step Five: Evaluate and Revise the Workforce Action Plan

Department	Rating	GAO assessment
Practice 5.1: Assess the effectiveness and efficiency of the cybersecurity workforce action plan and the progress made against its targets, baselines, outcomes, and performance measures.		
Commerce	○	Commerce did not assess the effectiveness and efficiency of the cybersecurity workforce action plan and the progress made against its targets, baselines, outcomes, and performance measures.
Department of Homeland Security (DHS)	●	DHS assessed the effectiveness and efficiency of the cybersecurity workforce action plan and the progress made against its targets, baselines, outcomes, and performance measures.
Department of Health and Human Services (HHS)	○	HHS did not assess the effectiveness and efficiency of the cybersecurity workforce action plan and the progress made against its targets, baselines, outcomes, and performance measures.
Treasury	○	Treasury did not assess the effectiveness and efficiency of the cybersecurity workforce action plan and the progress made against its targets, baselines, outcomes, and performance measures.
Department of Veterans Affairs (VA)	○	VA did not assess the effectiveness and efficiency of the cybersecurity workforce action plan and the progress made against its targets, baselines, outcomes, and performance measures.

Department	Rating	GAO assessment
Practice 5.2: Record actions taken, review lessons learned from its cybersecurity workforce action plan, and update or adjust metrics and targets as necessary.		
Commerce	○	Commerce did not record actions taken, review lessons learned from its cybersecurity workforce action plan, nor update or adjust metrics and targets as necessary.
DHS	●	DHS provided documentation of actions taken from its cybersecurity workforce action plan, and updated metrics and targets, specifically, for its cybersecurity work roles of need. However, the documentation did not include evidence of reviewing lessons learned.
HHS	○	HHS did not record actions taken, review lessons learned from its cybersecurity workforce action plan, nor update or adjust metrics and targets as necessary.
Treasury	○	Treasury did not record actions taken, review lessons learned from its cybersecurity workforce action plan, nor update or adjust metrics and targets as necessary.
VA	○	VA did not record actions taken, review lessons learned from its cybersecurity workforce action plan, nor update or adjust metrics and targets as necessary.
Practice 5.3: Conduct an analysis of the extent to which cybersecurity workforce strategic objectives are being achieved.		
Commerce	○	Commerce did not conduct an analysis of the extent to which cybersecurity workforce strategic objectives were being achieved.
DHS	●	DHS conducted an analysis of the extent to which cybersecurity workforce strategic objectives were being achieved.
HHS	○	HHS did not conduct an analysis of the extent to which cybersecurity workforce strategic objectives were being achieved.
Treasury	○	Treasury did not conduct an analysis of the extent to which cybersecurity workforce strategic objectives were being achieved.
VA	●	VA provided some analyses documentation of the extent to which its cybersecurity workforce strategic objectives were being achieved; however, it was limited in scope to analyzing employee retention concerns.

Legend: ● Fully implemented = departments' documentation demonstrated all aspects of the applicable practice;
 ● Partially implemented = departments' documentation demonstrated some, but not all, aspects of the applicable practice;
 ○ Not implemented = departments did not provide any documentation, or if documentation was provided, it did not demonstrate any aspect of the applicable practice.

Source: GAO analysis of department information technology workforce planning policies and documentation. | GAO-25-106795

According to officials at three of the five selected departments, they did not fully implement the selected practices because they were managing their cybersecurity workforces at the individual component level rather than at departmental level. Selected departments noted other reasons for not fully implementing the selected applicable practices.

- **Commerce.** According to Commerce officials, the department did not have a departmental-led cybersecurity workforce governance, instead, each individual Commerce components' Chief Information Security Officer was responsible for the planning and analysis of the component's cybersecurity workforces. In addition, according to Commerce officials, given the timing of this review, the department

was not able to issue a data call in which all of its individual components were able to support an overall departmental response.

- **DHS.** According to DHS officials, their review revealed a gap between specialty operational workforce planning and overarching DHS cybersecurity workforce planning. DHS officials also stated that the department was committed to working with key stakeholders to identify lessons learned and affirm the overarching cybersecurity workforce action plan.
- **HHS.** HHS officials stated that while the department followed OPM's guidance to implement workforce planning processes, it did not have a strategic plan specifically for the department's cybersecurity activities. HHS officials also stated a department-level cybersecurity workforce management strategic plan and business plan would be developed in 2024.
- **Treasury.** Treasury officials stated the department's workforce strategy was decentralized and individually handled by the department's individual components. Treasury officials also stated that Treasury's recruitment gap size and retention rate did not warrant a gap closure strategy, action plan, and implementation plan.
- **VA.** VA officials stated that while the department's Office of Information Technology developed several workforce-related documents, a specific cybersecurity workforce strategy had yet to be developed. VA officials add that they have taken the opportunity to use the insight provided in the OPM guide to assist in the creation of a new VA Workforce Strategy, which is intended to identify goals surrounding talent acquisition, workforce planning, competencies, and collaboration with other departments. VA completed this strategy in October 2024, and we updated our analysis accordingly; however, several workforce planning practices were still not fully implemented.

Until the departments implement all the selected applicable practices for their cybersecurity workforces, they will be challenged in having cybersecurity workforces with the necessary skills to protect federal IT systems and enable the government's day-to-day functions.

Most Departments Took Steps to Mitigate Identified Workforce Challenges, but No Departments Evaluated Their Actions

Officials at the five selected departments cited three primary types of cybersecurity workforce management challenges: inadequate funding, difficulties with recruitment, and challenges with retention. Within these three primary types, officials identified six specific challenges. Each of these was reported by at least two departments. To mitigate these challenges, department officials described actions, both underway and planned. However, none of the departments evaluated their actions to determine whether they were effective in addressing their cybersecurity workforce management challenges.

