United States Government Accountability Office

Report to Congressional Requesters

September 2025

CYBER WORKFORCE

Actions Needed to Improve Size and Cost Data

GAO Highlights

Highlights of GAO-25-107405, a report to congressional requesters

September 2025

CYBER WORKFORCE

Actions Needed to Improve Size and Cost Data

Why GAO Did This Study

A resilient and skilled cyber workforce is essential to protecting government IT infrastructure from cyber threats and risks. ONCD's July 2023 National Cyber Workforce and Education Strategy recognized the importance of strengthening the federal cyber workforce. GAO has previously reported on needed improvements in managing the cyber workforce. Since 2019 it has made 64 recommendations to address cyber workforce issues; 32 of these are not yet fully implemented.

GAO was asked to review agencies' efforts to manage their cyber workforce. This report assesses whether federal civilian departments and agencies (agencies) (1) used quality data to identify the size and cost of their federal and contractor cyber workforce and (2) followed federal guidance to evaluate existing cyber workforce initiatives.

GAO analyzed documentation such as cyber workforce metrics and related assessments for 23 agencies. GAO then compared this documentation to guidance from OMB and OPM on agencies (1) using quality data to support strategic workforce planning and (2) evaluating the effectiveness of initiatives. GAO also interviewed key officials from agencies, OMB, and ONCD on cyber workforce data quality, initiatives, and related assessments.

What GAO Recommends

GAO is making four recommendations to ONCD to address workforce data gaps, quality assurance, cyber staff identification, and efforts to assess effectiveness. ONCD neither agreed nor disagreed with the recommendations.

For more information, contact David B. Hinchman at HinchmanD@gao.gov.

What GAO Found

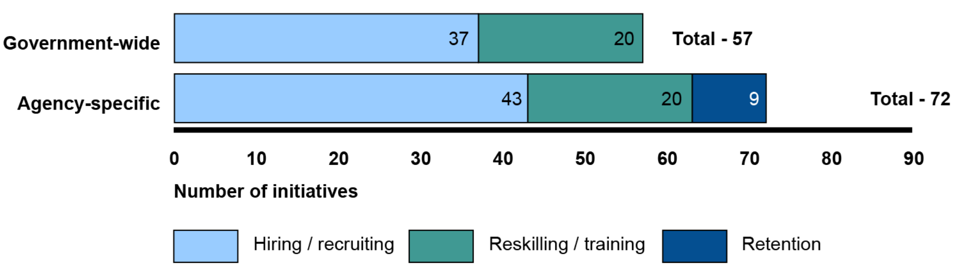
The federal cyber workforce consists of federal employees and contractors who perform IT, cybersecurity, and cyber-related functions. Federal guidance from the Office of Management and Budget (OMB) and Office of Personnel Management (OPM) call for having quality workforce data at the agency-level. In its 2023 cyber workforce strategy, the Office of the National Cyber Director (ONCD) also emphasized the importance of high-quality data for workforce management.

However, most agencies did not have quality information on their component-level and contractor cyber workforce. As a result, they could not accurately identify the size and cost of their cyber workforce. Using information readily available to agency-level offices, agencies reported at least 63,934 federal and 4,151 contractor staff at an annual cost of at least $9.3 billion and $5.2 billion, respectively, as of April 2024. However, these amounts are incomplete and unreliable and do not reflect the full size and cost of the cyber workforce.

A significant gap is that 22 of the 23 agencies reported partial or no data on their contractor cyber workforce. Further, 19 of 23 agencies did not have a documented quality assurance process to ensure accurate data. Also, 17 of 23 agencies lacked standardized procedures for identifying cyber employees. Until ONCD addresses these factors, it cannot ensure that agencies will have the information needed to support workforce decisions. This is especially important during administration transitions when new leadership needs assurance that the federal government is prepared and cyber-ready.

Twenty-two of the 23 agencies reported using various initiatives to help strengthen their federal cyber workforce through hiring/recruiting, reskilling/training, and retention efforts (see figure).

Total Number of Federal Cyber Workforce Initiatives Agencies Reported Using



Source: GAO analysis of data reported by federal agencies. | GAO-25-107405

However, agencies did not evaluate the effectiveness of most of these initiatives. Nine agencies evaluated aspects of costs, benefits, and performance while five agencies used assessments to justify expanding some of their initiatives. Agencies did not always evaluate effectiveness due, in part, to the lack of visibility into data to support such assessments. Further, ONCD's cyber workforce strategy did not call for such evaluations. Improved insight into the effectiveness of specific initiatives would help ONCD and agencies prioritize those providing the greatest return on investment.

Contents

Letter 1

Background 5
Agencies Lack Quality Workforce Size and Cost Data 11
Agencies Have Not Evaluated the Effectiveness of Most Cyber Workforce Initiatives 18
Conclusions 25
Recommendations for Executive Action 25
Agency Comments 26

Appendix I Objectives, Scope, and Methodology 28

Appendix II GAO Contact and Staff Acknowledgments 33

Figures

Figure 1: Agency Roles for Strengthening the Federal Cyber Workforce Through the National Cyber Workforce and Education Strategy (NCWES) 7
Figure 2: Examples of Federal Guidance and Tools for Cyber Workforce Planning 9
Figure 3: Total Number of Federal Cyber Workforce Initiatives Reported by Agencies 19

Abbreviations

CHCO	Chief Human Capital Officer
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
NCWES	National Cyber Workforce and Education Strategy
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

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 4, 2025

The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Andrew Garbarino
Chairman
Committee on Homeland Security
House of Representatives

Given the ever-present threat posed by cyberattacks and the risk of unauthorized access to IT systems, it is essential that federal departments and agencies ensure that proper workforce resources are in place to protect the government's technology infrastructure. A key component of the government's ability to mitigate and respond to cybersecurity threats is having a qualified, well-trained, federal and contractor cyber workforce with professionals who can help to prevent or mitigate vulnerabilities in federal IT systems.[1] As we have previously reported, strengthening and empowering the cyber workforce is one of the federal government's most important challenges.[2]

Nevertheless, the Office of Management and Budget (OMB), the Office of the National Cyber Director (ONCD), and our prior reports have highlighted that the federal government faces a persistent shortage of

[1] According to the Office of Personnel Management's (OPM) Cyber Workforce Dashboard, 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.

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

cyber and IT professionals.[3] In our 2024 High-Risk Series report, we identified four major cybersecurity challenges and 10 critical actions, which included addressing cybersecurity workforce management challenges.[4]

Given the importance of strengthening the federal and contractor cyber workforce, you asked us to review agencies' efforts to manage their cyber workforce. Our specific objectives were to assess whether civilian federal departments and agencies (agencies) (1) used quality data to identify the size and cost of their federal and contractor cyber workforce and (2) followed federal guidance to evaluate the effectiveness of their existing cyber workforce initiatives.

For our two objectives, we examined efforts from 23 of the 24 Chief Financial Officers Act agencies, excluding the Department of Defense.[5] For these agencies, we requested that agency-wide offices of the Chief Human Capital Officer (CHCO) and Chief Information Officer (CIO) provide cyber workforce data readily available to and managed by their offices. These offices have specific responsibilities for managing such information, as specified in OMB memorandum M-15-14, Circular A-130,[6]

[3] Office 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); *Cybersecurity Workforce: National Initiative Needs to Better Assess Its Performance*, GAO-23-105945 (Washington, D.C.: Jul. 27, 2023); and *Cybersecurity Workforce: Departments Need to Fully Implement Key Practices*, GAO-25-106795 (Washington, D.C.: Jan. 16, 2025); 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).

[4] GAO-24-107231.

[5] 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. The civilian CFO Act agencies include all of the aforementioned agencies except for the Department of Defense. We did not include the Department of Defense in our review due to ongoing, related work.

[6] OMB, *Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015); OMB, Circular A-130, Managing Information as a Strategic Resource (July 2016).

the Clinger-Cohen Act of 1996,[7] and the Federal Information Technology Acquisition Reform Act.[8] While such data may reside at component-level offices, we requested that agencies only provide workforce data readily available at the agency level.

