CYBER WORKFORCE

Evidence-Based Decision Needed for the Future of OPM's Dashboard

Report to Congressional Committees

March 2026
GAO-26-108098
United States Government Accountability Office

Accessible Version

GAO Highlights

CYBER WORKFORCE

Evidence-Based Decision Needed for the Future of OPM's Dashboard

GAO-26-108098
March 2026

Highlights of GAO-26-108098, a report to congressional committees
For more information, contact: David B. Hinchman at HinchmanD@gao.gov

What GAO Found

The Office of Personnel Management (OPM) launched its Cyber Workforce Dashboard in 2023 as a government-wide application for managing the cybersecurity workforce. The intended purpose of the Dashboard was to provide a comprehensive government-wide view of federal cyber workforce data and to allow agencies to benchmark their workforce data against other agencies.

However, five of six selected agencies and OPM, the administrator of the Dashboard, reported they were not using the Dashboard. The General Services Administration was the one agency using it, primarily for workforce planning. All six selected agencies reported limitations with the Dashboard, including communications with OPM, access, functionality, and use of data. OPM reported many of the same types of limitations in managing the effort.

Number of Office of Personnel Management's Cyber Workforce Dashboard Limitations Experienced by the Six Selected Agencies

	Agencies						
Limitations	Justice	State	Treasury	GSA	NSF	SBA	Total
Communication with OPM	✔	✔	✔	✔	✔		5
Access	✔		✔	✔			3
Functionality		✔		✔	✔		3
Data		✔	✔	✔	✔	✔	5

Justice (Department of Justice), State (Department of State), Treasury (Department of the Treasury), GSA (General Services Administration), NSF (National Science Foundation), SBA (Small Business Administration).

Sources: GAO analysis of Office of Personnel Management Cyber Workforce Dashboard limitations reported by the six selected agencies; Justice logo, State logo, Treasury logo, GSA logo, NSF logo, SBA logo. | GAO-26-108098

Accessible Data for Number of Office of Personnel Management's Cyber Workforce Dashboard Limitations Experienced by the Six Selected Agencies

Agency	Communication-with OPM	Access	Functionality	Data
Department of Justice	1	1	na	na
Department of State	1	na	1	1
Department of the Treasury	1	1	na	1
General Services Administration	1	1	1	1
National Science Foundation	1	na	1	1
Small Business Administration	na	na	na	1
Total	5	3	3	5

Sources: GAO analysis of Office of Personnel Management Cyber Workforce Dashboard limitations reported by the six selected agencies; Justice logo, State logo, Treasury logo, GSA logo, NSF logo, SBA logo. I GAO-26-108098

Given the lack of use, the Dashboard is not meeting its intended purpose for the six selected agencies. Further, OPM does not know the extent of non-use by the almost 20 other federal agencies that have access to the Dashboard. Additionally, OPM has not solicited feedback on it. Regarding costs, according to OPM officials, the funds spent on the Dashboard effort since its inception were minimal and therefore not covered by a separate budget line item. Officials added that they did not have an estimate of exact costs or future planned costs.

Without information on the extent of use among the more than 20 federal agencies, OPM is limited in knowing whether it should continue or terminate the effort. Expeditiously collecting and analyzing such information, soliciting feedback from agencies, and determining costs are essential to determining the future of the Dashboard.

Why GAO Did This Study

The Office of Management and Budget (OMB), the Office of the National Cyber Director (ONCD), and prior GAO reports have stated that the federal government faces a persistent shortage of cyber and IT professionals. Building and maintaining a talented cyber workforce is one of the federal government's most important challenges. The Federal Information Security Modernization Act of 2014 includes a provision for GAO to periodically evaluate federal agencies' information security policies and practices. This includes evaluating agencies' cybersecurity workforce management policies and applications, such as the Dashboard. This report (1) describes the Dashboard, (2) describes how selected federal agencies are using the Dashboard to support their workforce planning efforts, and (3) determines the extent to which the Dashboard is meeting its intended purpose. GAO randomly selected six agencies, divided into three tiers based on their reported fiscal year 2025 IT spending. GAO interviewed relevant OPM and agency officials and reviewed Dashboard documentation and usage metrics that OPM initially gathered after the Dashboard was launched. GAO also analyzed applicable guidance, best practices, and relevant Dashboard documentation.

What GAO Recommends

GAO is making one recommendation to OPM to collect and analyze information on Dashboard use, solicit agency feedback on Dashboard limitations, determine the costs, and make an evidence-based decision to either terminate the Dashboard or continue offering it to agencies with needed improvements. OPM partially concurred and stated that it will work with ONCD and OMB to determine what actions, if any, should be taken and OMB to determine what actions, if any, should be taken.

Contents

Abbreviations

- CFO Chief Financial Officer
- CHCO Chief Human Capital Officer
- DHS Department of Homeland Security
- EHRI Enterprise Human Resources Integration
- FISMA Federal Information Security Modernization Act of 2014
- FPPS Federal Personnel and Payroll System
- GEMS Global Employment Management System
- GSA General Services Administration
- IT information technology
- NICE National Initiative for Cybersecurity Education
- NIST National Institute of Standards and Technology
- NSF National Science Foundation
- OMB Office of Management and Budget
- ONCD Office of the National Cyber Director
- OPM Office of Personnel Management
- SBA Small Business Administration
- SFS Scholarship for Service

March 27, 2026

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 Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Federal agencies depend on IT systems to carry out operations that protect our nation's security. Given the ever-present threat posed by cyberattacks and the risk of unauthorized access to IT systems, it is essential that federal agencies ensure that the proper cybersecurity workforce resources are in place to protect the government's technology infrastructure. As a result, building and maintaining a talented cyber workforce is one of the federal government's most important challenges.

Nevertheless, the Office of Management and Budget (OMB), the Office of the National Cyber Director (ONCD), and our prior reports have stated that the federal government faces a persistent shortage of cyber and IT professionals.[1] For example, in our 2024 High-Risk Series report, we identified four major cybersecurity challenges and 10 critical actions that federal agencies need to take to address them. One of these actions was to address cyber workforce management challenges.[2]

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

[1]Office of Management and Budget, *Federal Cybersecurity Workforce Strategy*, Memorandum M-16-15 (July 12, 2016); The White House, Office of the National Cyber Director, Executive Office of the President, *National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent*, (Washington D.C.: July 31, 2023); GAO, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C.: Mar. 12, 2019); GAO, *Cybersecurity Workforce: National Initiative Needs to Better Assess Its Performance*, GAO-23-105945 (Washington, D.C.: Jul. 27, 2023); and GAO, *Cybersecurity Workforce: Departments Need to Fully Implement Key Practices*, GAO-25-106795 (Washington, D.C.: Jan. 16, 2025).

[2]GAO, *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, GAO-24-107231 (Washington, D.C.: June 13, 2024). According to the Office of Personnel Management's Cyber Workforce Dashboard, the cyber workforce includes employees in the federal government who are assigned a cyber position code, indicating the position performs IT, cybersecurity, and cyber-related functions.

the agencies' operations and assets.[3] 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 of these federal agency-wide cybersecurity programs include evaluating the agencies' cybersecurity workforce management policies and applications. A federal cybersecurity workforce management application available to both federal agencies and the public is the Office of Personnel Management's (OPM) Cyber Workforce Dashboard.[4]

Our specific objectives were to (1) describe the Cyber Workforce Dashboard, (2) describe how selected federal agencies are using the Cyber Workforce Dashboard to support their workforce planning efforts, and (3) determine the extent to which the Dashboard is meeting its intended purpose. For both objectives, we selected 21 of the 23 Chief Financial Officer (CFO) Act agencies included in the Dashboard.[5] To ensure that our evaluation included large, medium, and small agencies, we divided the 21 selected civilian CFO Act agencies into three tiers based on the amount of their fiscal year 2025 IT spending as reported in the General Services Administration's (GSA) Federal IT Dashboard.[6] We then randomly selected two agencies from each of the three tiers for a total of six agencies.