Selected Departments Identified Cybersecurity Workforce Challenges

Table 7 shows the three key types and six specific cybersecurity workforce challenges identified by department officials:

Table 7: Selected Departments' Reported Cybersecurity Workforce Challenges

Challenge type	Departments				
	Commerce	DHS	HHS	Treasury	VA
Inadequate funding for the cybersecurity workforce					
Pay disparity between federal agencies and the private sector	✓	✓	✓	✓	✓
Department budget limitations	X	✓	✓	✓	✓
Difficulties with recruiting the cybersecurity workforce					
Maintaining an adequate cybersecurity workforce	✓	✓	X	X	✓
Cybersecurity workforce candidates	✓	✓	✓	✓	X
Recruiting processing	✓	✓	✓	X	✓
Challenges with retaining the cybersecurity workforce					
High attrition due to cybersecurity employees choosing different career paths	✓	X	✓	X	X
Totals challenges by departments	5	5	5	3	4

Legend: ✓ = Department faced challenge; X = Department did not face challenge

Source: GAO analysis of department documentation. | GAO-25-106795

Inadequate Funding for the Cybersecurity Workforce

Officials from all five departments stated they faced challenges in inadequate funding for their cybersecurity workforces.

- Commerce, DHS, HHS, Treasury, and VA reported that **pay disparity between federal agencies and the private sector** was a challenge.

Many of the departments stated that it was difficult to recruit and retain employees, especially highly qualified candidates. For instance, staff from VA reported that existing salaries within certain geographic regions were not competitive with private sector salaries, even when combined with VA's compensation incentives and benefits.

- Staff from DHS, HHS, Treasury, and VA noted that **department cybersecurity workforce budget limitations** caused recruiting and retention complications.

Difficulties with Recruiting the Cybersecurity Workforce

Officials from all five selected departments stated that their departments faced difficulties with recruiting their cybersecurity workforces.

- Officials at Commerce, DHS, and VA stated it was **difficult to maintain an adequate cybersecurity workforce**. For example, Commerce reported that it experienced a shortage of cybersecurity workforce personnel, specifically for its 2210 Information Technology series positions.
- Officials at Commerce, DHS, HHS, and Treasury stated they had **difficulties with recruiting cybersecurity workforce candidates**. For example, DHS reported that since COVID-19, open cybersecurity position announcements for its U.S. Secret Service component no longer generated enough well-qualified applicants, thus resulting in a decreased talent pool of qualified cybersecurity candidates.
- Officials at Commerce, DHS, HHS, and VA stated that they experienced difficulties with **recruitment processing**. For example, VA reported that the lengthy time-to-hire cybersecurity personnel for vacant positions impacted its overall ability to deliver products and services.

Challenges with Retaining the Cybersecurity Workforce

Officials from all five selected departments stated that their departments faced difficulties with retaining their cybersecurity workforces. Specifically:

- Officials at Commerce and HHS reported challenges with **high attrition due to cybersecurity employees choosing different career paths**. For example, Commerce noted that cybersecurity employees would leave the department to choose a different career path or a job closer to home. HHS reported that cybersecurity trained staff were able to easily move through the federal government due to their essential skillset.

Selected Departments Took Actions to Mitigate Cybersecurity Workforce Challenges

Officials from all five selected departments stated that their departments identified mitigating actions to address each of the three cybersecurity workforce challenge types.

Inadequate Funding for the Cybersecurity Workforce

Officials from all five of the selected departments developed mitigation actions in response to their challenges with inadequate funding for their cybersecurity workforces. The following provides key examples:

- In response to the **pay disparity between the federal agencies and the private sector**, officials from the selected departments described mitigating actions. For example, Commerce officials reported that the department temporarily promoted employees in its competitive service and leveraged various authorities to hire cybersecurity professionals for special projects. Officials at DHS and HHS stated that their departments offered incentives such as student loan repayment. DHS officials also noted that the department offered market-sensitive pay for cybersecurity personnel. HHS officials stated the department offered higher starting salaries based on superior skills and qualifications. Treasury officials stated the department offered cash awards to cybersecurity personnel. VA officials stated the department offered special salary rates for IT and cybersecurity personnel.
- To address department **cybersecurity workforce funding and budget limitations**, officials from the selected departments described mitigating actions. For example, DHS reported that the U.S. Secret Service used all available hiring authorities, including special hiring authority and veteran hiring authority. DHS officials stated the department contracted support to assist with recruitment and retention activities. HHS officials stated the department provided human resources support and funding for additional human resources personnel. Treasury officials stated the department created workforce demand projections beyond the time frames of the current budget cycle to be better prepared for its future workforce needs.

Difficulties with Recruiting the Cybersecurity Workforce

Officials from selected departments developed mitigation actions in response to their challenges with difficulties recruiting their cybersecurity workforces. The following provides key examples:

- To address the **difficulty of maintaining an adequate cybersecurity workforce**, officials from the selected departments described mitigating actions. For example, Commerce officials stated the department planned to leverage various hiring authorities to hire cybersecurity professionals for special projects and considered using

special salary rates for the 2210 occupational series positions to expand its cybersecurity workforce. DHS officials reported the department's U.S. Secret Service component used all available hiring authorities, including special hiring authority and veteran hiring authority. VA officials reported that the department's Office of People Science continuously updated and analyzed VA personnel recruitment data to identify obstacles to recruiting and addressed delays to reduce the overall time to hire.