For the purposes of this review, we applied the Office of Personnel Management's (OPM) definition of the cyber workforce to include employees in the federal government who were assigned a cyber position code or under contract to perform IT, cybersecurity, and cyber-related functions for an agency. We included contractors in our review because they can help fill mission-critical skill gaps and the extent of their use is expected to be part of agencies' strategic workforce planning.[9] We excluded individuals within the intelligence-related cyber workforce because certain agencies do not include them within OPM's human capital data systems.

To address our first objective, we reviewed federal guidance such as OMB Circular A-130 and OPM's strategic workforce playbook to identify guidance for tracking workforce resources.[10] We also requested and reviewed data readily available to agency-wide offices of the CHCO and CIO on the size and cost of each agency's federal and contractor cyber workforce, as of April 2024. Due to the sensitivity regarding data on the size and cost of individual agencies' cyber workforce, we reported this information in the aggregate.

To assess the reliability of agency-reported cyber workforce data, we reviewed agency documentation, where available, on the functionality of systems that produced the data, guidance on how staff are to identify cyber-coded employees, and automated and manual quality assurance processes. We also asked officials to describe any limitations or assumptions in the data provided. Further, we reviewed raw and summary data that agencies provided and compared it to other sources,

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

[8] Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (Dec. 19, 2014).

[9] GAO-25-106795.

[10] OMB, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016); and OPM, *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).

including OPM's cyber workforce dashboard and FedScope, to identify any significant inconsistencies or outliers.[11] We determined that the data were sufficiently reliable for the purpose of identifying information that agency-wide offices of the CHCO and CIO had readily available on the size and cost of their cyber workforce and for comparing that information to other sources. This report describes limitations and challenges in agencies' efforts to report complete and accurate information on the size and cost of their cyber workforce using data readily available to agency-wide CHCOs and CIOs.

To address our second objective, we reviewed federal guidance, such as OMB's memorandum on evidence-based policymaking and Circular A-94, as well as OPM's Workforce Planning Guide and Evaluation System Standards.[12] We then identified relevant guidance and recommendations for agencies to evaluate the effectiveness of cyber workforce initiatives.

We reviewed documentation—such as agency websites, CIO memorandums, workforce plans, and national strategies—to identify government-wide and agency-specific initiatives that agencies used to hire, recruit, reskill, train, and retain cyber talent. We then compared agency documentation, where available, to federal guidance for agencies to evaluate the effectiveness of cyber workforce initiatives. To do so, we analyzed agencies' efforts to evaluate the effectiveness of initiatives through assessments of costs, benefits, and performance such as program evaluations or other pertinent assessments.

For both objectives, we interviewed relevant officials from agencies' offices of the CHCO and CIO to obtain data and perspectives on quality assurance processes, data limitations, cyber workforce initiatives, and related assessments. We also interviewed officials from OMB, ONCD, and OPM to obtain their government-wide perspectives on the federal cyber workforce and efforts to implement the National Cyber Workforce

[11] FedScope is a web-based tool developed by OPM that offers detailed data-driven insights and reports about the federal workforce.

[12] OMB, *Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans*, M-21-27 (Washington, D.C.: June 2021); and *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs,* Circular A-94 (Revised 2023); OPM, *Workforce Planning Guide* (Washington, D.C.: November 2022); and *Evaluation System Standards* (Revised September 2021).

and Education Strategy.[13] Additional details about our objectives, scope, and methodology are discussed in appendix I.

We conducted this performance audit from February 2024 to September 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

In March 2023 and July 2023, respectively, the White House released the National Cybersecurity Strategy and an accompanying implementation plan that included goals for strengthening the nation's cyber workforce.[14] Additionally, 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 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.

The strategy also called for agencies to explore steps needed, including working with Congress to expand CyberCorps Scholarship for Service

[13] 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).

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

and similar initiatives and programs to meet workforce needs across the federal government.[16] In addition, the strategy identified the need for better data-informed decision making based on high-quality data to guide federal cyber workforce management such as projecting cyber workforce needs and executing evidence-based workforce strategies.

The White House released an accompanying report in June 2024 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.

ONCD officials stated that, as of February 2025, they have suspended meetings within a working group that coordinated efforts among federal agencies while awaiting guidance from a new National Cyber Director. As a result, ONCD officials also stated that an updated report on agencies' progress in implementing the National Cyber Workforce and Education Strategy will not be produced until after October 2025.

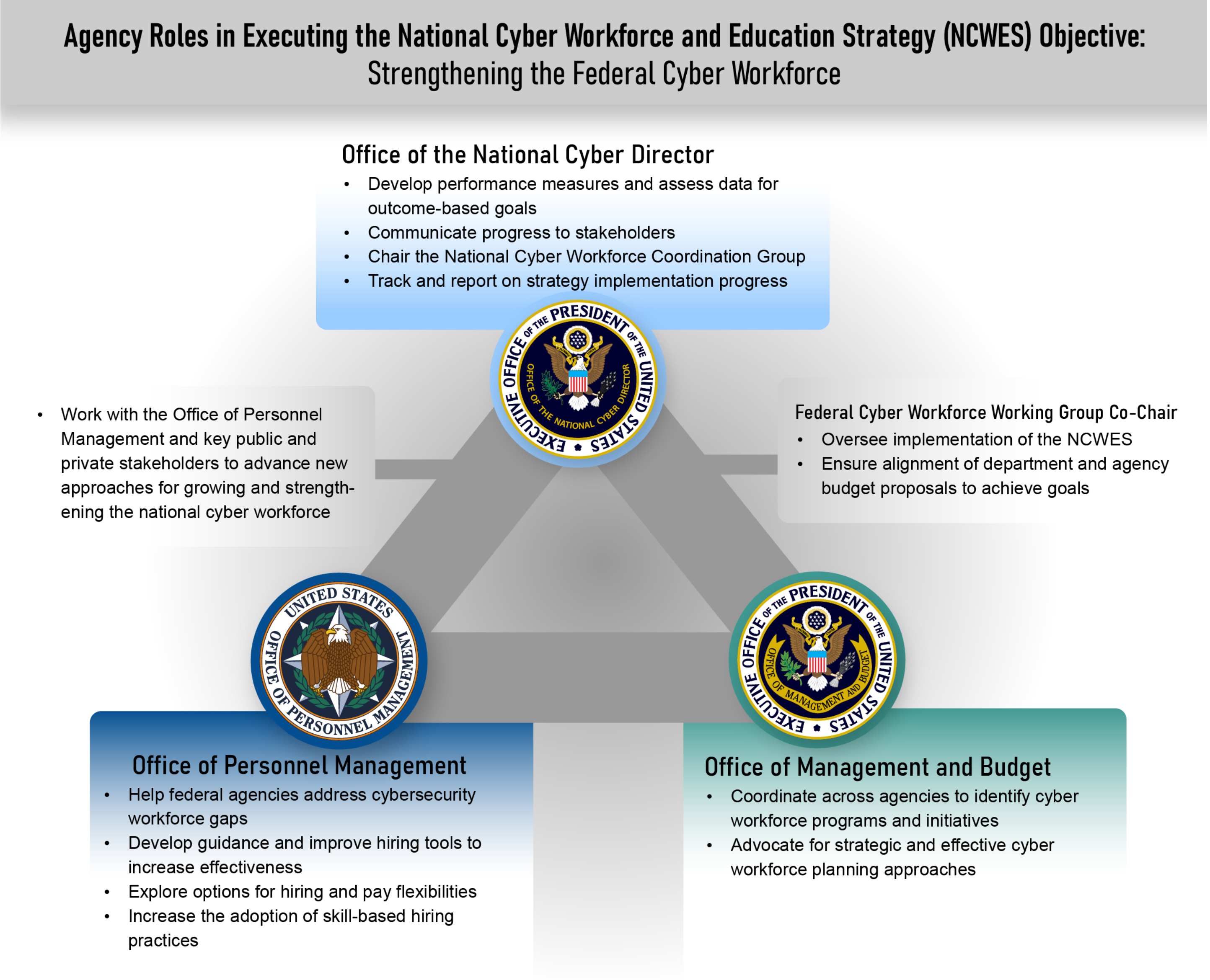
Agency Roles for Cyber Workforce Management

The White House's 2023 strategy documents identified agencies that are to have roles in implementing national efforts to strengthen the federal cyber workforce. Specifically, ONCD is to lead efforts to oversee the implementation of the National Cyber Workforce and Education Strategy with support from OMB and OPM, as well as other agencies. Figure 1 highlights the roles and responsibilities of ONCD, OMB, and OPM in implementing national efforts to strengthen the federal cyber workforce.

