GAO
Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-8, a report to the Chairman, Subcommittee on Immigration, Refugees, and Border Security, Committee on the Judiciary, United States Senate

November 2011

CYBERSECURITY HUMAN CAPITAL

Initiatives Need Better Planning and Coordination

Why GAO Did This Study

Threats to federal information technology (IT) infrastructure and systems continue to grow in number and sophistication. The ability to make federal IT infrastructure and systems secure depends on the knowledge, skills, and abilities of the federal and contractor workforce that implements and maintains these systems.

In light of the importance of recruiting and retaining cybersecurity personnel, GAO was asked to assess (1) the extent to which federal agencies have implemented and established workforce planning practices for cybersecurity personnel and (2) the status of and plans for governmentwide cybersecurity workforce initiatives.

GAO evaluated eight federal agencies with the highest IT budgets to determine their use of workforce planning practices for cybersecurity staff by analyzing plans, performance measures, and other information. GAO also reviewed plans and programs at agencies with responsibility for governmentwide cybersecurity workforce initiatives.

What GAO Recommends

GAO is making recommendations to enhance individual agency cybersecurity workforce planning activities and to address governmentwide cybersecurity workforce challenges through better planning, coordination, and evaluation of governmentwide activities. Agencies concurred with the majority of GAO's recommendations and outlined steps to address them. Two agencies did not provide comments on the report.

View GAO-12-8 or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Valerie C. Melvin at (202) 512-6304 or melvinv@gao.gov.

What GAO Found

Federal agencies have taken varied steps to implement workforce planning practices for cybersecurity personnel. Five of eight agencies, including the largest, the Department of Defense, have established cybersecurity workforce plans or other agencywide activities addressing cybersecurity workforce planning. However, all of the agencies GAO reviewed faced challenges determining the size of their cybersecurity workforce because of variations in how work is defined and the lack of an occupational series specific to cybersecurity. With respect to other workforce planning practices, all agencies had defined roles and responsibilities for their cybersecurity workforce, but these roles did not always align with guidelines issued by the federal Chief Information Officers Council and National Institute of Standards and Technology (NIST). Agencies reported challenges in filling highly technical positions, challenges due to the length and complexity of the federal hiring process, and discrepancies in compensation across agencies. Although most agencies used some form of incentives to support their cybersecurity workforce, none of the eight agencies had metrics to measure the effectiveness of these incentives. Finally, the robustness and availability of cybersecurity training and development programs varied significantly among the agencies. For example, the Departments of Commerce and Defense required cybersecurity personnel to obtain certifications and fulfill continuing education requirements. Other agencies used an informal or ad hoc approach to identifying required training.

The federal government has begun several governmentwide initiatives to enhance the federal cybersecurity workforce. The National Initiative for Cybersecurity Education, coordinated by NIST, includes activities to examine and more clearly define the federal cybersecurity workforce structure and roles and responsibilities, and to improve cybersecurity workforce training. However, the initiative lacks plans defining tasks and milestones to achieve its objectives, a clear list of agency activities that are part of the initiative, and a means to measure the progress of each activity. The Chief Information Officers Council, NIST, Office of Personnel Management, and the Department of Homeland Security (DHS) have also taken steps to define skills, competencies, roles, and responsibilities for the federal cybersecurity workforce. However, these efforts overlap and are potentially duplicative, although officials from these agencies reported beginning to take steps to coordinate activities. Furthermore, there is no plan to promote use of the outcomes of these efforts by individual agencies. The Office of Management and Budget and DHS have identified several agencies to be service centers for governmentwide cybersecurity training, but none of the service centers or DHS currently evaluates the training for duplicative content, effectiveness, or extent of use by federal agencies. The Scholarship for Service program, run by the National Science Foundation, is a small though useful source of new talent for the federal government, but the program lacks data on whether its participants remain in the government long-term.