- To address **difficulties with recruiting cybersecurity workforce candidates**, officials from the selected departments described mitigating actions. For example, Commerce officials reported the department expanded the talent pool for its cybersecurity workforce positions to include both internal and external candidates. DHS reported that U.S. Secret Service used, in addition to addressing this challenge through contracted support, all available hiring authorities, including special hiring authority and veteran hiring authority. HHS officials noted the department used the federal government's Pathways Program to hire recent IT graduates for the department's cybersecurity positions, in addition to participation in the Office of Personnel Management's Tech to Gov recruitment events. Treasury officials reported that the department dedicated \$1.1 million dollars for talent outreach to recruit for cybersecurity roles and other occupations.
- With respect to **recruitment processing** issues, officials from the selected departments described mitigating actions. For example, Commerce officials reported the department launched an 80-day time-to-hire dashboard that allowed managers to track how long it took the department to onboard IT employees. DHS officials reported that the department used its Cybersecurity Talent Management System (CTMS) for dissemination of broad recruiting announcements rather than posting for specific positions. HHS officials reported the department addressed recruitment processing challenges by using direct hire authority, a focus on reducing the amount of time it took to obtain security clearances, identification of efficiencies to process candidates requesting pay based on superior qualifications, and implementation of a workforce planning center of practice. VA officials reported that the department's Office of People Science continuously updated and analyzed personnel recruitment data to identify obstacles to recruiting and addressed delays to reduce the department's overall time to hire.

Challenges with Retaining the Cybersecurity Workforce

Officials from all five of the selected departments developed mitigation actions in response to their challenges with retaining their cybersecurity workforces. The following provides key examples:

- In response to the **higher attrition due to cybersecurity employees choosing different career paths**, officials from the selected departments described mitigating actions. For example, Commerce officials stated that the department offered temporary promotions with pay increase, opportunities for details across Commerce, and training opportunities. HHS officials stated that the department implemented a department-wide detail program and planned to provide HHS cybersecurity personnel with 6-month to 1-year rotations in cybersecurity positions in other departments.

None of the Selected Departments Evaluated the Effectiveness of their Mitigation Actions

OPM's Workforce Planning Guide and Model emphasizes that agencies should develop, monitor, evaluate, and revise a workforce action plan.²⁸ Further, our report on key principles of strategic workforce planning noted that periodic measurement of an agency's progress toward human capital goals and the extent of human capital activities provides information for identifying performance shortfalls.²⁹ Our report also stated workforce planning should be done at the departmental level.

However, none of the five selected departments evaluated the effectiveness of their mitigation actions in response to the identified workforce challenges. Officials from HHS, Treasury, and VA reported that they had not evaluated the effectiveness of their efforts. Commerce officials reported that the department monitors the effectiveness of its actions to respond to cyber workforce challenges but did not provide evidence to support these assertions. DHS officials reported that they plan to develop a strategy to measure the effectiveness of their efforts but did not provide a plan or time frame for doing so.

Without evaluating the effectiveness of their mitigation actions, agencies will not know the extent to which their actions are addressing challenges and helping to meet cybersecurity workforce goals.

²⁸Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: November 2022), and Office of Personnel Management, *Workforce Planning Model*, accessed on October 11, 2024, <https://www.opm.gov/policy-data-oversight/human-capital-framework/reference-materials/talent-management/workforce-planning-guide.pdf>

²⁹GAO-04-39.

Conclusions

Building and maintaining a cybersecurity workforce by addressing mission critical skills gaps is one of the federal government's most important challenges, as well as a national security priority. While DHS fully implemented almost all selected leading workforce management practices, the other four reviewed departments fully implemented less than half. Addressing these practices from a department-level perspective can help ensure that their cybersecurity workforces have the necessary skills and capabilities to protect federal IT systems and enable the government's day-to-day functions.

Selected departments have proactively identified challenges and implemented mitigation strategies and associated actions to strengthen their cybersecurity workforces. However, because the departments have not evaluated the effectiveness of their actions, officials do not know the extent to which their departments' cybersecurity workforce issues have been addressed and their cybersecurity postures have been strengthened.

Recommendations for Executive Action

We are making a total of 23 recommendations to the five selected departments.

The Secretary of Commerce should ensure that the Department of Commerce fully addresses the practices described in our report associated with conducting workforce analyses. (Recommendation 1)

The Secretary of Commerce should ensure that the Department of Commerce fully addresses the practices described in our report associated with developing a workforce action plan. (Recommendation 2)

The Secretary of Commerce should ensure that the Department of Commerce fully addresses the practices described in our report associated with implementing and monitoring a workforce action plan. (Recommendation 3)

The Secretary of Commerce should ensure that the Department of Commerce fully addresses the practices described in our report associated with evaluating and revising a workforce action plan. (Recommendation 4)

The Secretary of Commerce should ensure that the Department of Commerce identify and analyze the effectiveness of its mitigation actions on the cybersecurity workforce challenges. (Recommendation 5)

The Secretary of Homeland Security should ensure that the Department of Homeland Security fully addresses the practices described in our report associated with evaluating and revising a workforce action plan. (Recommendation 6)

The Secretary of Homeland Security should ensure that the Department of Homeland Security identify and analyze the effectiveness of its mitigation actions on the workforce challenges. (Recommendation 7)

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully addresses the practices described in our report associated with setting the strategic direction for the cybersecurity workforce. (Recommendation 8)

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully addresses the practices described in our report associated with conducting workforce analyses. (Recommendation 9)

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully addresses the practices described in our report associated with developing a workforce action plan. (Recommendation 10)

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully addresses the practices described in our report associated with implementing and monitoring a workforce action plan. (Recommendation 11)

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully addresses the practices described in our report associated with evaluating and revising a workforce action plan. (Recommendation 12)

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services identify and analyze the effectiveness of its mitigation actions on the cybersecurity workforce challenges. (Recommendation 13)