- The two tier I selected agencies with fiscal year 2025 IT spending over $3 billion were the Department of Justice and the Department of the Treasury.
- The two tier II selected agencies with fiscal year 2025 IT spending between $1 billion and $3 billion were GSA and the Department of State.
- The two tier III selected agencies with fiscal year 2025 IT spending less than $1 billion were the Small Business Administration (SBA) and the National Science Foundation (NSF).

To address the first objective, we interviewed OPM officials and reviewed Dashboard documentation, such as the Dashboard user guide. We also reviewed the Dashboard version for public use available on OPM's website to understand the data it provided to the public.

To address the second objective, we reviewed Dashboard program documentation from OPM, such as usage metrics that OPM initially gathered after the Dashboard was launched. We interviewed OPM officials to determine how the agency intended for federal agencies to use the Dashboard to inform their cyber workforce planning efforts. We then reviewed documentation and interviewed officials from the six selected agencies

[3]The 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.

[4]The Cyber Workforce Dashboard is a public, federal government website operated by OPM and accessible at https://www.opm.gov/data/data-products/cyber-workforce-dashboard/.

[5]The 21 civilian agencies covered by the Chief Financial Officers (CFO) Act of 1990, 31 U.S.C. § 901(b) and identified for our review are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency, the General Services Administration, the National Aeronautics and Space Administration, the National Science Foundation, the Nuclear Regulatory Commission, the Small Business Administration, and the Social Security Administration. The Office of Personnel Management (OPM) and the U.S. Agency for International Development (USAID) are also civilian agencies covered by the CFO Act. However, we excluded them from our review because USAID recently underwent a significant reduction in workforce, and OPM is the focus of the engagement and was evaluated as the owner of the Cyber Workforce Dashboard.

[6]The IT Dashboard is a public, federal government website previously operated by OMB and currently operated by GSA at https://itdashboard.gov. The purpose of the IT Dashboard is to enable those in the federal government and the public to understand the health of IT investments and the impact of federal IT portfolios.

regarding their use of the Dashboard. We also discussed with officials from the six selected agencies the use of any alternative workforce planning methods to inform their cyber workforce planning efforts.

To address the third objective, we reviewed OPM documentation that identified the Dashboard's intended purpose. We then compared the intended purpose for the Dashboard to the six selected agencies' use of the Dashboard that we identified in objective two. We also analyzed documentation and interviewed officials from OPM as to their own use of the Dashboard. We compared this information to OPM documentation to determine the extent to which the Dashboard was meeting its intended purpose.

We also identified federal guidance and best practices for determining if an initiative is meeting its intended purpose. Guidance such as OMB's *Evidence-Based Policymaking* and OPM's *Workforce Planning Guide,* and best practices such as GAO's *Key Principles for Effective Strategic Workforce Planning,* encourage evaluating the overall performance of initiatives by measuring progress towards defined objectives and goals and making evidence-based decisions.[7] We then reviewed OPM documentation and interviewed relevant officials to determine the extent to which OPM evaluated the Dashboard's effectiveness, to include usage and cost. We analyzed this information to determine if OPM made evidence-based decisions regarding the Dashboard as recommended by guidance and best practices.

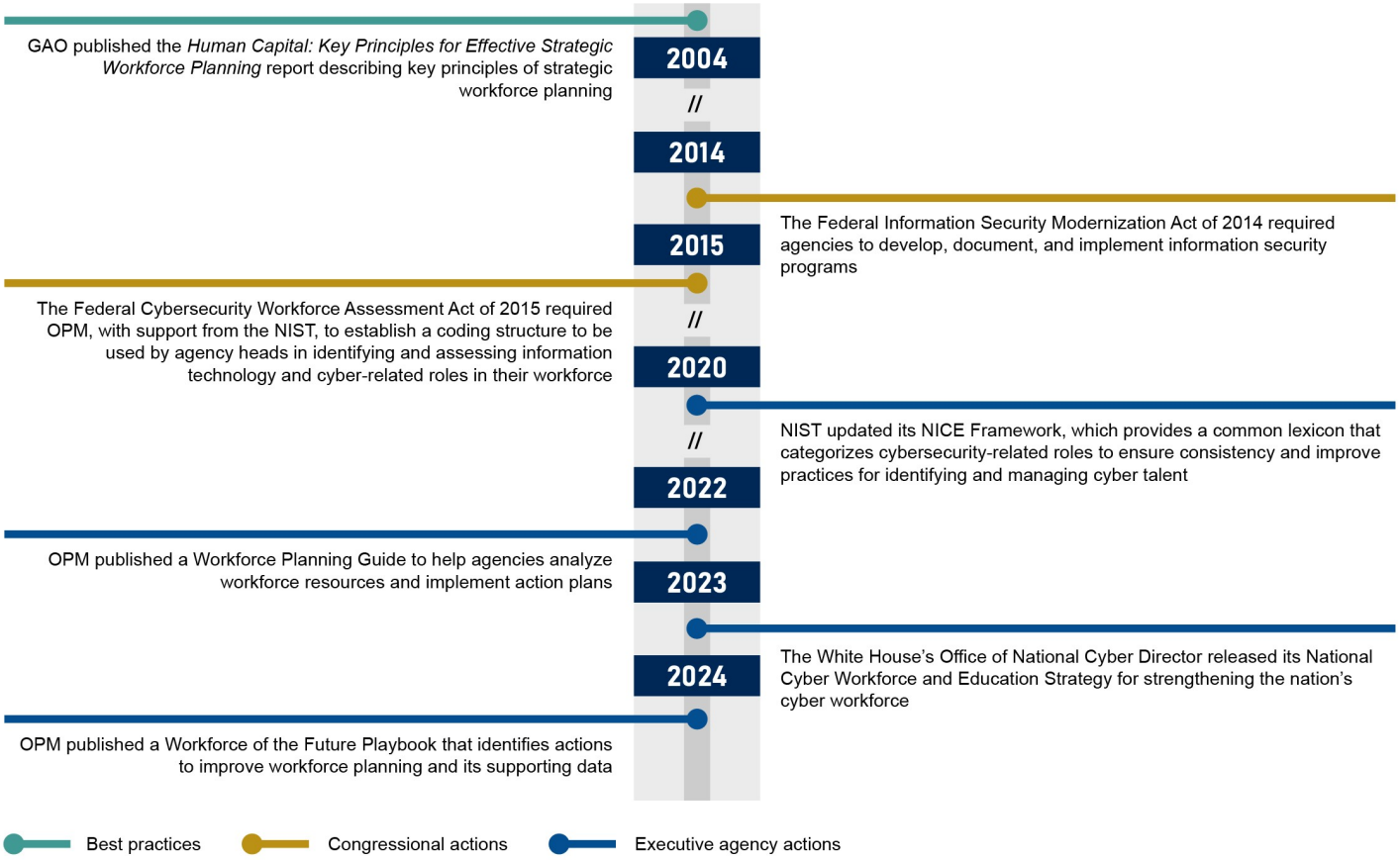
We conducted this performance audit from January 2025 to March 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions 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

Federal cyber workforce planning is governed and supported by legislation, guidance, and evolving best practices. The aim of these laws, guidance, and practices is to develop a robust federal cyber workforce equipped to successfully manage and protect the federal government's cyber infrastructure. Figure 1 displays a timeline of selected federal cyber workforce planning legislation, guidance, and best practices.