[16] The CyberCorps Scholarship for Service Program provides participating institutions of higher education with scholarships to students in approved IT and cybersecurity fields of study. As a condition of receiving scholarships, students are required to enter agreements to work in qualifying full-time jobs at federal, state, local, or tribal agencies upon graduation for a period equal in length to their scholarship. 15 U.S.C. § 7442.

[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).

Figure 1: Agency Roles for Strengthening the Federal Cyber Workforce Through the National Cyber Workforce and Education Strategy (NCWES)



Agency Roles in Executing the National Cyber Workforce and Education Strategy (NCWES) Objective: Strengthening the Federal Cyber Workforce

Office of the National Cyber Director

- Develop performance measures and assess data for outcome-based goals
- Communicate progress to stakeholders
- Chair the National Cyber Workforce Coordination Group
- Track and report on strategy implementation progress

- Work with the Office of Personnel Management and key public and private stakeholders to advance new approaches for growing and strengthening the national cyber workforce

Federal Cyber Workforce Working Group Co-Chair

- Oversee implementation of the NCWES
- Ensure alignment of department and agency budget proposals to achieve goals

Office of Personnel Management

- Help federal agencies address cybersecurity workforce gaps
- Develop guidance and improve hiring tools to increase effectiveness
- Explore options for hiring and pay flexibilities
- Increase the adoption of skill-based hiring practices

Office of Management and Budget

- Coordinate across agencies to identify cyber workforce programs and initiatives
- Advocate for strategic and effective cyber workforce planning approaches

Sources: GAO analysis of information from the Office of Management and Budget and the Office of the National Cyber Director; agencies (logos). | GAO-25-107405

In addition, according to the July 2023 National Cyber Workforce and Education strategy, the Cybersecurity and Infrastructure Security Agency (CISA) is to contribute to the Department of Homeland Security's (DHS) efforts to help strengthen the federal cyber workforce. For example, CISA provides learning opportunities to reskill and develop cyber talent.

Specifically, CISA manages the Federal Cyber Defense Skilling Academy, which provides full-time federal employees an opportunity to focus on professional growth through a full-time, virtual accelerated training program. The academy offers courses to prepare professionals for various cyber-related positions in areas such as defensive cybersecurity, incident detection and response, artificial intelligence and machine learning, and vulnerability assessment. CISA also manages a federal learning platform, called CISA Learning, which aims to support employee development of transferable skills and helps to improve career pathways into the federal government. Additionally, among other things, CISA added micro-challenges on its website for cybersecurity career exploration and established its Cybersecurity Workforce Development and Training for Underserved Communities initiative to expand training and retention opportunities.

Federal Cyber Workforce Guidance and Tools

In response to the Federal Cybersecurity Workforce Assessment Act, OPM and the National Institute of Standards and Technology (NIST) issued guidance to increase agencies' understanding of their cyber workforce (to include IT, cybersecurity, and cyber-related functions) through implementing various workforce planning processes.[18] These processes and tools can help federal agencies ensure that they have sufficient resources to execute their missions and program goals, including strengthening the federal cyber workforce.

For example, according to NIST, it updated its National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (also known as the NICE Framework) to include a common lexicon for categorizing cybersecurity roles.[19] In addition, OPM issued its Workforce Planning Guide to help agencies assess workforce resources and launched a Cyber Workforce Dashboard to help agencies track relevant

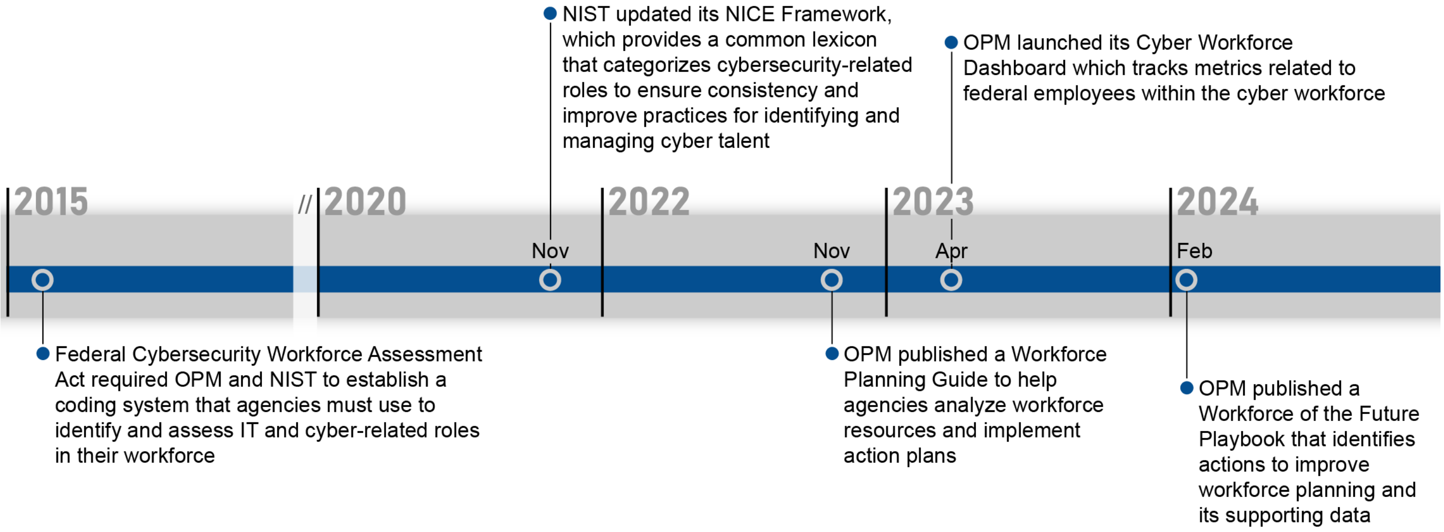
[18] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title III, 129 Stat. 2241, 2975 (Dec. 18, 2015). 5 U.S.C. § 301 note.

[19] 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.

cyber workforce metrics. OPM also published a Workforce of the Future Playbook to identify actions helpful for improving workforce planning.[20]

Figure 2 illustrates examples of workforce guidance and tools developed to help agencies make workforce planning decisions.

Figure 2: Examples of Federal Guidance and Tools for Cyber Workforce Planning


NIST updated its NICE Framework, which provides a common lexicon that categorizes cybersecurity-related roles to ensure consistency and improve practices for identifying and managing cyber talent
OPM launched its Cyber Workforce Dashboard which tracks metrics related to federal employees within the cyber workforce
2015
//
2020
Nov
2022
Nov
2023
Apr
2024
Feb
Federal Cybersecurity Workforce Assessment Act required OPM and NIST to establish a coding system that agencies must use to identify and assess IT and cyber-related roles in their workforce
OPM published a Workforce Planning Guide to help agencies analyze workforce resources and implement action plans
OPM published a Workforce of the Future Playbook that identifies actions to improve workforce planning and its supporting data

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

Source: GAO analysis of information reported by NIST and OPM. | GAO-25-107405

GAO Has Previously Made Recommendations to Address Cyber Workforce Challenges

We have previously reported on various cyber workforce management challenges and programs within the federal government.

- In January 2025, we reported that five departments varied in their implementation of 15 applicable practices for workforce planning.[21] Most of the selected departments reported that they had not fully

[20] National Institute of Standards and Technology, *Workforce Framework for Cybersecurity (NICE Framework*), Special Publication 800-181 revision 1 (Gaithersburg, MD: November 2020); OPM, *Workforce Planning Guide* (Washington, D.C.: November 2022); *Evaluation System Standards* (Revised September 2021); and *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).