The Secretary of the Treasury should ensure that the Department of the Treasury fully addresses the practices described in our report associated with conducting workforce analyses. (Recommendation 14)

The Secretary of the Treasury should ensure that the Department of the Treasury fully addresses the practices described in our report associated with developing a workforce action plan. (Recommendation 15)

The Secretary of the Treasury should ensure that the Department of the Treasury fully addresses the practices described in our report associated with implementing and monitoring a workforce action plan. (Recommendation 16)

The Secretary of the Treasury should ensure that the Department of the Treasury fully addresses the practices described in our report associated with evaluating and revising a workforce action plan. (Recommendation 17)

The Secretary of the Treasury should ensure that the Department of the Treasury identify and analyze the effectiveness of its mitigation actions on the cybersecurity workforce challenges. (Recommendation 18)

The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs fully addresses the practices described in our report associated with conducting workforce analyses. (Recommendation 19)

The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs fully addresses the practices described in our report associated with developing a workforce action plan. (Recommendation 20)

The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs fully addresses the practices described in our report associated with implementing and monitoring a workforce action plan. (Recommendation 21)

The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs fully addresses the practices described in our report associated with evaluating and revising a workforce action plan. (Recommendation 22)

The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs identify and analyze the effectiveness of its mitigation actions on the cybersecurity workforce challenges. (Recommendation 23)

Agency Comments and Our Evaluation

We provided a draft of this report to Commerce, DHS, HHS, Treasury, VA, and OPM, for their review and comment. Of the five departments to which we made recommendations, three departments (Commerce, DHS, and HHS) agreed with their recommendations, one department (VA) agreed with two and partially agreed with three recommendations, and one department (Treasury) neither agreed or disagreed with our recommendations. We did not make any recommendations to OPM and it did not state whether it agreed or disagreed with our report. We also received technical comments from DHS, OPM, and VA, which we have incorporated into the report as appropriate.

The following three departments agreed with our recommendations:

- In comments provided via email on December 17, 2024, Commerce's Internal Controls Officer from the Office of Business and Administrative Services, Office of the Chief Information Officer stated that the department agreed with our five recommendations. The officer stated that the department has begun preparing a formal action plan to specifically address noted shortcomings.
- In written comments, reprinted in appendix II, DHS agreed with our two recommendations and described the steps planned to address them. Specifically, DHS stated that it will (1) develop metrics to evaluate its Cybersecurity Workforce Strategy's effectiveness in supporting the department's cybersecurity hiring and retention efforts and (2) conduct a lessons learned assessment. DHS estimated a completion date of June and September 2025, respectively, for these efforts.
- In written comments, reprinted in appendix III, HHS agreed with our six recommendations and described the steps planned to address them. For example, HHS stated that it had efforts underway placing additional focus on its cyber workforce, including conducting a cybersecurity workforce analysis and updating future HHS strategic plans.

As noted above, VA agreed with two and partially agreed with three of our recommendations:

- In written comments, reprinted in appendix IV, VA agreed with recommendation 20, to fully address the practices associated with developing a workforce action plan described in our report. VA stated that its Office of Information Technology continues to actively implement the steps outlined in OPM's Workforce Planning Guide. VA

expects to complete a full workforce analysis of all of its Office of Information Technology's organizations by December 31, 2026.

- VA also agreed with recommendation 23, to identify and analyze the effectiveness of its mitigation actions on cybersecurity workforce challenges. VA stated that it used a method to evaluate the effectiveness of the efforts to mitigate challenges and provided a score to inform its Office of Information Technology if the analysis and mitigation strategies were appropriately aligned on an annual basis. VA also provided the workforce analysis data collection template, documentation that it had not previously provided to us. Although VA requested closure of this recommendation based on these assertions, we reviewed the documentation provided and determined that it did not fully satisfy our recommendation. Specifically, we could not determine how this documentation is used to track VA's cybersecurity challenges and the effectiveness of its mitigation actions in response to these challenges. The recommendation remains open and we will continue to monitor VA's efforts to address it.
- VA partially agreed with recommendation 19, to fully address the practices described in our report associated with conducting workforce analyses. VA stated that it agreed with portions of the recommendation related to three of the four workforce practices we found lacking. However, VA noted that it did not agree with the portion of the recommendation related to the practice of conducting workforce analyses to forecast supply. VA said that its Office of Information Technology managed the totality of the department's cybersecurity workforce analysis and all but 2 percent of its IT positions are in that office. VA further asserted that the Office of Information Technology completed a competency assessment that was included in the department's 2024 Succession Implementation Plan. However, the department did not provide the 2024 Succession Implementation Plan. We will assess the plan once the department provides it and close the recommendation if warranted.
- VA partially agreed with recommendation 21, to fully address the practices described in our report associated with implementing and monitoring a workforce action plan. The department stated that it agreed with portions of the recommendation related to two of the three workforce practices we found lacking. However, VA said that it did not agree with the portion of the recommendation related to the workforce practice of implementing and monitoring the cybersecurity workforce action plan.

VA provided evidence to support partial implementation of this practice with its participation in the department's workforce progress update

meetings and supporting documentation, which it had not previously provided to us. In addition, the department asserted these documents showed that it had a process for evaluating its action plans that included responsible parties, milestones, timeline, resources, potential barriers, and solution strategies to include baseline and targets. Based on our review of this new documentation, we changed VA's assessment rating in our report to partially implemented, as it relates to the practice of implementing and monitoring the cybersecurity workforce action plan. The new documents provided evidence of discussing the workforce status at the department dashboards. However, the department did not provide evidence of a cybersecurity workforce action plan. Thus, we believe our recommendation is valid.

