United States Government Accountability Office

Testimony

Before the Subcommittees on Cybersecurity and Infrastructure Protection and Oversight and Management Efficiency, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, March 7, 2018

CYBERSECURITY WORKFORCE

DHS Needs to Take Urgent Action to Identify Its Position and Critical Skill Requirements

Statement of Gregory C. Wilshusen
Director, Information Security Issues

Accessible Version

March 2018

CYBERSECURITY WORKFORCE

DHS Needs to Take Urgent Action to Identify Its Position and Critical Skill Requirements

GAO Highlights

Highlights of GAO-18-430T, a testimony before congressional subcommittees

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.

GAO was asked to testify on 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. To do so, GAO summarized the findings discussed in its February 2018 report on DHS's cybersecurity workforce (GAO-18-175).

What GAO Recommends

In its February 2018 report, GAO recommended 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 the six recommendations and described actions the department plans to take to address them.

View GAO-18-430T. 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 did not complete 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 Congress that it had coded 95 percent of the department's identified cybersecurity positions. However, 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 Congress on its departmentwide 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 Status In Implementing Requirements of the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, as of February 2018

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-18-430T

Without ensuring that its procedures are complete and that its progress in identifying and assigning codes to its cybersecurity positions is accurately reported, DHS will not be positioned to effectively examine its cybersecurity workforce, identify 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.

Chairmen Ratcliffe and Perry, Ranking Members Richmond and Correa, and Members of the Subcommittees:

Thank you for the opportunity to appear at today's hearing to discuss the Department of Homeland Security's (DHS) efforts to strengthen its cybersecurity workforce. In its important role of securing the nation's cyberspace, DHS is responsible for protecting the confidentiality, integrity, and availability of its own computer systems and information, and for leading the coordination with partners in the public and private sectors to protect the computer networks of federal civilian agencies and the nation's critical infrastructure from threats. As such, having an effective cybersecurity workforce is essential to accomplishing the department's mission.

Toward ensuring that it has an effective workforce, the *Homeland Security Cybersecurity Workforce Assessment Act of 2014* (hereafter referred to as "the act")[1] required DHS to identify all cybersecurity workforce positions within the department, determine the cybersecurity work category and specialty area of such positions, and assign the corresponding employment code to each cybersecurity position.[2] The act also required DHS to identify and report on its cybersecurity workforce areas of critical need.

In addition to the aforementioned requirements for DHS, the act included a provision for GAO to analyze and monitor the department's efforts to address its requirements. My testimony today provides an overview of our recently issued (February 2018) report, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*, based on our review of the its efforts.[3]

[1] The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* was enacted as part of the *Border Patrol Agent Pay Reform Act of 2014*, Pub. L. No. 113-277 § 4,128 Stat. 2995, 3008-3010 (Dec. 18, 2014), 6 U.S.C. § 146.

[2] The employment codes are standard codes for federal job classifications that were developed by the Office of Personnel Management (OPM), in alignment with the *National Initiative for Cybersecurity Education*'s National Cybersecurity Workforce Framework. See Office of Personnel Management, *The Guide to Data Standards* (Washington, D.C.: November 15, 2014).

[3] GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements,* GAO-18-175 (Washington, D.C.: Feb. 6, 2018).

In preparing this statement, we relied on our work supporting the February report. This work included comparing the department's actions to identify, categorize, and assign employment codes to its cybersecurity positions and to identify its cybersecurity workforce areas of critical need with the required activities specified in the act. We analyzed that information, including data on the coding of cybersecurity workforce positions, and also administered a data collection instrument to six components of DHS.[4] Further, we interviewed relevant officials from the DHS Office of Chief Human Capital Officer (OCHCO) and from the selected DHS components. We also interviewed relevant officials at the Office of Personnel Management (OPM).

The work on which this statement is based was conducted in accordance with generally accepted government auditing standards, which require audits to be planned and performed to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a reasonable basis for our findings and conclusions based on our audit objectives.

Background

DHS leads the federal government's efforts to secure our nation's public and private critical infrastructure information systems against cyber threats. As part of these efforts, cybersecurity professionals can help to prevent or mitigate the vulnerabilities that could allow malicious individuals and groups access to federal information technology (IT) systems. The ability to secure federal systems depends on the knowledge, skills, and abilities of the federal and contractor workforce that designs, develops, implements, secures, maintains, and uses these systems.

The Office of Management and Budget has noted that the federal government and private industry face a persistent shortage of cybersecurity and IT talent to implement and oversee information security

[4] The six components we reviewed are: Departmental Management and Operations, National Protection and Programs Directorate, Science and Technology Directorate, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, and U.S. Secret Service.

protections.[5] This shortage may leave federal IT systems vulnerable to malicious attacks. Experienced and qualified cybersecurity professionals are essential in performing DHS's work to mitigate vulnerabilities in its own and other agencies' computer systems and to defend against cyber threats.

Since 1997, we have identified the protection of federal information systems as a governmentwide high-risk area. In addition, in 2001, we introduced strategic governmentwide human capital management as another area of high risk.[6] We have also identified a number of challenges federal agencies are facing to ensure that they have a sufficient cybersecurity workforce with the skills necessary to protect their information and networks from cyber threats.[7] These challenges pertain to identifying and closing skill gaps as part of a comprehensive workforce planning process, recruiting and retaining qualified staff, and navigating the federal hiring process.