[7]Office of Management and Budget, *Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans*, OMB M-21-27 (Washington, D.C.: June 2021); Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: Nov. 2022); and GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

Figure 1: Timeline of Selected Federal Cyber Workforce Planning Legislation, Guidance, and Best Practices



OPM = Office of Personnel Management, NIST = National Institute of Standards and Technology, NICE = National Initiative for Cybersecurity Education

Source: GAO analysis of executive agency, Congressional, and GAO information. | GAO-26-108098

Federal Cyber Workforce Planning Legislation and Guidance

Congress has enacted legislation and the National Institute of Standards and Technology (NIST), along with the White House, have issued guidance to increase agencies' understanding of their cyber workforce (to include IT, cybersecurity, and cyber-related functions) through the implementation of various workforce planning processes. These processes are essential for ensuring that federal agencies have the talent, skills, and experience they need to execute their missions and program goals, including strengthening their cyber workforce.

FISMA. Enacted in 2014, FISMA requires agencies to develop, document, and implement agency-wide information security programs to protect their IT systems.[8] The act also requires agencies to submit FISMA

[8]The 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.

reports on their information security programs to OMB, the Department of Homeland Security, Congress, and GAO. FISMA also includes a provision for GAO to evaluate agencies' implementation of FISMA requirements, which include having trained personnel sufficient to carry out the responsibilities under FISMA.

The Federal Cybersecurity Workforce Assessment Act of 2015. Enacted in 2015, the act 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.[9] The act also required agencies, in consultation with OPM and NIST, to 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.[10]

NIST's Workforce Framework for Cybersecurity. In November 2020, NIST published an updated National Initiative for Cybersecurity Education (NICE) *Workforce Framework for Cybersecurity* that included a common lexicon for categorizing and describing cybersecurity-related work roles and functions.[11] It is intended to improve communication about how to identify, recruit, develop, and retain cyber talent.

OPM's Workforce Planning Guide. In November 2022, OPM published the *Workforce Planning Guide* as a resource for agencies to use when planning and analyzing their workforce, identifying gaps, and implementing workforce action planning efforts.[12] Among other things, the *Workforce Planning Guide* describes the importance of using metrics with quantifiable data to measure whether goals and objectives are being adequately achieved and support timely interventions, as needed, to improve performance and overall efficiency of services.

National Cybersecurity Strategy. In March 2023, the White House released its *National Cybersecurity Strategy* that included goals for strengthening the nation's cybersecurity workforce.[13] In July 2023, the White House released the *National Cybersecurity Strategy Implementation Plan* that supported the *National Cybersecurity Strategy* and subsequently updated this plan in May 2024.[14]

National Cyber Workforce and Education Strategy. In July 2023, the White House's ONCD released its *National Cyber Workforce and Education Strategy*.[15] ONCD's strategy identified four pillars for strengthening the nation's cyber workforce, one of which focused on the federal cyber workforce. Specifically, the strategy detailed an approach for strengthening the federal cyber workforce through four strategic objectives: (1) drive sustained progress through greater federal collaboration, (2) attract and hire a qualified and diverse federal

[9]The Federal Cybersecurity Workforce Assessment Act of 2015 was enacted as part of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title III, sec. 301 (Dec. 18, 2015) 129 Stat. 2242, 2975-77.

[10]Fiscal year 2022 was the final year that OPM required agencies to submit these mission- critical occupation documents.

[11]National Institute of Standards and Technology, *Workforce Framework for Cybersecurity*, (NICE Framework), Special Publication 800-181 revision 1 (Gaithersburg, MD: Nov. 2020). This version replaced an earlier version that was published in August 2017. See https://csrc.nist.gov/pubs/sp/800/181/r1/final. According to NIST, the National Initiative for Cybersecurity Education is now just referred to as NICE. The NICE Framework includes a broad range of roles, including those related to IT, cyber, and cybersecurity.

[12]Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: Nov. 2022).

[13]The White House, *National Cybersecurity Strategy* (Washington, D.C.: March 2023).

[14]The White House, *National Cybersecurity Strategy Implementation Plan* (Washington, D.C.: July 13, 2023). The White House subsequently updated the *National Cybersecurity Strategy Implementation Plan* in May 2024. See White House, *National Cybersecurity Strategy Implementation Plan*, Version 2 (Washington, D.C.: May 2024).

[15]The White House, Office of the National Cyber Director, Executive Office of the President, *National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent* (Washington, D.C.: July 31, 2023).

cyber workforce, (3) improve career pathways in the federal cyber workforce, and (4) invest in human resources capabilities and personnel. Such efforts were to include increasing access to cyber jobs, communicating the benefits of public service careers, and lowering the barriers associated with hiring and onboarding.

OPM's Workforce of the Future Playbook. In February 2024, OPM published the *Workforce of the Future Playbook* that identifies the specific actions agencies could take to provide the foundation for the workforce of the future.[16] The *Playbook* is 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.

National Cyber Workforce and Education Strategy: Initial Stages of Implementation. In June 2024, the White House released the *National Cyber Workforce and Education Strategy: Initial Stages of Implementation* to identify federal agencies' ongoing efforts to implement the *National Cyber Workforce and Education Strategy*.[17] Among other initial steps noted in the report, ONCD and OMB compiled a list of commitments and initiatives from 14 agencies aimed at increasing cyber hiring and talent development in the federal government. As a result of awaiting guidance from a new National Cyber Director, ONCD officials stated that an updated report on agencies' progress in implementing the *National Cyber Workforce and Education Strategy* would be produced after October 2025. As of March 2026, this report had not yet been produced.

Best Practices for Federal Cyber Workforce Planning

In addition to the legislation and guidance discussed above, GAO developed best practices for federal workforce planning. Specifically, in 2004, GAO published the *Human Capital: Key Principles for Effective Strategic Workforce Planning* report.[18] This report describes the key principles of strategic workforce planning and provides illustrative examples of these principles drawn from selected agencies' strategic workforce planning experiences. It also includes a framework of best practices for developing, communicating, and implementing strategic workforce planning, and encourages federal agencies to use metrics to monitor and evaluate progress toward workforce goals.

OPM guidance, described above, supplements the GAO best practices by calling for the use of metrics to measure program progress and ensuring that agencies' workforce planning processes and applications are achieving program goals.[19] Furthermore, OMB's *Evidence-Based Policymaking* guidance calls for agencies to

[16]Office 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.: Feb. 2024).

[17]The White House, Office of the National Cyber Director, Executive Office of the President, *National Cyber Workforce and Education Strategy: Initial Stages of Implementation*, (Washington, D.C.: June 25, 2024); and The White House, Office of the National Cyber Director, Executive Office of the President, *National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent* (Washington, D.C.: July 31, 2023).

[18]GAO-04-39.

[19]Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: Nov. 2022).

measure progress towards defined program objectives and goals, and making evidence-based decisions regarding the programs also reinforces these practices.[20]

GAO Has Reported on Efforts to Address Cyber Workforce Challenges

During the past several years, we have reported on various federal cyber workforce challenges and the importance of federal agencies following workforce planning best practices to ensure they have the cyber talent, skills, and experience needed to execute their missions and achieve program goals.

In September 2025, we reported on civilian federal agencies' ability to identify the size and cost of their federal and contractor cyber workforce, as well as federal guidance to evaluate the effectiveness of their existing cyber workforce initiatives.[21] We found that most agencies did not have quality information regarding the size and cost of their cyber workforce. Accordingly, we made a total of four recommendations to ONCD to address workforce data gaps, quality assurance, cyber staff identification, and efforts to assess effectiveness of workforce initiatives. As of March 2026, none of the recommendations had been implemented.

