April 4, 2017

GAO Highlights

Highlights of GAO-17-533T, a testimony before the Subcommittee on Information Technology, Committee on Oversight and Government Reform, House of Representatives

CYBERSECURITY

Federal Efforts Are Under Way That May Address Workforce Challenges

Why GAO Did This Study

The federal government faces an ever-evolving array of cyber-based threats to its systems and information. Further, federal systems and networks are inherently at risk because of their complexity, technological diversity, and geographic dispersion, among other reasons. GAO has designated the protection of federal information systems as a government-wide high-risk area since 1997. In 2001, GAO introduced strategic government-wide human capital management as another area of high risk. A key component of the government's ability to mitigate and respond to cyber threats is having a qualified, well-trained cybersecurity workforce. However, shortages in qualified cybersecurity professionals have been identified, which can hinder the government's ability to ensure an effective workforce.

This statement discusses challenges agencies face in ensuring an effective cybersecurity workforce, recent initiatives aimed at improving the federal cyber workforce, and ongoing activities that could assist in recruiting and retaining cybersecurity professionals. In preparing this statement, GAO relied on published work related to federal cybersecurity workforce efforts, and information reported by other federal and non-federal entities focusing on cybersecurity workforce challenges.

What GAO Recommends

Over the past several years, GAO has made several recommendations to federal agencies to enhance their IT workforce efforts. Agencies are in various stages of implementing these recommendations.

View GAO-17-533T. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

GAO and others have identified a number of key challenges facing federal agencies in ensuring that they have an effective cybersecurity workforce:

- **Identifying skills gaps:** As GAO reported in 2011, 2015, and 2016, federal agencies have faced challenges in effectively implementing workforce planning processes for information technology (IT) and defining cybersecurity staffing needs. GAO also reported that the Office of Personnel Management (OPM) could improve its efforts to close government-wide skills gaps.
- **Recruiting and retaining qualified staff:** Federal agencies continue to be challenged in recruiting and retaining qualified cybersecurity staff. For example, in August 2016, GAO reported that federal chief information security officers faced significant challenges in recruiting and retaining personnel with high-demand skills.
- **Federal hiring activities:** The federal hiring process may cause agencies to lose out on qualified candidates. In August 2016 GAO reported that OPM and agencies needed to assess available federal hiring authorities to more effectively meet their workforce needs.

To address these and other challenges, several executive branch initiatives have been launched and federal laws enacted. For example, in July 2016, OPM and the Office of Management and Budget issued a strategy with goals, actions, and timelines for improving the cybersecurity workforce. In addition, laws such as the Federal Cybersecurity Workforce Assessment Act of 2015 require agencies to identify IT and cyber-related positions of greatest need.

Further, other ongoing activities have the potential to assist agencies in developing, recruiting, and retaining an effective cybersecurity workforce. For example:

- **Promoting cyber and science, technology, engineering and mathematics (STEM) education:** A center funded by the Department of Homeland Security (DHS) developed a kindergarten to 12th grade-level cyber-based curriculum that provides opportunities for students to become aware of cyber issues, engage in cyber education, and enter cyber career fields.
- **Cybersecurity scholarships:** Programs such as Scholarship for Service provide tuition assistance to undergraduate and graduate students studying cybersecurity in exchange for a commitment to federal service.
- **National Initiative for Cybersecurity Careers and Studies:** DHS, in partnership with several other agencies, launched the National Initiative for Cybersecurity Careers and Studies in 2013 as an online resource to connect government employees, students, educators, and industry with cybersecurity training providers across the nation.

If effectively implemented, these initiatives, laws, and activities could further agencies' efforts to establish the cybersecurity workforce needed to secure and protect federal IT systems.