[21] GAO, *Cybersecurity Workforce: Departments Need to Fully Implement Key Practices*, GAO-25-106795 (Washington, D.C.: Jan. 16, 2025).

implemented all 15 practices due, in part, to managing their cybersecurity workforce at the component level rather than the departmental level, as intended by OPM. While agencies identified inadequate funding and difficulties with recruiting and retaining cyber talent as major challenges, none of the departments had evaluated their actions taken to determine the extent to which they had been effective in addressing them.

Accordingly, we made 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. As of June 2025, the recommendations have not been implemented.

- 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.[22] Specifically, among the nine selected key practices for establishing a program performance process, NIST fully implemented the practice for involving stakeholders, partially implemented five, and did not implement 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 June 2025, the recommendations have not been implemented.
- In September 2022, we reported that OPM and the National Science Foundation (NSF) varied in their compliance with 19 selected legal requirements for how they are to manage the CyberCorps Scholarship for Service program.[23] Specifically, OPM and NSF fully complied with 13 of the requirements and partially complied with six, which include requiring recipients to provide OPM annual verifiable documentation of post-award employment and NSF to periodically report on program performance. Moreover, NSF did not implement a risk management strategy and process to effectively identify, analyze, mitigate, and report on program risks and challenges.

[22] GAO, *Cybersecurity Workforce: National Initiative Needs to Better Assess Its Performance*, GAO-23-105945, (Washington, D.C.: July 27, 2023).

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

We made three recommendations to NSF and two to OPM to comply with legal requirements and implement a risk management strategy. Both agencies agreed with our recommendations. As of June 2025, NSF addressed its three recommendations and OPM addressed one recommendation and did not yet address the other.

- In March 2019, we reported that agencies needed to accurately categorize positions to effectively identify critical staffing needs.[24] Specifically, the 24 CFO Act agencies generally assigned OPM codes to relevant positions within their cyber workforce. However, six agencies did not assign work role codes (cyber position codes) to vacant positions. Further, 22 agencies likely miscategorized their positions by assigning a non-IT/cyber code or "000" to 15,779 (about 19 percent) of their positions within the GS-2210 IT management occupational series. The six agencies that we selected for additional review had assigned cyber position codes that were not consistent with the work roles and duties described in corresponding position descriptions for 63 of 120 positions within the GS-2210 occupational series that we examined.

  As a result, we made 28 recommendations to 22 agencies to review and assign the appropriate codes to their IT, cybersecurity, and cyber-related positions. The 22 agencies have implemented all the recommendations.

Agencies Lack Quality Workforce Size and Cost Data

Agency-level CHCOs and CIOs in our review lacked quality in the information that was readily available on their federal and contractor cyber workforce. Consequently, agencies had limited visibility into and usually could not accurately identify the full size and cost of their federal and contractor cyber workforce. Further, agencies lacked documented data quality assurance processes and varied in how they identified cyber personnel. This was due, in part, to ONCD not identifying steps that are needed to improve the quality of cyber workforce data used by agency-level CHCOs and CIOs.

Federal Guidance Recommends Quality Data to Manage the Cyber Workforce

Federal guidance from OMB and OPM call for federal agency CHCOs and CIOs to track workforce resources using quality data to support strategic workforce planning and decision-making. Specifically, OMB Circular A-130 requires agencies to develop and maintain a workforce planning process to recruit and retain IT talent needed to accomplish the

[24] GAO, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs,* GAO-19-144, (Washington, D.C.: Mar. 12, 2019).

mission.[25] OPM's Workforce Planning Guide calls for agencies to track the size and cost of their workforce.[26] In particular, this information helps agencies establish a baseline for effectively managing and aligning resources as part of their workforce planning processes. We have previously reported that strategic workforce planning associated with an organization's total workforce includes full- and part-time federal staff and contractors.[27] For example, agencies are to have workforce plans that include strategies such as recruiting, training, and using contractors, among other things.[28]

Additionally, OPM guidance recommends that agencies' data be accurate, timely, and readily available to agencies and agency leaders through dashboards, reports, and research studies and are consistently used to inform workforce policy decisions.[29] To do so, OPM calls for agencies to, among other efforts, ensure data standards are implemented, improve data accuracy and timeliness, and set targets to track key workforce data.

Various Issues Limited Cyber Workforce Data Quality

Agency-level offices of the CHCO and CIO reported data on the size and cost of their federal and contractor cyber workforce—identifying a total federal cyber workforce of at least 63,934 employees at a salary-based cost of $9,396,606,633, based on readily available data as of April 2024. Federal agencies also reported the size and cost of their contractor cyber workforce—reporting at least 4,151 contractor staff with $5,222,725,515 in associated labor costs, as of April 2024.

However, agency-level CHCOs and CIOs lacked quality data when reporting the size and cost of their federal and contractor cyber workforce. Specifically, agencies:

[25] OMB, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016); and OPM, *Workforce Planning Guide* (November 2022).

[26] OPM, *Workforce Planning Guide* (November 2022).

[27] GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning,* GAO-04-39, (Washington, D.C.: Dec. 11, 2003).

[28] GAO-25-106795.

[29] OPM, *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).

- had gaps in data about their federal or contractor cyber workforce, or both;
- lacked documented data quality assurance processes; and
- varied in how they identified cyber personnel.

Gaps in Federal and Contractor Cyber Workforce Data

Regarding the federal cyber workforce, 19 of the 23 agencies provided size and cost data that they believed represented their entire federal cyber workforce and the remaining four agencies reported partial data. Of the 19 agencies that provided data on their entire cyber workforce, 14 reported that they had high confidence or were generally confident in their data regarding the federal cyber workforce. Among the four agencies that provided partial data, two agencies' offices of the CIO did not have visibility into the size and cost of their cyber workforce at the component level or outside of their respective offices, one agency did not have access to detailed salary data, and one did not have supporting documentation. For example:

- The National Aeronautics and Space Administration reported data on the size and cost of its federal cyber workforce. However, the reported size and cost only represented the cyber workforce within the agency's Cybersecurity and Privacy Division, which resides in the office of the CIO. According to office of the CIO officials, the agency's other components manage their federal cyber workforce. Additionally, officials acknowledged that the office of the CIO has limited insight into the entire agency's federal cyber workforce as it lacks a mechanism to identify all cyber roles across the agency.
- The Department of Health and Human Services reported on the total size and cost of its federal cyber workforce. However, it did not have documentation to support 79 percent of its reported federal cyber workforce.

Regarding the contractor cyber workforce, one agency—OPM—reported size and cost data that it believed represented its entire contractor cyber workforce, 14 agencies reported partial data, and eight agencies did not have data to report. Generally, agencies attributed their data gaps to either the lack of an agency-wide reporting mechanism or the structure of their contracts. Agency officials stated that obtaining data on their contractor cyber workforce required an agency-wide data call or manual review. For example:

- The Department of Education could not report the number of contractor staff performing cyber-related functions for the agency due to the structure of its contracts. The agency reported data on contractor labor costs in fiscal year 2024 based on its IT budget-related reporting on external labor costs and outside services associated with IT investments. Officials stated that it could not distinctly identify contractor labor without including administrative, service, and other associated costs.

- The Department of Energy stated that it could not report on the size or cost of the agency's contractor cyber workforce. According to agency officials, Energy was unable to identify its contractor resources because the structure of its contracts limited its ability to track labor costs per full-time equivalent and its procurement system lacked cyber identifiers. Officials also stated that identifying the size and cost of the agency's contractor cyber workforce required a manual data collection process and the agency did not believe its efforts would yield valuable information.

Lack of Documented Quality Assurance Processes

Although most agencies reported that they had a high level of confidence in their cyber workforce data, they did not have documented quality assurance procedures for how their offices of the CHCO and CIO could ensure the accuracy of the data. Specifically, 19 of 23 agencies did not have a documented quality assurance process.

One agency documented quality assurance steps intended for their component agencies, but the steps did not include oversight from the CIO or CHCO offices. Additionally, the remaining 18 agencies did not document procedures to ensure the accuracy of their cyber workforce data.