- Finally, VA partially agreed with recommendation 22, to fully address the practices described in our report associated with evaluating and revising a workforce action plan. VA noted that it agreed with the portion of the recommendation related to the workforce practice of conducting an analysis of the extent to which cybersecurity workforce strategic objectives were being achieved. However, the department did not agree with the portions of the recommendation related to the other two workforce practices we found lacking. Specifically, VA did not agree with our evaluation of the practice related to assessing the effectiveness and efficiency of the cybersecurity workforce action plan. The department also did not agree with the practice related to recording actions taken and reviewing lessons learned from the cybersecurity workforce action plan.


VA noted that it provided evidence to support partial implementation of these two practices. The department pointed to its previously-provided Strategic Workforce Plan as well as new documentation supporting workforce progress update meetings. VA added that it had an evaluation process for quarterly workforce progress update meetings that included providing feedback on milestones, metrics, targets, and whether there was a need to extend the initiative. We will review the new documentation and follow up with the department to determine the extent to which this recommendation has been implemented.

The Department of Treasury did not state whether it agreed or disagreed with our recommendations. In written comments, reprinted in appendix V, Treasury stated that it supports our objectives to determine the extent to which agencies implemented applicable cybersecurity workforce practices and the assessment of those practices. The department noted that it uses workforce planning processes to identify workforce gaps as required in its Strategic Workforce Planning Program Policy. Treasury also asserted that it continues to monitor and assess the cyber workforce for gaps impacting

agency strategic objectives and will adjust agency strategies and/or workforce planning activities as determined by leadership and available agency resources. We will follow-up on Treasury's actions to determine the extent to which it has implemented the recommendations.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Commerce, Health and Human Services, Homeland Security, Treasury, and Veterans Affairs; and other interested parties. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at 214-777-5719 or at hinchmand@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.

A handwritten signature in black ink that reads "David B Hinchman". The signature is written in a cursive, flowing style with a long horizontal flourish at the end.

David B. Hinchman
Director, Information Technology and Cybersecurity

List of Addresses

The Honorable Rand Paul, M.D.
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable James Comer
Chairman
The Honorable Gerald E. Connolly
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Mark E. Green, M.D.
Chairman
Committee on Homeland Security
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our specific objectives were to (1) determine the extent to which selected departments implemented applicable cybersecurity workforce management practices, and (2) describe the cybersecurity workforce management challenges and mitigation actions that selected departments have identified and determine the extent to which departments evaluated the effectiveness of those actions.

For both objectives, we identified the five federal non-military agencies with the largest number of cybersecurity employees based on Office of Personnel Management's (OPM) Enterprise Human Resources Integration system for fiscal year 2021 data.¹ Specifically, we identified five federal agencies with the greatest number of cybersecurity employees assigned to OPM's General Schedule 1550 (Computer Science) and 2210 (Information Technology Management) occupational series codes. According to our prior work and OPM, these codes were the most frequently used for identifying federal cybersecurity professionals.² The five federal non-military agencies with the largest number of cybersecurity employees were the Departments of Commerce, Health and Human Services, Homeland Security, the Treasury, and Veterans Affairs.

To address the first objective, we identified applicable workforce management practices based on our review of IT and cybersecurity workforce planning and management practices identified in OPM's Workforce Planning Guide and GAO's Key Principles for Effective Strategic Workforce Planning.³ OPM's Workforce Planning Guide outlines a continuous five-step process for (1) setting the strategic direction, (2) conducting workforce analyses, (3) developing the workforce action plan, (4) implementing and monitoring workforce action plan, and (5) evaluating

¹The system is a collection of human resources, payroll, and training data, and the information in it is used to provide human resource and demographic information on each federal civilian employee. Executive Order 13197 empowers OPM to collect the personnel data in the system.

²The General Schedule classification and pay system covers the majority of civilian white-collar federal employees (about 1.5 million worldwide) in professional, technical, administrative, and clerical positions. General Schedule classification standards, qualifications, pay structure, and related human resources policies (e.g., general staffing and pay administration policies) are administered by OPM on a government-wide basis. Each agency classifies its General Schedule positions and appoints and pays its General Schedule employees filling those positions following statutory and OPM guidelines.

³Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: November 2022) and GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, [GAO-04-39](#) (Washington, D.C.: Dec. 11, 2003).

and revising the workforce action plan. In addition, GAO's Key Principles for Effective Strategic Workforce Planning includes a framework for designing, developing, and implementing strategic workforce planning.

We analyzed these documents and the five steps and selected 15 practices from both documents that can be categorized as supporting federal cybersecurity workforce management.⁴ While the OPM Workforce Planning Guide included many different workforce practices, we selected the most important practices that were applicable to our review.⁵ We selected practices that were related to effective management of the workforce, including whether agencies had workforce strategic plans and action plans in place, analyzed their workforce capabilities, and maintained workforce metrics, among others. We supplemented the practices with GAO's Key Principles for Effective Strategic Workforce Planning.⁶

We reviewed department-level cybersecurity workforce management practice documentation from the five selected departments, including workforce planning policies and procedures, strategic plans, cybersecurity workforce documents, and staffing performance metrics, and compared them to the 15 selected applicable practices. We determined whether the five selected departments had fully implemented, partially implemented, or not implemented each of the 15 selected applicable practices.⁷ We provided the selected applicable practices and our assessment to officials from the five selected departments for their review and incorporated their comments in our assessment, as appropriate.

To address the second objective, we conducted interviews with relevant officials from the five selected departments, and reviewed department documentation to identify information on challenges the selected departments faced in managing their cybersecurity workforces. We met

⁴We tailored OPM's *Workforce Planning Guide* applicable practices to be specific to our scope in reviewing the cybersecurity workforce.