In January 2025, we reported on the extent to which selected agencies implemented 15 applicable practices for cybersecurity workforce planning.[22] We found that most of the selected agencies 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. We noted that officials at the selected agencies cited inadequate funding, difficulties with recruitment, and difficulties with retention as three primary types of cybersecurity workforce management challenges. Accordingly, we made a total of 23 recommendations to 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. As of March 2026, the Department of Veterans Affairs had implemented one of the recommendations.

In July 2023, we reported that while NIST's NICE program took steps to strengthen the cybersecurity workforce, additional efforts were needed to better assess performance.[23] Specifically, among the nine selected key practices for establishing a program performance process, NIST fully implemented one practice, partially implemented five, and did not implement the remaining three practices. For example, NIST partially implemented the practice for tracking information that is timely, accurate, and useful. It also did not implement efforts to use data to assess progress towards goals and identify gaps. Consequently, we made eight recommendations to NIST to address the eight practices it did not fully implement. Commerce agreed with our recommendations. As of March 2026, none of the recommendations had been implemented.

In September 2022, we reviewed the CyberCorps® Scholarship for Service Program (SFS), an important federal cyber workforce recruitment program operated by the National Science Foundation (NSF) in conjunction with OPM and the Department of Homeland Security (DHS).[24] We reported that NSF and OPM partially complied with certain selected SFS program legal requirements. We noted that this impacted SFS's

[20]Office of Management and Budget, *Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans*, OMB M-21-27 (Washington, D.C.: June 2021).

[21]GAO, *Cybersecurity Workforce: Actions Needed to Improve Size and Cost Data*, GAO-25-107405 (Washington, D.C.: Sept. 4, 2025).

[22]GAO-25-106795.

[23]GAO-23-105945.

[24]GAO, *Cybersecurity Workforce: Actions Needed to Improve CyberCorps® Scholarship for Service Program,* GAO-22-105187 (Washington, D.C.: Sept. 29, 2022).

ability to achieve its goal of attracting and retaining high-quality graduates in the public sector cybersecurity workforce and supporting the U.S. government's strategy to develop a superior cybersecurity workforce. Accordingly, we made three recommendations to NSF and two to OPM to fully comply with SFS program legal requirements and implement a risk management strategy. As of March 2026, all five recommendations had been implemented.

In March 2019, we reported on how federal agencies categorized IT and cybersecurity positions to identify critical staffing needs in accordance with the Federal Cybersecurity Workforce Assessment Act of 2015.[25] We found that most of the 24 agencies reviewed had miscategorized several IT and cyber-related positions. In addition, we found that six of the 24 agencies had not completed work role code assignments to their vacant positions, noting that ongoing shortages of qualified cybersecurity professionals put federal IT systems at risk. Accordingly, we made 28 recommendations directing 22 agencies to review and assign the appropriate codes to their IT, cybersecurity, and cyber-related positions. As of March 2026, the agencies had fully implemented all 28 of the recommendations.

OPM Established the Cyber Workforce Dashboard

In April 2023, the Federal Cyber Workforce Working Group, co-chaired by ONCD and OMB, in consultation with OPM, established the Cyber Workforce Dashboard as a government-wide application for managing the cyber workforce.[26] The Dashboard is intended to support agencies in cybersecurity workforce planning efforts and in making data-driven decisions regarding current and future cybersecurity workforce requirements. Managed by OPM's Workforce Policy and Innovation group's Strategic Workforce Planning and Forecasting Methods team, the Dashboard includes, among other things, detailed cyber workforce data for OMB, the Smithsonian Institution, and the National Archives and Records Administration, as well as 24 agencies covered by the Chief Human Capital Officers Act of 2002.[27] The data is compiled from OPM's Enterprise Human Resources Integration system, OPM's Chief Human Capital Officer (CHCO) Hiring Manager Satisfaction Survey, and OPM's annual request to federal agencies for workforce data.[28] The Dashboard contains two viewing options: a version for public use and one for agency use. Figure 2 displays a graphic of the Dashboard version for public use.

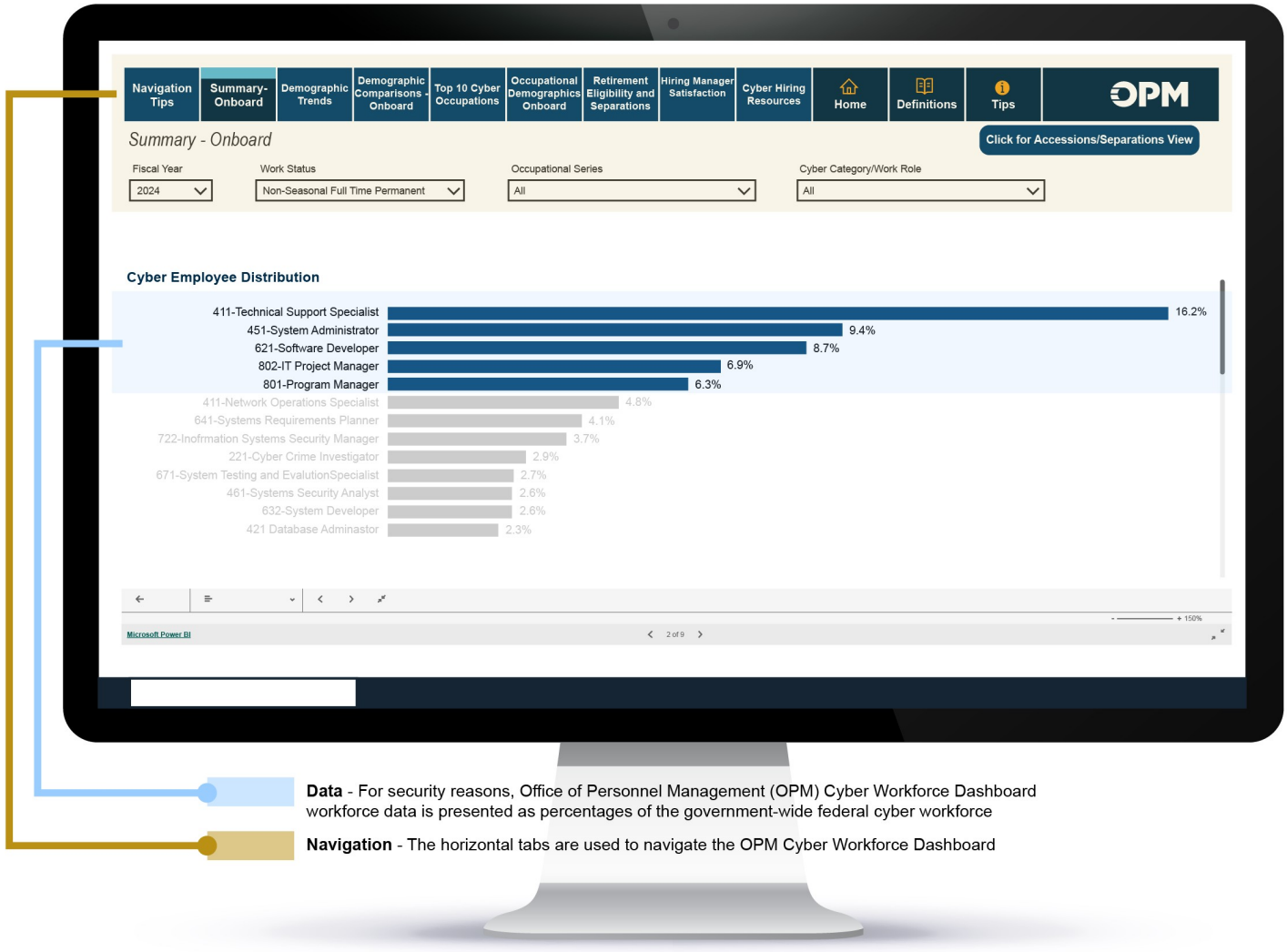
[25]GAO-19-144.