A lack of documented quality assurance processes can contribute to data discrepancies and reduce the accuracy of agencies' cyber workforce data. For example, the fiscal year 2024 federal and contractor labor costs reported by agencies on the Federal IT Dashboard were $1.56 billion and $23.9 billion (approximately five times) higher than, respectively, what the agencies reported to us.[30]

[30] The Federal IT Dashboard is a public, government website operated by the General Services Administration at https://itdashboard.gov/. It includes data on IT investments to enable agencies and Congress to better understand and manage federal IT portfolios. We compared agencies' federal and contractor cyber workforce costs—total annual salaries and contract labor costs—with the total "internal labor" and "external labor" costs associated with IT investments on the dashboard.

Further, agencies' reported total number of GS-2210 IT management employees in April 2024 was 11 percent less than OPM FedScope data as of March 2024.[31] For example, two agencies that did not document quality assurance steps had the largest discrepancies with OPM data. Specifically:

- The Department of Agriculture reported 89 percent fewer total number of cyber-coded employees compared to the data OPM had for the agency, as of April 2024. Additionally, we identified that the agency reported 90 percent fewer total GS-2210 IT management occupational series[32] employees as of April 2024 compared to OPM's FedScope in March 2024. According to the agency, its office of the CIO had readily available data on employees conducting cyber-related work at the agency level but not within component-level offices. Agency officials stated that OPM's reported data may have included mission-area employees. Agency officials stated that the office of the CIO does not validate cyber position codes for the entire agency.[33]
- The Department of Health and Human Services reported 42 percent fewer GS-2210 IT management employees in April 2024 compared to data that OPM had via FedScope as of March 2024. Agency officials stated that it is challenging for the offices of the CHCO and CIO to achieve agency-wide visibility into the size of the agency's federal cyber employees due to the unique nature of each component agency's mission.

In contrast to those agencies without quality assurance processes, the Department of Transportation monitors cyber-coded positions on a bi-weekly basis and generates quarterly reports for the office of the CHCO's

[31] FedScope is a web-based tool developed by OPM that offers detailed data-driven insights and reports about the federal workforce.

[32] According to OPM, an occupational series is a grouping of positions with a similar line of work and qualification requirements. For example, the 2210 IT management occupational series covers positions that manage, supervise, lead, administer, develop, deliver, and support information technology systems and services. This series covers positions for which the paramount requirement is knowledge of IT principles, concepts, and methods (e.g., data storage, software applications, and networking). For the purposes of this report, we also refer to the GS-2210 IT management occupational series as GS-2210 IT management positions.

[33] According to OPM, cyber position codes are used to identify incumbents or positions that have IT, cybersecurity, or cyber-related work roles. Use of this code enables OPM and federal agencies to identify the cyber workforce, determine baseline capabilities, examine hiring trends, identify skill gaps, and more effectively recruit, hire, train, develop, and retain an effective cyber workforce.

review. These quarterly reports support the agency's strategic priority to ensure a 98 percent accuracy rate on pay actions and a 95 percent rate on non-pay actions.

Varied Approaches to Identifying Cyber Personnel

Agencies varied in how they implemented OPM's guidance and the NICE Framework when applying OPM's cyber position codes to employees. For example, the Environmental Protection Agency's procedures required cyber position codes for federal employees who spend at least 10 percent of their time performing IT, cybersecurity, or cyber-related duties as part of their current role. Similarly, the Department of State used a 25 percent threshold for determining whether a position should be cyber coded.

Moreover, most agencies (17 of the 23) lacked procedures with defined thresholds for identifying cyber employees. According to OPM officials, such determinations impact the accuracy of agencies' reported size and cost of their federal cyber workforce because employees may perform a combination of cyber and non-cyber roles.

In addition, two agencies used codes to indicate that hundreds of employees were not part of their cyber workforce. However, the occupational series associated with these employees indicated that they were performing IT, cybersecurity, or cyber-related functions. As a result, these agencies likely undercounted the size of their federal cyber workforce.

For example, according to Department of Homeland Security officials, the agency assigned a "000" cyber position code—meaning that IT or cybersecurity work was not applicable—to 688 of its GS-2210 IT management employees, including IT project managers.[34] According to agency officials, the position description for an IT project manager within one component did not include any references to cybersecurity and an applicable code was not found in the NICE Framework. However, the position description included IT duties that align with OPM standards and the NICE Framework's position code for IT project managers.

[34] According to OPM standards, agencies must assign "000" to positions that do not perform IT, cybersecurity, or cyber-related work roles and functions. We previously reported that GS-2210 IT management positions are most likely to perform IT, cybersecurity, or cyber-related functions, as defined by the NICE Framework. See GAO, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C.: Mar. 12, 2019).

According to officials within the Department of Homeland Security's office of the CHCO, OPM is the sole decider as to whether cyber coding is correct and accurate as prescribed and OPM did not report any concerns with the "000" assigned to an IT project manager. Nevertheless, OPM officials stated federal agencies are responsible for validating the quality of the cyber workforce data submitted. Further, according to OPM officials, while its human resources system automatically verifies completeness of agency reporting, the agency does not perform any assurance of codes assigned by agencies. By not having documented procedures of the thresholds for when a cyber position code is to be applied or not applied, agencies are more likely to have less accurate cyber workforce data.

Incomplete Cyber Workforce Data Is Due, in Part, to Lack of ONCD Guidance

The data quality issues led to agency-wide CHCOs and CIOs having reduced visibility into their component-level federal cyber workforce and contractor cyber workforce. Further, agencies had discrepancies in their reporting. As a result, agencies usually could not identify the full size and cost of their federal and contractor workforce and had less assurance that their reported totals were complete and accurate.

The concerns with data quality exist in part because ONCD has not identified steps that are needed to improve the quality of cyber workforce data used by agency-level CHCOs and CIOs. ONCD and OMB have recognized the importance of having quality data on the cyber workforce and established working groups to strengthen data-informed decision making. Nonetheless, issues remain with respect to data gaps, quality assurance processes, and variances in identifying cyber personnel.

As the lead on national cyber policy and strategy, ONCD is responsible for coordinating and implementing activities intended to improve the security posture of government systems.[35] These activities rely on having adequate cyber workforce resources. In the National Cyber Workforce and Education Strategy, ONCD emphasized the importance of using high-quality data to improve workforce management. It also stated that reaching the federal government's hiring goals requires continued improvements to data on the federal cyber workforce. To do so, ONCD established a line of effort to enable better data-informed decision making by strengthening the use of work roles or cyber codes.

[35] Pub. L. No. 116-283, Div. A, Title XVII, § 1752, 134 Stat. 3388, 4144 (Jan. 1, 2021), codified at 6 U.S.C. § 1500.

However, as the co-chairs of the Federal Cyber Workforce Working Group—the lead for implementing the effort—ONCD and OMB did not identify any plans to strengthen the quality of cyber workforce data to inform decisions. Further, it is not clear whether the efforts of the working group will continue. ONCD officials stated that, as of February 2025, they have suspended meetings within a working group that coordinated efforts among federal agencies while awaiting guidance from a new National Cyber Director. This could potentially result in changes in direction that the working group takes to implement goals for strengthening the federal workforce. Further, the Administration has initiated a number of ongoing actions to reshape the federal workforce.[36]

The lack of quality data available to agency-level CHCOs and CIOs hinders visibility into cyber workforce resources and affects strategic efforts to meet national and agency-specific cyber workforce priorities. Until ONCD takes steps to improve the quality of information on agencies' cyber workforce resources, it cannot ensure that agencies have baseline, quality data from which to support cyber workforce decisions. This can be especially important during times of change or transition in the federal workforce when new leadership needs assurance that the federal government is prepared and cyber ready.

Agencies Have Not Evaluated the Effectiveness of Most Cyber Workforce Initiatives

Almost all agencies identified government-wide and agency-specific initiatives used to strengthen their federal cyber workforce. However, agencies did not evaluate the effectiveness of most cyber initiatives consistent with guidance from OMB and OPM.