⁵Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: November 2022).

⁶[GAO-04-39](#).

⁷*Fully implemented* = selected departments' documentation demonstrated all aspects of the applicable practice; *partially implemented* = selected departments' documentation demonstrated some but not all aspects of the applicable practice; and *not implemented* = selected departments did not provide any documentation or if documentation was provided it did not demonstrate any aspect of the applicable practice.

with officials from the selected departments and from these interviews, supplemented by written documentation, developed a list of cybersecurity workforce management challenges identified by the five selected departments and grouped them into three primary types of challenges that were experienced by at least two of the selected departments.

Further, we determined the extent to which the five selected departments had identified actions to mitigate their challenges through those interviews and document reviews. We then determined the extent to which the selected departments had evaluated the effectiveness of their mitigation actions by comparing their efforts to practices identified in OPM's Workforce Planning Guide and GAO's prior work for measuring workforce performance.⁸

We supplemented our analyses with interviews of staff from the five selected departments who performed various IT, cybersecurity-related, and human capital functions. Specifically, we conducted interviews with relevant department-level human capital management officials and IT staff at department headquarters to obtain perspectives on the cybersecurity workforce environment, processes, challenges, and mitigating actions to address those challenges.

We conducted this performance audit from April 2023 to January 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

⁸Office of Personnel Management, *Workforce Planning Guide* (Washington D.C.: November 2022), and Office of Personnel Management, *Workforce Planning Model*, accessed on March 13, 2024, <https://www.opm.gov/reference-materials/strategic-alignment/workforceplanning.pdf>, and GAO-04-39.

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

BY ELECTRONIC SUBMISSION

December 18, 2024

David B. Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-25-106795, "CYBERSECURITY WORKFORCE: Departments Need to Fully Implement Key Practices"

Dear Mr. Hinchman:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's positive recognition that the Department fully implemented 14 of 15 recommended practices identified by the U.S. Office of Personnel Management's (OPM) Workforce Planning Guide as being central to the effective management of the cybersecurity workforce. The Department remains committed to developing, managing, and protecting the systems that support the Department's mission and operations, such as through creation of the DHS Information Technology (IT) Strategic Plan for fiscal years (FY) 2024 – 2028,¹ which describes the Department's cybersecurity goals and mission, including investments in the DHS IT Workforce as well as identifies anticipated changes to the Department's cybersecurity landscape. DHS also created a Cybersecurity Workforce Strategy² that formalizes the Department's workforce strategy efforts pursuant to the Cybersecurity Workforce Assessment Act (Public Law 113-246),³ and conducted an analysis forecasting the likely demand for the DHS

¹ "DHS Information Technology Strategic Plan FY 2024-2028," dated September 26, 2023; <https://www.dhs.gov/publication/dhs-information-technology-strategic-plan-2024-2028>.

² "DHS Cybersecurity Workforce Strategy" <https://acrobat.adobe.com/id/urn:aaid:sc:VA6C2:87a5e3bf-4448-488f-a93c-88d2da4d461f>

³ The Cybersecurity Workforce Assessment Act (Public Law 113-246), enacted on December 18, 2014, mandates that the Secretary of Homeland Security evaluate the Department's cybersecurity workforce and formulate a comprehensive strategy to enhance its readiness, capacity, training, recruitment, and retention.

**Appendix II: Comments from the Department
of Homeland Security**

cybersecurity work roles of critical need, what skills and competencies the workforce requires to meet the Department's future organizational needs.

The draft report contained 23 recommendations, including two for DHS with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration, as appropriate.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER Digitally signed by JIM H
CRUMPACKER
Date: 2024.12.18 17:14:34 -05'00'

JIM H. CRUMPACKER
Director
Departmental GAO-OIG Liaison Office

Enclosure

**Enclosure: Management Response to Recommendations
Contained in GAO-25-106795**

GAO recommended that the Secretary of Homeland Security:

Recommendation 6: Ensure that the Department of Homeland Security fully addresses the practices described in our report associated with evaluating and revising a workforce action plan.

Response: Concur. The DHS Office of the Chief Information Officer (OCIO), Business Management Directorate (BMD), in collaboration with personnel from the DHS Office of the Chief Human Capital Officer (OCHCO), the Cybersecurity and Infrastructure Security Agency (CISA), and other DHS Components, as needed, will develop metrics to evaluate the DHS Cybersecurity Workforce Strategy's effectiveness in supporting DHS cybersecurity hiring and retention efforts. This will include outlining a plan to obtain the metrics and assess results in a written report that will be available to DHS and OPM stakeholders, as appropriate, and include will include next steps and recommendations for improvements identified by this effort. Estimated Completion Date (ECD): June 30, 2025.

Recommendation 7: Ensure that the Department of Homeland Security identify and analyze the effectiveness of its mitigation actions on the workforce challenges.

Response: Concur. DHS OCIO BMD, in collaboration with personnel from DHS OCHCO, CISA, and other DHS Components, as needed, will conduct a lessons learned assessment to determine the effectiveness of the Cybersecurity Workforce Strategy in mitigating workforce challenges. Specifically, this effort will include determining effectiveness of mitigation actions in meeting each of the Cybersecurity Workforce Strategy goals based on the metrics developed in the Cybersecurity Workforce Strategy. Further, DHS OCHCO will develop and provide a lessons-learned report to DHS Stakeholders and OPM that includes recommendations for improvements. ECD: September 30, 2025.

