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

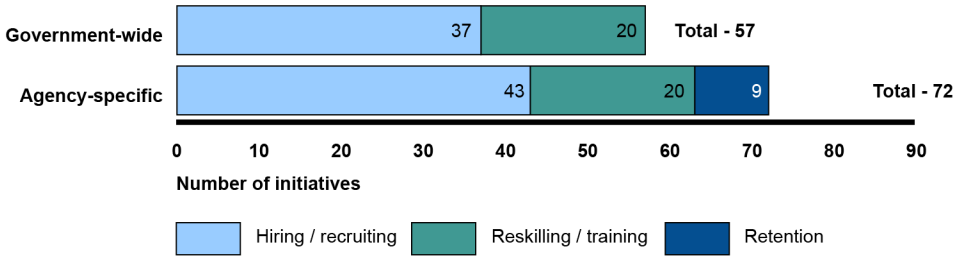
The federal cyber workforce consists of federal employees and contractors who perform IT, cybersecurity, and cyber-related functions. Federal guidance from the Office of Management and Budget (OMB) and Office of Personnel Management (OPM) call for having quality workforce data at the agency-level. In 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.