GAO Highlights

Highlights of GAO-19-144, a report to congressional committees

March 2019

CYBERSECURITY WORKFORCE

Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs

Why GAO Did This Study

A key component of mitigating and responding to cyber threats is having a qualified, well-trained cybersecurity workforce. The act requires OPM and federal agencies to take several actions related to cybersecurity workforce planning. These actions include categorizing all IT, cybersecurity, and cyber-related positions using OPM personnel codes for specific work roles, and identifying critical staffing needs.

The act contains a provision for GAO to analyze and monitor agencies' workforce planning. GAO's objectives were to (1) determine the extent to which federal agencies have assigned work roles for positions performing IT, cybersecurity, or cyber-related functions and (2) describe the steps federal agencies took to identify work roles of critical need. GAO administered a questionnaire to 24 agencies, analyzed coding data from personnel systems, and examined preliminary reports on critical needs. GAO selected six of the 24 agencies based on cybersecurity spending levels to determine the accuracy of codes assigned to a random sample of IT positions. GAO also interviewed relevant OPM and agency officials.

What GAO Recommends

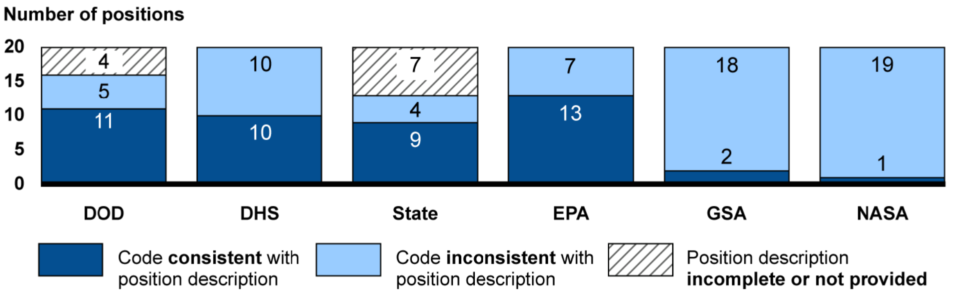
GAO is making 28 recommendations to 22 agencies to review and assign the appropriate codes to their IT, cybersecurity, and cyber-related positions. Of the 22 agencies to which GAO made recommendations, 20 agreed with the recommendations, one partially agreed, and one did not agree with one of two recommendations. GAO continues to believe that all of the recommendations are warranted.

View GAO-19-144. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

What GAO Found

The 24 reviewed federal agencies generally assigned work roles to filled and vacant positions that performed information technology (IT), cybersecurity, or cyber-related functions as required by the *Federal Cybersecurity Workforce Assessment Act of 2015* (the act). However, six of the 24 agencies reported that they had not completed assigning the associated work role codes to their vacant positions, although they were required to do so by April 2018. In addition, most agencies had likely miscategorized the work roles of many positions. Specifically, 22 of the 24 agencies assigned a "non-IT" work role code to 15,779 (about 19 percent) of their IT positions within the 2210 occupational series. Further, the six agencies that GAO selected for additional review had assigned work role codes that were not consistent with the work roles and duties described in corresponding position descriptions for 63 of 120 positions within the 2210 occupational series that GAO examined (see figure).

Consistency of Assigned Work Role Codes with Position Descriptions for Random Sample of IT Positions Within the 2210 Occupational Series at Six Selected Agencies



DOD (Department of Defense), DHS (Department of Homeland Security), State (Department of State), EPA (Environmental Protection Agency), GSA (General Services Administration), NASA (National Aeronautics and Space Administration),

Source: GAO analysis of DOD, DHS, State, NASA, EPA and GSA cybersecurity coding data. | GAO-19-144

Human resource and IT officials from the 24 agencies generally reported that they had not completely or accurately categorized work roles for IT positions within the 2210 occupational series, in part, because they may have assigned the associated codes in error or had not completed validating the accuracy of the assigned codes. By assigning work roles that are inconsistent with the IT, cybersecurity, and cyber-related positions, the agencies are diminishing the reliability of the information they need to improve workforce planning.

The act also required agencies to identify work roles of critical need by April 2019. To aid agencies with identifying their critical needs, the Office of Personnel Management (OPM) developed guidance and required agencies to provide a preliminary report by August 2018. The 24 agencies have begun to identify critical needs and submitted a preliminary report to OPM that identified information systems security manager, IT project manager, and systems security analyst as the top three work roles of critical need. Nevertheless, until agencies accurately categorize their positions, their ability to effectively identify critical staffing needs will be impaired.