Appendix III: Comments from the Department of Health & Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

December 16, 2024

David B. Hinchman
Director, Information Technology and
Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Hinchman:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "**CYBERSECURITY WORKFORCE: Departments Need to Fully Implement Key Practices**" (GAO-25-106795).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Melanie Anne Egorin

Melanie Anne Egorin, PhD
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH AND HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – CYBERSECURITY WORKFORCE: DEPARTMENTS NEED TO FULLY IMPLEMENT KEY PRACTICES (GAO-25-106795)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

Recommendation 8

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully addresses the practices described in our report associated with setting the strategic direction for the cybersecurity workforce.

HHS Response

HHS concurs with GAO's recommendation. Previously, HHS developed an IT strategic plan for fiscal years 2021 to 2023 and a department-level strategic plan for fiscal years 2022 to 2026 that discussed objectives and goals to optimize the workforce. While HHS currently does not have a strategic plan that focuses solely on cyber security, HHS had other efforts underway to that will place additional focus on the cyber workforce. For example, HHS is conducting a cybersecurity workforce analysis. HHS can use this information, as well as other information it is collecting and analyzing, to update and augment future strategic plans and related documents.

For this and all other recommendations directed to HHS, HHS will provide further updates to GAO when HHS responds to the GAO final report.

Recommendation 9

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully addresses the practices described in our report associated with conducting workforce analyses.

HHS Response

HHS concurs with GAO's recommendation. As briefly described in the update to recommendation 8, HHS is continuing efforts to conduct a cybersecurity workforce analysis and will work to incorporate and address practices referenced in the GAO report.

Recommendation 10

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully addresses the practices described in our report associated with developing a workforce action plan.

HHS Response

HHS concurs with GAO's recommendation. HHS is continuing efforts to develop a workforce action plan and will work to incorporate and address the practices referenced in the GAO report.

Recommendation 11

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully addresses the practices described in our report associated with implementing and monitoring a workforce action plan.

**Appendix III: Comments from the Department
of Health & Human Services**

HHS Response

HHS concurs with GAO's recommendation. HHS is continuing efforts to develop a workforce action plan. HHS uses various existing mechanisms to evaluate and revise plans and will expand and augment those mechanisms to address this GAO recommendation.

Recommendation 12

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services fully addresses the practices described in our report associated with evaluating and revising a workforce action plan.

HHS Response

HHS concurs with GAO's recommendation. HHS is continuing efforts to develop a workforce action plan. HHS uses various existing mechanisms to evaluate and revise plans and will expand and augment those mechanisms to address this GAO recommendation.

Recommendation 13

The Secretary of Health and Human Services should ensure that the Department of Health and Human Services identify and analyze the effectiveness of its mitigation actions on the cybersecurity workforce challenges

HHS Response

HHS concurs with GAO's recommendation. HHS uses various existing mechanisms to evaluate and revise workforce challenges and will expand and augment those mechanisms to address this GAO recommendation.

Appendix IV: Comments from the Department of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

December 20, 2024

Mr. David B. Hinchman
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Hinchman:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report, **CYBERSECURITY WORKFORCE: Departments Need to Fully Implement Key Practices** (GAO-25-106795).

The enclosure contains a technical comment and the action plan to implement the draft report recommendations. VA appreciates the opportunity to comment on your draft report.

Sincerely,

A handwritten signature in black ink that reads "Margaret B. Kabat".

Margaret Kabat, LCSW-C, CCM
Chief of Staff

Enclosure

**Appendix IV: Comments from the Department
of Veterans Affairs**

Enclosure

Department of Veterans Affairs (VA) Comments to the
Government Accountability Office (GAO) Draft Report
Cybersecurity Workforce: Departments Need to Fully Implement Key Practices
(GAO-25-106795)

Recommendation 1: The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs fully addresses the practices described in our report associated with conducting workforce analyses. (Recommendation 19).

VA Response: Partially concur. The Department of Veterans Affairs (VA) concurs with GAO's assessment of the Department for Practices 2.1, 2.3, and 2.4. VA non-concurs with GAO's assessment of the Department for Practices 2.2, as outlined below:

Practice 2.2: "Conduct workforce analyses to forecast supply including current staffing levels, skills, and competencies; and anticipated recruitments, attrition, retirements, and separations."

Non-concur. VA notes that the Office of Information Technology (OIT) manages the totality of the Department's cybersecurity workforce analysis, because all information technology positions reside in OIT except for a limited number (approximately 100, or less than 2%). OIT completed a competency assessment in the 2024 Succession Implementation Plan inclusive of cybersecurity positions at an aggregate-level. VA has fully implemented the practice.

Recommendation 2: The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs fully addresses the practices described in our report associated with developing a workforce action plan. (Recommendation 20).

VA Response: Concur. OIT concurs with GAO's assessment of the Department for Practices 3.1-3.3. OIT continues to actively implement the steps in the Office of Personnel Management (OPM) Workforce Planning Guide. OIT initiated full implementation of the five steps beginning in 2024. Using the five steps, OIT performs comprehensive workforce analyses by examining each OIT service organization. OIT is on a 3-year workforce analysis study schedule, in accordance with VA Directive 5010, VA Manpower Management Policy. OIT expects to complete a full workforce analysis of all OIT organizations by the end of 2026.

Target Implementation Date: December 31, 2026.

**Appendix IV: Comments from the Department
of Veterans Affairs**

Enclosure

Department of Veterans Affairs (VA) Comments to the
Government Accountability Office (GAO) Draft Report
Cybersecurity Workforce: Departments Need to Fully Implement Key Practices
(GAO-25-106795)

Recommendation 3: The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs fully addresses the practices described in our report associated with implementing and monitoring a workforce action plan. (Recommendation 21).

