GAO Highlights

Highlights of GAO-18-175, a report to congressional committees

February 2018

CYBERSECURITY WORKFORCE

Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements

Why GAO Did This Study

DHS is the lead agency tasked with protecting the nation's critical infrastructure from cyber threats. The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* required DHS to identify, categorize, and assign employment codes to all of the department's cybersecurity workforce positions. These codes define work roles and tasks for cybersecurity specialty areas such as program management and system administration. Further, the act required DHS to identify and report its cybersecurity workforce critical needs.

The act included a provision for GAO to analyze and monitor DHS's implementation of the requirements. GAO's objectives were to assess the extent to which DHS has (1) identified, categorized, and assigned employment codes to its cybersecurity positions and (2) identified its cybersecurity workforce areas of critical need. GAO analyzed DHS and OPM workforce documentation and administered a data collection instrument to six major DHS components. GAO also interviewed relevant DHS and OPM officials.

What GAO Recommends

GAO recommends that DHS take six actions, including ensuring that its cybersecurity workforce procedures identify position vacancies and responsibilities; reported workforce data are complete and accurate; and plans for reporting on critical needs are developed. DHS concurred with our six recommendations and described actions the department plans to take to address them. OPM did not have any comments.

View GAO-18-175. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Chris P. Currie at (404) 679-1875 or curriec@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) has taken actions to identify, categorize, and assign employment codes to its cybersecurity positions, as required by the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*; however, its actions have not been timely and complete. For example, DHS did not establish timely and complete procedures to identify, categorize, and code its cybersecurity position vacancies and responsibilities. Further, DHS has not yet completed its efforts to identify all of the department's cybersecurity positions and accurately assign codes to all filled and vacant cybersecurity positions. In August 2017, DHS reported to the Congress that it had coded 95 percent of the department's identified cybersecurity positions. However, GAO's analysis determined that the department had, at that time, coded approximately 79 percent of the positions. DHS's 95 percent estimate was overstated primarily because it excluded vacant positions, even though the act required DHS to report these positions.

In addition, although DHS has taken steps to identify its workforce capability gaps, it has not identified or reported to the Congress on its department-wide cybersecurity critical needs that align with specialty areas. The department also has not reported annually its cybersecurity critical needs to the Office of Personnel Management (OPM), as required, and has not developed plans with clearly defined time frames for doing so. (See table).

The Department of Homeland Security's Progress in Implementing Requirements of the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, as of December 2017

	Required activity	Due date	Completion date
1.	Establish procedures to identify, categorize, and code cybersecurity positions.	Mar. 2015	Apr. 2016
2.	Identify all positions with cybersecurity functions and determine work category and specialty areas of each position.	Sept. 2015	Ongoing
3.	Assign codes to all filled and vacant cybersecurity positions.	Sept. 2015	Ongoing
4.	Identify and report critical needs in specialty areas to Congress.	Jun. 2016	Not addressed
5.	Report critical needs annually to OPM.	Sept. 2016	Not addressed

Source: GAO analysis of DHS documentation and the *Homeland Security Cybersecurity Workforce Assessment Act of 2014.* | GAO-18-175

Without ensuring that its procedures are complete and that its progress in identifying and assigning codes to its positions is accurately reported, DHS will not be positioned to effectively examine its cybersecurity workforce, identify its critical skill gaps, or improve its workforce planning. Further, until DHS establishes plans and time frames for reporting on its critical needs, the department may not be able to ensure that it has the necessary cybersecurity personnel to help protect the department's and the nation's federal networks and critical infrastructure from cyber threats. The commitment of DHS's leadership to addressing these matters is essential to helping the department fulfill the act's requirements.