[26]The Cyber Workforce Dashboard is a public, federal government website operated by OPM and accessible at https://www.opm.gov/data/data-products/cyber-workforce-dashboard/.

[27]The 24 agencies covered by the Chief Human Capital Officers Act of 2002, 5 U.S.C. § 1401 are the same as the 23 civilian agencies and the Department of Defense covered by the Chief Financial Officers (CFO) Act of 1990, 31 U.S.C. § 901(b).

[28]OPM's Enterprise Human Resources Integration system (EHRI) is one of five OPM led e-Government initiatives designed to leverage the benefits of IT. EHRI includes some legislative branch entities, the U.S. Tax Court, and most executive branch entities. 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 the White House Office.

Figure 2: Office of Personnel Management's Cyber Workforce Dashboard Version for Public Use



Sources: GAO analysis of OPM Cyber Workforce Dashboard website information; Can Yesil/stock.adobe.com (desktop). | GAO-26-108098

Accessible Data for Figure 2: Office of Personnel Management's Cyber Workforce Dashboard Version for Public Use

Cyber Employee Distribution

Category	Percentage
411-Technical Support Specialist	16.2%
451-System Administrator	9.4%
621-Software Developer	8.7%
802-IT Project Manager	6.9%
801-Program Manager	6.3%
411-Network Operations Specialist	4.8%
641-Systems Requirements Planner	4.1%

Category	Percentage
722-Inofrmation Systems Security Manager	3.7%
221-Cyber Crime Investigator	2.9%
671-System Testing and Evaluation Specialist	2.7%
461-Systems Security Analyst	2.6%
632-System Developer	2.6%
421 Database Administrator	2.3%

Sources: GAO analysis of OPM Cyber Workforce Dashboard website information; Can Yesil/stock.adobe.com (desktop). I GAO-26-108098

Both OPM officials and Dashboard documentation state the Dashboard version for public use, launched in April 2023, was intended to provide a comprehensive government-wide view of federal cyber workforce data, including work roles; demographic trends and comparisons; the top 10 cybersecurity occupations; retirement eligibility; and separations. While the Dashboard presents a significant amount of data to the public, it does not include absolute federal cybersecurity workforce numbers, such as agency headcount and workforce size data. To reduce any potential security risks to the individual agencies as well as the larger federal government, OPM stated that it masks the absolute federal cybersecurity workforce numbers by displaying the data as general percentages of the government-wide federal cyber workforce.

In September 2023, OPM launched a Dashboard version for agency use. According to OPM Dashboard documentation, this version is to be managed by a designated employee at each agency, known as a data champion. OPM officials stated that the Dashboard version for agency use displays cyber work roles, hiring trends, and workforce demographics in a restricted manner that is not available to the public or to other agencies. They stated that agencies could use the Dashboard to track cyber work role metrics such as separations and to benchmark data against other agencies across the federal government. Similar to the Dashboard version for public use, the data available in the version for agency use is also presented as percentages instead of absolute numbers, although OPM officials stated that individual agencies could work with OPM to obtain their specific agency's cyber workforce data. To facilitate agency use of the Dashboard, OPM officials stated that a help desk email account was established for agencies to use for contacting OPM regarding Dashboard questions or issues. OPM officials also noted that OPM provided training to agency employees on the Dashboard.

Table 1 describes the different Dashboard data tabs available in both the public and agency versions. The Dashboard version for agency use includes one additional tab titled "Agencies" that is not found in the version for public use. The "Agencies" tab contains cyber workforce data specific to the individual agency viewing the Dashboard and allows individual agencies to compare their cyber workforce data to government-wide cyber workforce data.

Table 1: The Office of Personnel Management's (OPM) Cyber Workforce Dashboard Versions for Public and Agency Use Tab Names and Descriptions

Dashboard tab name	Dashboard tab description
Summary	The Summary tab has two views, the Onboard view and the Accessions/Separations view. The Onboard view displays summary statistics by fiscal year for OPM Occupational Series cyber-coded employees, limited to Chief Human Capital Officers (CHCO) Council member agencies, the Office of Management and Budget, the Smithsonian Institution, and the National Archives and Records Administration.[a] These statistics include the average employee age, average employee adjusted base pay, average length of service, and retention rate, among others. The Accessions/Separations view displays the average employee age, average employee base pay, and average length of service for employee accessions and separations by fiscal year for the same agencies as the Onboard view.
Demographic Trends	The Demographic Trend tab displays how Dashboard metrics for each cyber-coded employee demographic category have changed over time, by fiscal year.
Demographic Comparisons - Onboard	The Demographic Comparisons – Onboard tab displays comparisons of agency cyber-coded employee demographics using government-wide percentages.
Top 10 Cyber Occupations	The Top 10 Cyber Occupations tab displays four different views of the individual OPM Occupational Series with the 10 highest numbers of cyber-coded employees.[b]
Occupational Demographics - Onboard	The Occupational Demographics – Onboard tab displays the percentages of cyber-coded employees in each OPM Occupational Series as compared to all cyber-coded employees.
Retirement Eligibility and Separations	The Retirement Eligibility and Separations tab displays comparisons of individual agency cyber workforce retirement eligibility and separation rates to those of the federal government.
Hiring Manager Satisfaction	The Hiring Manager Satisfaction page displays information from the government-wide CHCO Council's Management Satisfaction Survey.
Cyber Hiring Resources	The Cyber Hiring Resources tab displays links to resources that agencies can use when recruiting, hiring, and retaining cyber employees.

Source: GAO analysis of Office of Personnel Management Cyber Workforce Dashboard. | GAO-26-108098

[a]The OPM Cyber Workforce Dashboard contains data for the Office of Management and Budget, the Smithsonian Institution, and the National Archives and Records Administration, as well as 24 agencies covered by the Chief Human Capital Officers Act of 2002, 5 U.S.C. § 1401, which are agencies covered by the Chief Financial Officers (CFO) Act of 1990, 31 U.S.C. § 901(b). The 24 agencies covered by the Chief Financial Officers (CFO) Act of 1990, 31 U.S.C. § 901(b) are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency, the General Services Administration, the National Aeronautics and Space Administration, the National Science Foundation, the Nuclear Regulatory Commission, the Office of Personnel Management, the Small Business Administration, the Social Security Administration, and the U.S. Agency for International Development.

[b]The Office of Personnel Management's Occupational Series is a grouping of positions with a similar line of work and qualification requirements.

Most Selected Agencies Do Not Use the Dashboard

Five of the six selected agencies reported they do not use the Dashboard. These agencies also identified various limitations with Dashboard usage.

Specifically, of the six selected agencies, three agencies (Justice, NSF, and State), reported they had never used the Dashboard. Two agencies (SBA and Treasury) reported they had used the Dashboard in the past but did not currently use it. One agency, GSA, reported that it currently uses the Dashboard to establish a benchmark of the agency's cyber workforce during workforce planning at the beginning of each fiscal year.

Officials from five of the six selected agencies not using the Dashboard (Justice, NSF, SBA, State, and Treasury) stated that they used other workforce planning methods, such as internally developed reports and applications. These officials stated that, unlike the Dashboard, these agency-specific workforce planning

methods provided functionality the agencies needed, such as the ability to filter and format cyber workforce data.

Table 2 describes the six selected agencies' use of the Dashboard and other agency-specific workforce planning methods.