VA Response: Partially Concur. OIT concurs with GAO's assessment of the Department for Practices 4.1-4.2. OIT continues to implement the steps in the Office of Personnel Management (OPM) Workforce Planning Guide. OIT initiated full implementation of the five steps beginning in 2024. Using the five steps, OIT performs comprehensive workforce analysis by examining each OIT service organization. OIT is on a 3-year workforce analysis study schedule, in accordance with VA Directive 5010, VA Manpower Management Policy. OIT expects to complete a full workforce analysis of all OIT organizations by the end of 2026.

Practice 4.3: "Implement and monitor the cybersecurity workforce action plan, including tracking information on the milestones, metrics, and targets from the cybersecurity workforce action plan."

Non-concur. VA provided evidence of partial implementation per compliance with participation in the Department's Strategic Workforce Plan Action Plan progress update meetings. The Department's evaluation rubric for action plans includes responsible parties, milestones, timeline, resources, potential barriers, and solution strategies identified; clear, relevant, time-bound, traceable metrics; metrics clearly tied to risk/gap being addressed; and include baseline and target.

Target Implementation Date: December 31, 2026.

Recommendation 4: The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs fully addresses the practices described in our report associated with evaluating and revising a workforce action plan. (Recommendation 22).

VA Response: Partially concur. OIT concurs with GAO's assessment of the Department for Practice 5.3. OIT continues to actively implement the steps in the OPM Workforce Planning Guide. OIT initiated full implementation of the five steps beginning in 2024. Using the five steps, OIT performs comprehensive workforce analysis by examining each OIT service organization. OIT is on a 3-year workforce analysis study schedule, in accordance with VA Directive 5010, VA Manpower Management Policy. OIT expects to complete a full workforce analysis of all OIT organizations by the end of 2026.

**Appendix IV: Comments from the Department
of Veterans Affairs**

Enclosure

Department of Veterans Affairs (VA) Comments to the
Government Accountability Office (GAO) Draft Report
Cybersecurity Workforce: Departments Need to Fully Implement Key Practices
(GAO-25-106795)

Practice 5.1: “Assess the effectiveness and efficiency of the cybersecurity workforce action plan and the progress made against its targets, baselines, outcomes, and performance measures.”

Non-concur. VA provided evidence of partial implementation. The Department has an evaluation rubric for quarterly strategic workforce planning action plan progress update meetings which include providing feedback on milestones, metrics, on target, and whether there is a need to extend the initiative. VA is providing the Department’s Strategic Workforce Action Plan planning progress update meeting slides from March, May, and November 2024 to demonstrate the sustained implementation of the evaluation rubric. See Attachments A-C.

Practice 5.2: Record actions taken, review lessons learned from the cybersecurity workforce action plan, and update or adjust metrics and targets as necessary.”

Non-concur. VA provided evidence of partial implementation. Some updates were previously provided in the OIT strategic workforce planning action plans inclusive of successes, challenges, and adjustments. The provided Strategic Workforce Action Plan planning progress update meeting slides from March, May, and November 2024 demonstrate inclusion of successes, challenges, and adjustments. See Attachments A-C.

Target Implementation Date: December 31, 2026.

Recommendation 5: The Secretary of Veterans Affairs should ensure that the Department of Veterans Affairs identify and analyze the effectiveness of its mitigation actions on the cybersecurity workforce challenges.

VA Response: Concur. VA currently uses a rubric to evaluate the effectiveness of cybersecurity workforce challenges and provides a score to inform OIT if the analysis and mitigation strategies are appropriately aligned each year. VA is providing the workforce analysis data collection template as evidence that VA identifies and analyzes the effectiveness of its mitigation actions on cybersecurity workforce challenges and barriers. See Attachment D.

VA requests closure of the recommendation.

Appendix V: Comments from the Department of Treasury



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

December 19, 2024

Mr. David Hinchman
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G St NW
Washington, DC 20548

Dear Mr. Hinchman,

Thank you for the opportunity to review the report regarding the Cybersecurity Workforce. This letter serves as the official response of the Department of the Treasury (Treasury).

Treasury supports GAO's objectives to determine the extent to which agencies implement applicable cybersecurity workforce practices and the assessment of those practices.

Treasury uses workforce planning processes to identify workforce gaps as required in Treasury Strategic Workforce Planning Program Policy (TN-20-002) and in accordance with 5 CFR 250 requirements. The workforce planning processes include a review of agency strategic objectives, a gap analysis between current workforce capabilities and future workforce needs, a risk assessment to prioritize gap closure strategies with associated resourcing levels, and action plans to close prioritized gaps. Treasury assessed its cyber workforce within the context of current resourcing levels and found that attrition, retention, and hiring rates were effectively closing cyber workforce gaps.

Treasury continues to monitor and assess the cyber workforce for gaps impacting agency strategic objectives and will adjust agency strategies and/or workforce planning activities as determined by leadership and available agency resources.

We look forward to continuing to work with your office in the future.

Sincerely,
Carrie R.
Sharp
Carrie R. Sharp
Director
Office of Strategy, Evaluation and Analysis
U.S. Department of the Treasury

Digitally signed by Carrie
R. Sharp
Date: 2024.12.19
16:13:36 -0500

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

David B. Hinchman at (214) 777-5719, hinchmand@gao.gov

Staff Acknowledgments

In addition to the contact named above, Tammi Kalugdan (Assistant Director), Andrea Starosciak (Analyst-in-Charge), Rebecca Eyler, Catherine Fan, Matt Gray, David Hong, Smith Julmisse, Anh-Thi Le, Michael Lebowitz, Steven Lozano, Rachael Scott, Elizabeth Simonelli, Teresa Smith, Andrew Stavisky, Adam Vodraska, and Alec Yohn made significant contributions to this report.

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](#), [X](#), 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

Sarah Kaczmarek, Managing Director, KaczmarekS@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