Agencies Identified Numerous Federal Cyber Workforce Initiatives

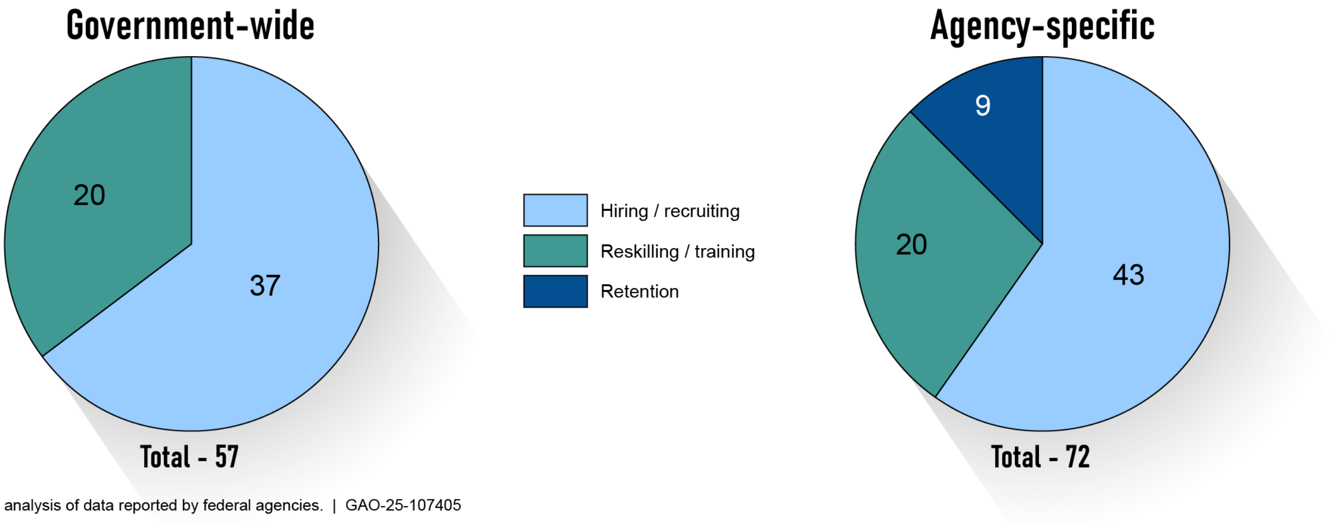
Almost all of the federal agencies reported using various initiatives to help strengthen their cyber workforce. Specifically, 22 of the 23 agencies identified government-wide or agency-specific initiatives used to build and maintain a skilled cyber workforce through targeted hiring/recruiting, reskilling/training, and retention efforts.[37]

[36] See, e.g., OMB and OPM, *Guidance on Agency RIF and Reorganization Plans Requested by Implementing the President's "Department of Government Efficiency" Workforce Optimization Initiative,* Memorandum to Heads of Executive Departments and Agencies (Feb. 26, 2025).

[37] Commerce did not identify any initiatives or programs it uses to strengthen its cyber workforce.

Figure 3 illustrates the total number of government-wide and agency-specific federal cyber workforce initiatives that agencies reported using across three major categories.

Figure 3: Total Number of Federal Cyber Workforce Initiatives Reported by Agencies



Source: GAO analysis of data reported by federal agencies. | GAO-25-107405

Note: The data represents totals from 22 of the 24 CFO Act agencies, excluding the Departments of Defense and Commerce. Fourteen of the 129 initiatives are from hiring authorities such as Direct-Hire Authority, Special Salary Rates, and Career Conditional Appointments. To use these authorities, OPM must determine that there is either a severe shortage of candidates or a critical hiring need for a position or group of positions.

Government-wide. Twenty of the 22 agencies reported government-wide hiring/recruiting initiatives such as Tech to Gov, the Cybersecurity and Artificial Intelligence Talent Initiative, Pathways, and other government-wide cyber workforce initiatives. These programs are aimed at helping agencies to hire both entry-level cyber talent and experienced, highly skilled professionals. Additionally, 11 of the 22 agencies also reported using CyberCorps Scholarship for Service, which intends to build a pipeline of skilled professionals for U.S. government agencies.[38]

[38] CyberCorps Scholarship for Service is a unique program designed to recruit and train the next generation of IT professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for federal, state, local, and tribal governments. In return for their scholarships, recipients must agree to work after graduation at qualifying federal, state, local, or tribal agencies, in a position related to cybersecurity, for a period equal to the length of the scholarship.

In addition, 13 of the 22 agencies used government-wide reskilling/training programs to equip personnel with new skills to transition to a different role or enhance their existing expertise to meet evolving workforce needs. For example, agencies cited using detailee programs among agencies and upskilling programs. CISA's Federal Cyber Security Defense Skilling Academy[39] and OPM's Federal Cyber Rotation Program[40] were among the most reported training and reskilling initiatives.[41]

Agency-specific. Twenty of the 22 agencies reported using agency-specific hiring/recruiting, reskilling/training, and retention initiatives. For example, DHS reported using its Cybersecurity Talent Management System to increase its cyber workforce. According to DHS officials, the program enables the agency to effectively recruit, develop, and maintain cyber talent with specific skills. DHS stated that it also allows the agency to offer individuals salaries comparable to contractors and place them into cyber positions as federal employees.

Additionally, 13 of the 22 agencies reported using hiring authorities, such as career conditional appointments[42] and Direct-Hire Authority to fill critical cyber roles.[43] For example, OPM expanded its Direct-Hire

[39] According to DHS, CISA's Federal Cyber Security Defense Skilling Academy provides full-time federal employees an opportunity to focus on professional growth through a full-time accelerated training program. The program is also available to those interested in developing foundational cybersecurity skills.

[40] OPM's Federal Cyber Rotation Program was created 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.

[41] The Federal Rotational Cyber Workforce Program Act required certain federal agencies to develop and issue a program operation plan with policies, processes, and procedures for detailing employees among rotational cyber workforce positions at other agencies. It also mandated GAO to assess and report on the operation and effectiveness of the program by September 2026. Public Law No. 117-149.

[42] According to OPM, career conditional appointments refer to permanent federal employees in the competitive service who have not completed 3 years of substantially continuous service to become a full career employee.

[43] Direct-Hire Authority allows agencies to appoint candidates to positions without regard to the requirements in 5 U.S.C. §§ 3309-3318. In order for an agency to use direct hire, OPM must determine that there is either a severe shortage of candidates or a critical hiring need for a position or group of positions.

Authority for cyber roles in December 2023 to include artificial intelligence-related positions to adapt to the growing need of related skills. Additionally, in September 2024, OPM extended and expanded the authority to include cyber positions—such as IT cybersecurity specialists and computer engineers—to attract talent and address critical workforce gaps. The Departments of the Treasury and Transportation reported that leveraging hiring authorities have made the greatest impact on expanding their respective federal cyber workforce.

Furthermore, six agencies offered retention incentives such as special salary rates for the GS-2210 IT management employees and student loan repayment. For example, Justice developed a retention program aimed at offering competitive salary rates for its skilled professionals.

Agencies Have Not Evaluated the Effectiveness of Most Initiatives

According to OMB and OPM guidance, agencies are to evaluate the effectiveness of workforce initiatives to support related decisions and plans.[44] Specifically, agencies are to assess the costs, benefits, and overall performance of their initiatives to inform data-driven workforce decisions, such as initiating, renewing, expanding, or discontinuing programs to meet their goals.

However, most agencies did not evaluate the effectiveness of their federal cyber workforce initiatives. Nine agencies evaluated aspects of effectiveness for 13 of their reported 56 government-wide and agency-specific initiatives but did not do so for 43 other initiatives. The remaining 13 agencies did not assess any of their 73 reported initiatives, meaning that only 13 of 129 (or approximately 10 percent) of total reported initiatives were evaluated.

Specifically, nine agencies—the Departments of Agriculture, Education, Energy, Homeland Security, Justice, and State; the OPM and NSF; and the Social Security Administration—evaluated aspects of costs, benefits, and performance for the 13 initiatives they reviewed. For example:

- Energy evaluated the cost, benefits, and performance for one of its six initiatives. The agency's Cybersecurity Retention Incentive Program was designed to offer a pay incentive to current cyber employees,

[44] OMB, *Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans*, OMB M-21-27 (Washington, D.C.: June 2021); *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs;* and Circular A-94 (Revised 2023); OPM, *Evaluation System Standards* (Revised September 2021); and *Workforce Planning Guide* (November 2022).

with unusually high or unique qualifications and skills, who would be likely to leave the government in the absence of a retention incentive. Energy reported the total cost of its program and the number of enrollees.