Table 2: Selected Federal Agencies' Use of the Office of Personnel Management's (OPM) Cyber Workforce Dashboard and Other Workforce Planning Methods

Agency	Use of OPM Cyber Workforce Dashboard	Description of other agency-specific workforce planning methods
Department of Justice	No agency use of the Dashboard	Justice officials reported that they had limited information about the Dashboard and that it was not used at the agency. Justice officials reported using the National Finance Center's Insight application to extract the data Justice needs for their data reporting.[a]
Department of State	No agency use of the Dashboard	State's Diplomatic Technology Bureau officials reported that the agency was aware of the Dashboard's existence, but it was not used by the agency for cyber workforce planning efforts. They noted that this was because the Dashboard did not provide the ability to filter State's civil service, and the data did not include State's foreign service personnel. State officials noted that the agency stored its human resources data in its Global Employment Management System (GEMS).[b] They also stated the agency relied on internal human resource systems, workforce data analysis, and planning tools for workforce management. They further stated that these methods were tailored to State's organizational structure, operational needs, and aligned with the agency's strategic planning processes.
Department of the Treasury	Past agency use of the Dashboard	Treasury officials reported previous use of the Dashboard for benchmarking purposes but stated the agency no longer used the Dashboard. Treasury officials stated that the agency's internal Workforce Planning Dashboard offered better support for the agency's workforce planning efforts. They added that it enables complete, descriptive, and predictive data analysis, including the ability to filter cyber work role codes. Further, Treasury officials noted that the agency's internal data was more current and accurate compared to OPM's Dashboard's data.
General Services Administration (GSA)	Current agency use of the Dashboard	GSA officials reported current and consistent use of the Dashboard version for public use, primarily to view government-wide benchmarks for the agency's most prevalent cyber workforce roles. GSA officials stated the agency developed a Human Resources Business Partner Report that provided enhanced workforce planning functionality not available through the Dashboard. They added that this report, which functioned like an electronic dashboard, provided the agency with accurate cyber workforce information. This information included cybersecurity workforce codes that were consistent with the information GSA sent to OPM through the Enterprise Human Resources Integration (EHRI) system.[c] GSA officials stated the report also enabled the agency to identify gaps, implement strategies, and make progress to build an experienced cyber workforce.
National Science Foundation (NSF)	No agency use of the Dashboard	NSF officials stated that they did not use the Dashboard. NSF officials reported that the agency used other dashboards developed by OPM, alongside other systems such as the reports generated by the Federal Personnel and Payroll System (FPPS).[d]

Agency	Use of OPM Cyber Workforce Dashboard	Description of other agency-specific workforce planning methods
Small Business Administration (SBA)	Past agency use of the Dashboard	SBA officials stated that the agency used the Dashboard for fiscal year 2024 benchmarking purposes but no longer used it for workforce planning. SBA officials cited use of an internal IT workforce plan, specifically the Information Technology Workforce Plan. They stated that this plan enabled SBA to establish an agency-wide approach to developing a high-performing IT workforce that could meet the needs of its internal customers and the nation's small businesses. SBA officials noted the plan included analyses of SBA workforce demographics, occupational series, positions, functions, and future competencies and skills.

Source: GAO analysis of Office of Personnel Management Cyber Workforce Dashboard use reported by the six selected agencies. | GAO-26-108098

[a]The National Finance Center's Insight application is an enterprise-wide data warehouse with reporting and business intelligence capabilities.

[b]The Department of State's Global Employment Management System (GEMS) was the agency's primary system of record for human resources and personnel data. It provided comprehensive employment data for all direct-hire State employees.

[c]OPM's Enterprise Human Resources Integration (EHRI) 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.

[d]The Federal Personnel and Payroll System (FPPS) is the U.S. Department of the Interior's comprehensive personnel and payroll system that presents real-time updates of employee personnel and payroll data. The system is operated by the Interior Business Center and services over 50 agencies, including the National Science Foundation.

Selected Agencies Experienced Dashboard Limitations

All six of the selected agencies reported limitations with using the Dashboard. Table 3 provides a detailed description of the limitations experienced by the six selected agencies, identified and organized by the four categories: communication, access, functionality, and data.

Table 3: Selected Agencies Limitations with Use of the Office of Personnel Management's (OPM) Cyber Workforce Dashboard

Category	Source of limitation	Description of limitation
Communication limitations with OPM	Department of Justice	Justice officials stated they had received no communication from OPM about the Dashboard despite being involved with other initiatives such as OPM's Federal Cyber Rotation Program.[a] Officials stated they attempted to communicate with OPM regarding the Dashboard after hearing from GAO about this review, but as of May 2025 had not yet received a response from OPM.
Communication limitations with OPM	Department of State	State officials stated that they were unaware of any communication or formal outreach from OPM regarding the agency's ability to manage its cyber workforce using the Dashboard.
Communication limitations with OPM	Department of the Treasury	Treasury officials stated that a lack of timely responses and support from OPM regarding Dashboard usage by Treasury was a limitation that led to a decline in the agency using the Dashboard.
Communication limitations with OPM	General Services Administration (GSA)	GSA officials reported that they attempted to contact OPM to inquire about the ability to filter Dashboard data to the agency level but had not received a response to their inquiry as of May 2025.
Communication limitations with OPM	National Science Foundation (NSF)	NSF officials stated that the lack of communication from OPM regarding the Dashboard was a significant limitation. NSF officials stated that the agency discussed other OPM dashboards with OPM officials, but the Cyber Workforce Dashboard was not included in these discussions.

Category	Source of limitation	Description of limitation
Dashboard access limitations	Justice	As of May 2025, Justice officials had requested access to the Dashboard on two separate occasions, but the officials stated they did not receive a response from OPM.
Dashboard access limitations	GSA	GSA officials stated that the agency's human resources team only uses the Dashboard version for public use, as the GSA employee with access to the Dashboard version for agency use did not reside within the Human Capital office.
Dashboard access limitations	Treasury	Treasury officials reported the agency lost access to the Dashboard in January 2025 due to technological changes to the Dashboard. As of June 2025, Treasury officials stated the agency's access to the Dashboard had been restored. Treasury officials cited the agency's lack of reliable access to the Dashboard as a limitation.
Dashboard functionality limitations	GSA	GSA officials stated that its ability to use the Dashboard was limited due to gaps in Dashboard functionality. Specifically, GSA officials reported that the agency was unable to filter Dashboard data to the agency level so it could be used for workforce planning purposes.
Dashboard functionality limitations	NSF	NSF officials stated that the agency decided to not use the Dashboard due to its limited functionality, including difficulties with validating and using the Dashboard data since the data was displayed as percentages rather than absolute numbers.
Dashboard functionality limitations	State	State officials stated that the Dashboard data could not be filtered by State's domestic or overseas employees. According to OPM officials, this was due to a limitation in the data used to populate the Dashboard.
Dashboard data limitations	GSA	GSA officials reported gaps in the Dashboard data, specifically that the requirement eligibility view of the Dashboard was not displaying data.
Dashboard data limitations	NSF	NSF officials stated that the inability to extract agency-specific data from the Dashboard and the inability to view data in any form other than percentages impacted the agency's ability to use the Dashboard.
Dashboard data limitations	Small Business Administration (SBA)	SBA officials stated that the Dashboard's outdated data presented limitations to the agency during its prior attempts to use the data for making data-driven decisions, which then led to the agency not using the Dashboard.
Dashboard data limitations	State	State officials stated that the Dashboard could not be used for cyber workforce planning purposes because the Dashboard data did not include State Foreign Service employees.
Dashboard data limitations	Treasury	Treasury officials cited concerns regarding OPM's validation of the Dashboard data and its management of Dashboard changes as reasons for the agency's declining use of the Dashboard.

