January 2025

CYBERSECURITY WORKFORCE

Departments Need to Fully Implement Key Practices

GAO Highlights

Highlights of GAO-25-106795, a report to congressional addressees

Why GAO Did This Study

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

What GAO Recommends

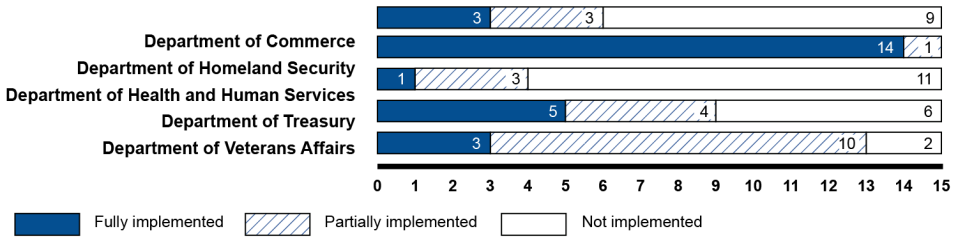
GAO is making a total of 23 recommendations to the five departments--Commerce, Homeland Security, Health and Human Services, Treasury, and Veterans Affairs--to fully implement applicable practices and determine the effectiveness of mitigation actions. Three departments agreed with the recommendations,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

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

What GAO Found

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

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



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

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

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

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

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

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