In addition, the agency conducted a program evaluation, which compared past separation rates among eight work roles of critical need to the rates 1 year into the incentive program. It found that across the eight critical work roles, four separation rates declined, one stayed the same, and three rates increased slightly. Energy also conducted an annual mid-point survey that found 93 percent of respondents were positively impacted to stay beyond their service agreement. Energy found that 61 percent of recipients who participated in the program from fiscal year 2023 to 2024 indicated that the incentive actively supported their decision to stay within the agency.

- NSF did not evaluate its two agency-specific initiatives. However, it evaluated benefits and performance of the government-wide CyberCorps Scholarship for Service program. NSF operates this program in conjunction with OPM and DHS. Specifically, NSF, in coordination with OPM, evaluated the benefits and performance of the program in January 2024. According to NSF, the Scholarship for Service program has graduated more than 4,000 participants over the past 20 years. The agency reported that graduated scholars have joined and provided cybersecurity expertise to more than 145 government organizations, including more than 700 participants placed at the National Security Agency. The agency also reported that 31.3 percent of Scholarship for Service participants stayed in the same position in the federal government for an average of 7 years or more after completing their obligation.

  NSF also assessed performance metrics such as placement rates, placement locations, time in position upon graduation, number of participants released from obligations, and whether remedial training was required. However, the agency had not demonstrated that it assessed the costs of the program to help inform its effectiveness. As previously mentioned, we issued a prior report on additional challenges associated with NSF's and OPM's efforts to assess and report the performance of their Scholarship for Service program.[45]

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

Additionally, several agencies demonstrated tracking the number of attendees at agency hiring and career events. For example, Education reported that 130 attendees visited their booth at the Scholarship for Service hiring event held in January 2024 and 100 students expressed their interests in cyber careers at the agency. However, none of the agencies demonstrated effectiveness by linking attendance to the number of applications following the event.

For the 13 agencies that did not evaluate any aspect of the 73 initiatives they reported, most identified their three most impactful initiatives in the past 5 years. However, none demonstrated that their conclusions were supported by an assessment of effectiveness. For example, according to Nuclear Regulatory Commission officials, its direct hiring authority, summer internship program, and Co-Operative Education program were among its top three initiatives that made the greatest impact to the agency's federal cyber workforce.[46] However, the agency did not assess the effectiveness of its cyber workforce initiatives to support its assertion.

Of the nine agencies that evaluated aspects of their initiatives' costs, benefits, or performance, five agencies—Agriculture, Energy, NSF, OPM, and State—used assessments to justify expanding five of their 26 initiatives. For example, State made a data-driven decision to expand one of its initiatives—its Cybersecurity Skill Initiative Program. The department previously documented plans to expand this initiative in fiscal year 2025. The department based its decision on its assessment of the program's cost, benefits, performance, and other factors. As part of its justification package, State provided a written basis, criteria, and recommendations for continuing the program into 2025.

The remaining 17 agencies did not make such determinations for any of their 103 initiatives, meaning that 22 agencies evaluated less than 4 percent of their initiatives.[47] Although nine agencies cited informal plans to initiate, expand, or maintain their existing initiatives, they did not

[46] The Nuclear Regulatory Commission's Co-Operative Education Program aims to recruit students, while still in school, to fill permanent positions upon graduation. Student participants alternate between periods of academic study and work experience, or parallel periods of academic study and work experience. This program is available to undergraduate and graduate students in science, engineering, technology, and other disciplines related to the Nuclear Regulatory Commission's mission.

[47] As previously mentioned, Commerce did not identify any initiatives it uses to strengthen its cyber workforce. Therefore, we could not assess whether Commerce evaluated expansion of its initiatives.

demonstrate that their plans were documented and informed by assessments of their cyber workforce initiatives.

Officials from the offices of the CHCO and CIO cited various reasons for their lack of visibility into the cost, benefits, and performance-related data to assess the effectiveness of their federal cyber workforce initiatives and inform data-driven workforce decisions. For example, agencies and agency officials noted that assessing the effectiveness of federal cyber workforce initiatives was not a priority or a role within their offices of the CHCO and CIO. Specifically:

- The Small Business Administration and Department of Veterans Affairs prioritized other federal cyber workforce planning efforts—such as assessing competencies, supply, and demand of GS-2210 IT management employees—over assessing metrics on the effectiveness of initiatives.
- Officials from Commerce stated that the agency lacks a governance framework to assess effectiveness of federal cyber workforce initiatives.
- Officials from Labor stated that conducting such evaluations is not a role within the agency's offices of the CHCO and CIO.
- Officials from State noted that the decentralized nature of the agency makes it challenging to gather the information related to cyber workforce initiatives across its components.

Agencies have not evaluated the effectiveness of their initiatives in part because ONCD's National Cyber Workforce and Education Strategy does not require agencies to do so. Nevertheless, such assessments are a key aspect of hiring and retaining a qualified workforce and supporting related data-driven decisions. As the lead for cyber policy and strategy, ONCD is responsible for leading collaboration with other relevant entities to monitor and assess the effectiveness, (e.g., cost-effectiveness) of cyber programs and policies.[48]

Until ONCD directs agencies to evaluate the effectiveness of their initiatives, ONCD's goal of strengthening the federal cyber workforce through strategic workforce initiatives will be difficult to measure and may not be achieved. Further, improved insight into effective initiatives may

[48] Pub. L. No. 116-283, Div. A, Title XVII, § 1752, 134 Stat. 3388, 4144 (Jan. 1, 2021), codified at 6 U.S.C. § 1500.

help agencies prioritize initiatives with the greatest impact and return on investment.

Conclusions

In light of the serious external threats posed to government IT systems, strengthening the cyber workforce is one of the federal government's most important challenges. However, the current lack of quality workforce data due to data gaps, lack of documented quality assurance processes, and variances in identifying cyber personnel limits what agencies know about the size and cost of their federal and contractor cyber workers. This also limits the quality of input available for agencies to make important strategic workforce planning decisions. Additional guidance to agencies on how to improve the quality and consistency of their cyber workforce data could help establish a baseline from which the government can more effectively align this important resource. Such a baseline can provide agencies with the information needed to ensure that appropriate cyber resources are focused where and when they are needed to address growing and changing cyber threats.

In addition, while agencies identified over a hundred initiatives to hire, recruit, reskill, train, and retain talented federal cyber workers, little information is being collected on what impact these programs are having or whether to scale back or expand them. Similar to workforce data quality, additional direction on determining initiative effectiveness could help agencies strengthen their cyber workforce and further support key federal cyber priorities.

Recommendations for Executive Action

We are making four recommendations to ONCD:

The National Cyber Director, in collaboration with OMB and other federal agencies as appropriate, should expeditiously take steps to address gaps in cyber workforce size and cost data used by agency-level CIOs and CHCOs. (Recommendation 1)

The National Cyber Director, in collaboration with OMB and other federal agencies as appropriate, should expeditiously take steps to address the lack of documented quality assurance processes in cyber workforce data used by agency-level CIOs and CHCOs. (Recommendation 2)

The National Cyber Director, in collaboration with OMB and other federal agencies as appropriate, should expeditiously take steps to address variances in identifying cyber personnel in cyber workforce data used by agency-level CIOs and CHCOs. (Recommendation 3)

The National Cyber Director, in collaboration with OMB and other entities as appropriate, should direct federal agencies to assess the effectiveness of agency-specific cyber workforce initiatives using costs, benefits, performance, and other relevant metrics. (Recommendation 4)

Agency Comments

We provided a draft of this report to ONCD, OMB, and the 23 civilian CFO Act agencies for their review and comment. We received responses from all of the agencies except one, as summarized below. ONCD, the only agency to which we made recommendations, did not agree or disagree with those recommendations.

In a response emailed by the ONCD Acting General Counsel, the agency neither agreed nor disagreed with our four recommendations and stated that the report will serve as a retrospective assessment of federal cyber workforce data collection efforts during the previous Administration. ONCD said that there should be improvement on data quality on the size and cost of the federal cyber workforce, as well as the collaborative processes used to collect and evaluate data. ONCD noted that it is dependent on collaboration with OMB and OPM to issue guidance for agencies to improve programs and reconcile data on the federal cyber workforce. ONCD also provided technical comments, which we incorporated as appropriate.