Source: GAO analysis of Office of Personnel Management Cyber Workforce Dashboard limitations reported by the six selected agencies. | GAO-26-108098

[a]The Office of Personnel Management's Federal Cyber Rotation Program was established by the Federal Rotational Cyber Workforce Program Act of 2021, Pub. L. No. 117-149, 136 Stat. 1289 (June 21, 2022). It provides opportunities for cyber workforce employees to serve in rotational assignments (or details) at agencies outside of their home agency. The details are non-reimbursable and last from 6 months to 1 year. The program helps federal agencies continue to enhance their cyber workforce by developing critical cyber skills and creating environments where employees have ongoing learning and development opportunities.

OPM Has Taken Actions to Address Limitations it Experienced in Managing the Dashboard

In addition to five of the six selected agencies not using the Dashboard, OPM, the administrator of the Dashboard, reported that it was not using the Dashboard for the agency's own cyber workforce planning purposes. OPM officials did not provide reasons as to why the agency did not use it. However, in their role as Dashboard Administrator, OPM officials cited observed limitations they encountered while managing the Dashboard. These limitations were similar to the types experienced by the six selected agencies. OPM has taken steps to address most of the limitations it identified.

Dashboard communication limitation. As previously mentioned, the Dashboard version for agencies is managed by a designated employee at each agency, known as a data champion. OPM officials described issues with identifying and assigning a Dashboard data champion at the agencies. In April 2025, OPM officials stated that approximately two-thirds of the agencies eligible to access the Dashboard version for agencies did not have a properly identified data champion. In July 2025, they stated this was due to turnover at many agencies and that they did not have contact information for some agencies. They noted there was still work to be done to expand agency access to the Dashboard. After our April 2025 meeting, OPM officials stated they had updated the data champion assignments. In July 2025, they stated that all but the following five agencies had an assigned data champion: Department of Defense, the Department of Health and Human Services, DHS, Justice, and USAID.

Dashboard access limitations. In April 2025, OPM officials cited limitations with the technology used to grant agency employee access to the Dashboard when it was initially launched. However, they stated that this limitation had since been addressed.

OPM officials also stated that in June 2025, technology changes were made to the Dashboard to move the application to a cloud environment. They noted these changes could have resulted in approximately 24 hours when the Dashboard might have been unavailable to both the public and agencies. However, they stated that there would have been a notice on the Dashboard that informed users the Dashboard was temporarily unavailable.

Dashboard functionality limitation. OPM officials acknowledged that the agency was aware that the Dashboard could have been developed to display more detailed cyber workforce data. However, they stated that the agency's overriding concern was to protect sensitive agency cyber workforce data while also providing a useful tool to the agencies.

Dashboard data limitations. In April 2025, OPM officials stated that they were aware of agencies experiencing limitations with authenticating and therefore accessing their individual Dashboard data. According to OPM officials, this was due to authentication barriers on the users end. They noted that OPM was in the process of transitioning to a different Dashboard data format that would resolve this limitation.

In addition, OPM did not routinely update the Dashboard data, and as of August 2025, the Dashboard was displaying September 2024 cyber workforce data. However, after our July 2025 meeting with OPM officials, the agency updated the Dashboard to display March 2025 data. They stated that after the government shutdown ended in November 2025, the agency updated the Dashboard data with September 2025 Hiring Manager Satisfaction Survey data as well as employee accessions and separations data.

The Dashboard Is Not Meeting Its Intended Purpose for the Selected Agencies

According to the OPM Dashboard website and OPM officials, the intended purpose of the Dashboard is to inform agencies' cyber workforce planning efforts and support data-driven decision making on current and

future cyber workforce requirements.[29] Additionally, OPM officials stated that the Dashboard was also intended to provide a comprehensive government-wide view of cyber work roles and competencies.

OPM officials stated the Dashboard was meeting its intended purpose as determined by the Federal Cyber Workforce Working Group. As previously stated, this group, co-chaired by ONCD and OMB, in consultation with OPM, established the Dashboard. Specifically, OPM officials stated the Dashboard provided agencies with the ability to access cyber workforce data, so they did not need to request it from OPM. OPM officials also noted that the Dashboard was meeting its intended purpose as it was aligned with ONCD's *National Cyber Workforce and Education Strategy* and organized federal cyber workforce data by individual roles.[30] Finally, OPM officials stated that the Dashboard was meeting its intended purpose by providing the public with government-wide cyber workforce data.

However, given the lack of use by the six selected agencies as well as OPM, the Dashboard is not meeting its purpose to inform cyber workforce planning efforts. Further, none of the six selected agencies reported using the Dashboard for data-driven decision making on current and future cyber workforce requirements.

According to guidance and related best practices, initiatives such as the Dashboard benefit from an evaluation of their effectiveness and the subsequent use of this information by agencies when making evidence-based decisions. For example, OMB's *Evidence-Based Policymaking* guidance for agencies encourages evaluating the overall performance of initiatives by measuring progress towards defined objectives and goals and making evidence-based decisions.[31] OPM's *Workforce Planning Guide* emphasizes the use of metrics to support timely interventions, as needed, to improve performance and overall efficiency of services.[32] In addition, GAO's *Key Principles for Effective Strategic Workforce Planning* framework highlights the importance of federal agencies using metrics to monitor and evaluate progress toward goals.[33]

However, OPM does not know the extent of non-use by the remaining 21 federal agencies that should have access to the Dashboard.[34] OPM officials stated that after the Dashboard version for agency use was launched in September 2023, OPM conducted an initial analysis to determine the extent of agency Dashboard usage by compiling and monitoring metrics including page views and unique visitors to the Dashboard, among others. However, OPM's actions only included ensuring agencies had access to the Dashboard, reviewing the quality of Dashboard data, and updating this data. OPM officials did not compile or monitor Dashboard usage

[29]The OPM Cyber Workforce Dashboard intended purpose is found on the Dashboard homepage, accessible at https://www.opm.gov/data/data-products/cyber-workforce-dashboard/.

[30]The White House, Office of the National Cyber Director, Executive Office of the President, *National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent* (Washington, D.C.: July 31, 2023).

[31]Office of Management and Budget, *Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans*, OMB M-21-27 (Washington, D.C.: June 2021).

[32]Office of Personnel Management, *Workforce Planning Guide* (Washington, D.C.: Nov. 2022).

[33]GAO-04-39.

[34]The 21 civilian agencies covered by the Chief Financial Officers (CFO) Act of 1990, 31 U.S.C. § 901(b) and identified for our review are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency, the General Services Administration, the National Aeronautics and Space Administration, the National Science Foundation, the Nuclear Regulatory Commission, the Small Business Administration, and the Social Security Administration. The Office of Personnel Management (OPM) and the U.S. Agency for International Development (USAID) are also civilian agencies covered by the CFO Act. However, we excluded them from our review because USAID recently underwent a significant reduction in workforce, and OPM is the focus of the engagement and was evaluated as the owner of the Cyber Workforce Dashboard.

metrics after the initial launch—metrics that could have been used to monitor progress and make evidence-based decisions.

OPM officials stated that they no longer collected data on Dashboard usage because OPM considered the Dashboard as an optional tool for agencies. Furthermore, OPM officials noted that the information sessions OPM provided to agencies when the Dashboard was initially launched were considered by OPM as the primary means of communication with agencies to discuss Dashboard usage and effectiveness.

In addition, OPM has not solicited feedback from agencies regarding the Dashboard after it was initially launched. OPM officials stated that while they experienced some issues with the Dashboard, as discussed earlier, they were not aware of the limitations identified by the selected agencies. Specifically, OPM officials stated that agencies had not requested more detailed data to be displayed in the Dashboard. OPM officials also stated that they were unaware of requests from agencies to add additional functionality or make changes to the Dashboard. As a result, they stated that OPM had not made any changes to the Dashboard based on agency feedback. However, OPM officials noted that OPM would consider potential future changes to the Dashboard in response to future federal cybersecurity initiatives or agency requests for Dashboard data.

Moreover, OPM officials stated they did not have an estimate of exact Dashboard costs dating back to the inception of the Dashboard, nor how much more funding would be needed for future planned operations and maintenance expenditures. According to OPM officials, the funds spent on the Dashboard effort since its inception were minimal and therefore not covered by a separate budget line item. They also stated that OPM's current Human Capital Data Management and Modernization Directorate operating budget was used to centrally fund the type of infrastructure and reporting provided by the Dashboard.[35] However, no additional information was available on costs of the Dashboard.

Although OPM maintained that it will consider future changes to the Dashboard, OPM's lack of data on the use and costs of the Dashboard increases the risk that it will continue to not meet its intended purpose. Further, without collecting agency feedback and addressing agency-identified limitations, OPM will be challenged in making effective evidence-based decisions regarding the future of the Dashboard. One key decision will be on whether it is beneficial for OPM to continue to offer the Dashboard or terminate the effort.

Conclusions

A robust federal cyber workforce is essential to withstand the ever-present threat posed by cyberattacks and to protect our nation's security. An important component to effectively maintaining this important segment of the workforce is access to accurate and timely cyber workforce data. When the Dashboard was created, OPM intended for this tool to inform agency cyber workforce planning efforts and to support data-driven decisions on current and future cyber workforce requirements.

However, in the face of challenges to increased agency use of the Dashboard, OPM has not evaluated the extent of the tool's non-use among the more than 20 federal agencies with access to the Dashboard, solicited feedback from agencies, or determined how much the Dashboard costs. Without this information, OPM would not know whether it should continue or terminate the Dashboard effort. Expeditiously collecting and analyzing

[35]OPM's Human Capital Data Management and Modernization Directorate is responsible for the agency's strategic use of government-wide human capital data for management, analytics, standards, and modernization initiatives.

such information, soliciting feedback from agencies, and determining costs are essential to determining the future of the Dashboard. Absent these critical data, OPM will lack the information needed to make evidence-based decisions, such as whether it is beneficial for OPM to terminate or to continue to offer the Dashboard with improvements.

Recommendations for Executive Action

The Director of the Office of Personnel Management should collect and analyze information on Dashboard use, solicit agency feedback on Dashboard limitations, determine the costs, and make an evidence-based decision to either terminate the Dashboard or continue offering it to agencies with needed improvements. (Recommendation 1)

Agency Comments and Our Evaluation

We provided a draft of this report to OPM and to six other agencies—GSA, Justice, NSF, SBA, State, and Treasury—for review and comment. We received written comments from OPM, which are reproduced in appendix I and summarized below. We also received responses from five of the other six agencies that stated they had no comments. The remaining agency, SBA, did not provide any comments.

In its written comments, OPM partially concurred with our recommendation. Noting the recently launched Federal Workforce Data website and its workforce management capabilities, OPM stated that it will engage with ONCD and OMB to review our findings and recommendation and determine what actions, if any, are appropriate.[36] We continue to believe that OPM's consideration of the Dashboard will be best served by gathering data that allow the agency to make an informed, evidence-based decision about the tool's future. OPM also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees; the Attorney General at the Department of Justice; the Secretaries of the Departments of State and the Treasury; the Administrators of the General Services and the Small Business Administration; the Directors of the National Science Foundation and the Office of Personnel Management; and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

[36]OPM's Federal Workforce Data website was launched in January 2026 and is the federal government's official source for comprehensive statistics and visualizations on the federal civilian workforce. It is accessible at https://data.opm.gov.

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

//SIGNED//

David B. Hinchman
Director, Information Technology and Cybersecurity

List of Addressees

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 Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Appendix I: Comments from the Office of Personnel Management

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

March 9, 2026

Ms. Orice Williams Brown
Acting Comptroller General
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Acting Comptroller General Williams Brown:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, Cyber Workforce: Evidence-Based Decision Needed for the Future of OPM's Dashboard, GAO-26-108098.

The response to your recommendation is provided below.

Recommendation: The Director of the Office of Personnel Management (OPM) should collect and analyze information on Dashboard use, solicit agency feedback on Dashboard limitations, determine the costs, and make an evidence-based decision to either terminate the Dashboard or continue offering it to agencies with needed improvements.

Management Response: We partially concur. At the request of the Office of the National Cyber Director (ONCD) and the Federal Cyber Workforce Working Group (FCWWG), OPM developed and hosted the Federal Cyber Workforce Dashboard to support agencies' efforts to support transparency and strengthen the federal cyber workforce. The FCWWG, established under the auspices of ONCD and co-chaired by ONCD and the Office of Management and Budget (OMB), provided strategic direction for this work. OPM provided technical development and ongoing platform support for the Dashboard and continues to provide human capital strategy expertise to inform cyber workforce strategies.

With the recent launch of OPM's Federal Workforce Data (FWD) website (https://data.opm.gov), which provides enhanced capabilities to share and leverage timely federal workforce data, OPM will engage with ONCD and OMB to review GAO's findings and recommendation and determine what actions, if any, are appropriate—such as whether the Dashboard should be improved, transitioned, continued, or sunset in light of the expanded data functionality now available through the FWD platform.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Andrew Hopkins, Deputy Director, Office of Legislative Affairs, via email at Andrew.Hopkins@opm.gov.

Sincerely,

Veronica E. Hinton
Associate Director
Workforce Policy and Innovation

Enclosure

Accessible Text for Appendix I: Comments from the Office of Personnel Management

March 9, 2026

Ms. Orice Williams Brown
Acting Comptroller General
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Acting Comptroller General Williams Brown:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, Cyber Workforce: Evidence-Based Decision Needed for the Future of OPM's Dashboard, GAO-26-108098.

The response to your recommendation is provided below.

Recommendation: The Director of the Office of Personnel Management (OPM) should collect and analyze information on Dashboard use, solicit agency feedback on Dashboard limitations, determine the costs, and make an evidence-based decision to either terminate the Dashboard or continue offering it to agencies with needed improvements.

Management Response: We partially concur. At the request of the Office of the National Cyber Director (ONCD) and the Federal Cyber Workforce Working Group (FCWWG), OPM developed and hosted the Federal Cyber Workforce Dashboard to support agencies' efforts to support transparency and strengthen the federal cyber workforce. The FCWWG, established under the auspices of ONCD and co-chaired by ONCD and the Office of Management and Budget (OMB), provided strategic direction for this work. OPM provided technical development and ongoing platform support for the Dashboard and continues to provide human capital strategy expertise to inform cyber workforce strategies.

With the recent launch of OPM's Federal Workforce Data (FWD) website (https://data.opm.gov), which provides enhanced capabilities to share and leverage timely federal workforce data, OPM will engage with ONCD and OMB to review GAO's findings and recommendation and determine what actions, if any, are appropriate—such as whether the Dashboard should be improved, transitioned, continued, or sunset in light of the expanded data functionality now available through the FWD platform.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Andrew Hopkins, Deputy Director, Office of Legislative Affairs, via email at Andrew.Hopkins@opm.gov.

Sincerely,

Veronica E. Hinton
Associate Director
Workforce Policy and Innovation

Enclosure

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

David B. Hinchman at HinchmanD@gao.gov

Staff Acknowledgments

In addition to the contact named above, Neelaxi Lakhmani (Assistant Director), Tammi Kalugdan (Assistant Director), Andrea Starosciak (Analyst in Charge), Olivia Adams, Jonnie Genova, Colin Jenkins, Smith Julmisse, Anh-Thi Le, and Andrew Stavisky 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 X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us