Three agencies—Commerce, DHS, and the National Aeronautics and Space Administration—provided technical comments, which we incorporated as appropriate. Twenty agencies—the Departments of Agriculture, Education, Energy, Health and Human Services, 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 Science Foundation, the Nuclear Regulatory Commission, OPM, the Small Business Administration, the Social Security Administration, and the U.S. Agency for International Development—did not have any comments on the report. OMB did not provide comments on the report.

We are sending copies of this report to the appropriate congressional committees, the heads of the agencies in our review, and other interested parties. In addition, this report is available at no charge on the GAO website at http://www.gao.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 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 II.

//SIGNED//

David B. Hinchman
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to assess whether civilian federal agencies (agencies) (1) used quality data to identify the size and cost of their federal and contractor cyber workforce and (2) followed federal guidance to evaluate the effectiveness of their existing cyber workforce initiatives.

For our two objectives, we examined efforts from 23 of the 24 Chief Financial Officers Act agencies, excluding the Department of Defense.[1] For these agencies, we requested that agency-wide offices of the Chief Human Capital Officer (CHCO) and Chief Information Officer (CIO) provide cyber workforce data readily available to and managed by their offices. These offices have specific responsibilities for managing such information, as specified in OMB memorandum M-15-14, Circular A-130,[2] the Clinger-Cohen Act of 1996,[3] and the Federal Information Technology Acquisition Reform Act.[4] While such data may reside at component-level offices, we requested that agencies provide readily available data at the agency-level.

For the purposes of this review, we applied the Office of Personnel Management's (OPM) definition of the cyber workforce to include employees in the federal government who were assigned a cyber-position code or under contract to perform IT, cybersecurity, and cyber-related functions for an agency. We included contractors in our review because they can help fill mission-critical skill gaps and the extent of their use is expected to be part of agencies' strategic workforce planning.[5] We

[1] 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. The civilian CFO Act agencies include all of the aforementioned agencies except for the Department of Defense. We did not include the Department of Defense in our review due to ongoing, related work.

[2] OMB, *Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015); OMB, Circular A-130, *Managing Information as a Strategic Resource* (July 2016).

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

[4] Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (Dec. 19, 2014).

[5] GAO-25-106795.

excluded individuals within the intelligence-related cyber workforce because certain agencies do not include them within OPM's human capital data systems.

To address our first objective, we reviewed federal guidance such as OMB Circular A-130, OPM's strategic workforce playbook, and OPM's Workforce Planning Guide to identify guidance and recommendations for tracking workforce resources such as size and costs.[6] We also requested and reviewed data readily available to agency-level offices of the CHCO and CIO on the size and cost of each agency's federal and contractor cyber workforce, as of April 2024.

To do so, we requested:

- the total number of federal cyber workforce employees with a breakdown total for each OPM cyber position code;
- the average annual salary (referred to by OPM as "annualized adjusted basic pay") for federal cyber workforce employees with a breakdown total for each OPM cyber position code;
- a breakdown of the total number of employees by work status, including non-seasonal, full-time permanent federal employees, and other employees; and
- a breakdown of the total number of employees by occupational series.

We also requested similar data for agencies' contractor cyber workforce, as applicable. Given its sensitive nature, we reported the size and cost of the agencies' cyber workforce in the aggregate.

To assess the reliability and quality of agency-reported cyber workforce data, we reviewed agency documentation, where available, on the functionality of systems that produced the data, guidance on how staff are to identify cyber-coded employees, and automated and manual quality assurance processes. We also asked officials to describe any limitations or assumptions in the data provided. Further, we reviewed raw and summary data that agencies provided and compared it to other sources,

[6] OMB, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016); OPM, *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).

including OPM's cyber workforce dashboard, OPM's FedScope,[7] and the General Service Administration's Federal IT Dashboard to identify any significant inconsistencies or outliers.[8] We determined that the data were sufficiently reliable for the purpose of identifying information that agency-wide offices of the CHCO and CIO had readily available on the size and cost of their cyber workforce and for comparing that information to other sources.

We used the results to ask agencies to identify their confidence level in the reported data and to provide the quality assurance processes used to validate the data. We assessed agencies' efforts to track their resources based on whether they reported data on the size and cost for their entire federal and contractor cyber workforce. This report also describes limitations and challenges in agencies' efforts to report complete and accurate information on the size and cost of their cyber workforce using data readily available to agency-level CHCOs and CIOs. Given its sensitive nature, we reported the size and cost of agencies' cyber workforce in the aggregate.

To address our second objective, we reviewed federal guidance, such as OMB's memorandum on evidence-based policymaking and Circular A-94 as well as OPM's Workforce Planning Guide and Evaluation System Standards.[9] We then identified relevant guidance for agencies to evaluate the effectiveness of cyber workforce initiatives. We reviewed documentation—such as agency websites, workforce plans, CIO memorandums, and national strategies—to identify government-wide and

[7] FedScope is a web-based tool developed by OPM that offers detailed data-driven insights and reports about the federal workforce.

[8] The Federal IT Dashboard is a public, government website operated by the General Services Administration at https://itdashboard.gov/. It includes streamlined data on IT investments to enable agencies and Congress to better understand and manage federal IT portfolios. We compared agencies' federal and contractor cyber workforce costs—total annual salaries and contract labor costs— with the total "internal labor" and "external labor" costs associated with IT investments on the dashboard.

[9] OMB, *Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans*, OMB M-21-27 (Washington, D.C.: June 2021); and *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs,* Circular A-94 (Revised 2023); OPM, *Workforce Planning Guide* (Washington, D.C.: November 2022); and *Evaluation System Standards* (Revised September 2021).

agency-specific initiatives that agencies used to hire, recruit, reskill, train, and retain cyber talent.

We asked agencies to identify their own initiatives used to strengthen their cyber workforce. To summarize the various cyber workforce initiatives across the government, we compiled a list of government-wide and agency-specific cyber workforce initiatives from various sources, including agency websites, program overviews, and workforce plans. We confirmed those that were relevant and used by the agencies, and categorized the initiatives as one of three types—hiring/recruiting, reskilling/training, and retention. We included any hiring authorities that agencies identified, such as direct hire, special salary rates, and career conditional appointments under the hiring and recruiting category.

We then requested and reviewed documentation, where available, demonstrating agencies' efforts to evaluate the effectiveness of initiatives through assessments. Specifically, we requested and reviewed cost-benefit analyses, program evaluations, and other assessments that demonstrated agencies' efforts to evaluate the costs, benefits, and performance of their cyber workforce initiatives. We then compared agency documentation, where available, to federal guidance for agencies to evaluate the effectiveness of cyber workforce initiatives.

We determined the extent to which agencies assessed effectiveness of initiatives by evaluating their efforts. We determined that an agency fully evaluated effectiveness if the agency assessed the effectiveness of each cyber workforce initiative it had identified. We determined that an agency partially evaluated effectiveness if the agency assessed aspects of costs, benefits, or performance for some, but not all, of its initiatives. We determined that an agency had not evaluated effectiveness if the agency did not assess its initiatives.

For both objectives, we interviewed and obtained perspectives from relevant officials within agencies' agency-level offices of the CHCO and CIO to obtain data on quality assurance processes, data limitations, cyber workforce initiatives, and related assessments. We also interviewed and requested information from agencies to clarify the data and gain insight into the quality assurance processes the agencies used, if any, to validate the information. We also interviewed officials from OMB, ONCD, and OPM to obtain their government-wide perspectives on the federal cyber workforce and efforts to implement the National Cyber Workforce and Education Strategy.[10]

We conducted this performance audit from February 2024 to September 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.

[10] 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).

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

David Hinchman at hinchmand@gao.gov

Staff Acknowledgments

In addition to the individual named above, Josh Leiling (Assistant Director), Torrey Hardee (Analyst-in-Charge), Amanda Andrade, Prisca Anyiam, Chris Businsky, Olga Dye, Corey Evans, Rebecca Eyler, Hassan Kane, and Andrew Stavisky made key 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

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

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