Federal Initiative and Guidance Are Intended to Improve Cybersecurity Workforces

In recent years, the federal government has taken various steps aimed at improving the cybersecurity workforce. These include establishing a national initiative to promote cybersecurity training and skills and developing guidance to address cybersecurity workforce challenges.

Founded in 2010, the National Initiative for Cybersecurity Education (NICE) is a partnership among government, academia, and the private sector, and is coordinated by the National Institute of Standards and Technology (NIST). The NICE mission promotes cybersecurity education, training, and workforce development in coordination with its partners. The initiative's goal is to increase the number of skilled cybersecurity professionals in order to boost national IT security.

[5] Office of Management and Budget, *Federal Cybersecurity Workforce Strategy, Memorandum M-16-15* (Washington, D.C.: July 12, 2016).

[6] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[7] GAO, *Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges*, GAO-17-533T (Washington, D.C.: Apr. 4, 2017).

In 2013, NICE published the *National Cybersecurity Workforce Framework* to provide a consistent way to define and describe cybersecurity work at any public or private organization, including federal agencies.[8] In 2014, OPM developed guidance for assigning 2-digit employment codes for each cybersecurity work category and specialty area identified in the 2013 NICE framework.[9] Federal agencies can use the codes to identify cybersecurity positions in personnel and payroll systems, such the system of the National Finance Center.[10]

To further enhance efforts to strengthen the cybersecurity workforce, NICE subsequently revised the framework in 2017 to include 33 cybersecurity-related specialty areas organized into 7 categories—securely provision, operate and maintain, protect and defend, investigate, collect and operate, analyze, and oversee and govern. The revision defined work roles in specialty areas and cybersecurity tasks for each work role,[11] as well as the knowledge, skills, and abilities that a person should have in order to perform each work role.[12] Also, in 2017, OPM issued guidance creating a unique 3-digit employment code for each cybersecurity work role.[13] In October 2017, NIST issued guidance that reflected the finalized 2017 NICE framework and included a crosswalk of OPM's 2-digit employment codes to the 3-digit codes.[14]

[8] National Institute of Standards and Technology, *NICE Cybersecurity Workforce Framework (Version 1.0)* (Gaithersburg, Md.: April 2013).

[9] Office of Personnel and Management, *The Guide to Data Standards* (Washington, D.C.: November 15, 2014).

[10] The National Finance Center personnel and payroll systems are used by DHS and other agencies for processing personnel and payroll information. In addition, they are DHS's system of record for employment codes assigned to cybersecurity employees.

[11] National Institute of Standards and Technology, *NICE Cybersecurity Workforce Framework*, Special Publication 800-181 (Gaithersburg, Md.: August 2017).

[12] According to the National Institute of Standards and Technology, work roles are the most detailed groupings of IT, cybersecurity, or cyber-related work. Examples of work roles include an authorizing official, a software developer, or a system administrator.

[13] Office of Personnel Management, *Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions* (Washington D.C.: Jan. 4, 2017).

[14] National Institute of Standards and Technology, *OPM Federal Cybersecurity Coding Structure* (Gaithersburg, Md.: Oct. 18, 2017).

DHS's Cybersecurity Workforce Performs a Wide Range of Critical Missions

DHS is the third largest department in the federal government, employing approximately 240,000 people, and operating with an annual budget of about $60 billion, of which about $6.4 billion was reportedly spent on IT in fiscal year 2017. In leading the federal government's efforts to secure our nation's public and private critical infrastructure information systems, the department, among other things, collects and shares information related to cyber threats and cybersecurity risks and incidents with other federal partners to enable real-time actions to address these risks and incidents.

The department is made up of 15 operational and support components that perform its critical mission functions. Table 1 describes the 6 components that we included in our review.

Table 1: Missions and Cybersecurity Functions of Selected Department of Homeland Security Components

DHS Component	Description
U.S. Customs and Border Protection (CBP)	CBP is to safeguard America's borders, thereby protecting the public from dangerous people and materials while enhancing the nation's global economic competitiveness by enabling legitimate trade and travel. CBP's cybersecurity workforce primarily protects the component's internal systems, networks, and data.
Departmental Management and Operations (DMO)	DMO is to provide support to the Secretary and Deputy Secretary in the overall leadership, direction, and management of DHS and all of its components. DMO is responsible for DHS's budgets and appropriations, expenditure of funds, information technology systems, facilities and equipment, and the identification and tracking of performance measurements. DMO's cybersecurity workforce is to develop and implement DHS's cybersecurity-related workforce policies and programs and protect DHS's systems, networks, and data. As part of DMO, the Office of Chief Human Capital Officer (OCHCO) is responsible for personnel policy development and implementation. The Office of the Chief Information Officer, among other things, is to develop and implement information security programs.
National Protection and Programs Directorate (NPPD)	NPPD is expected to protect and enhance the resilience of the nation's physical and cyber infrastructure, working with partners at all levels of government and the private and nonprofit sectors, to share information and build greater trust to make physical and cyber infrastructure more secure. NPPD is the lead component for fulfilling the department's national, non-law enforcement cybersecurity missions, as well as providing crisis management, incident response, and defense against cyberattacks for federal government networks.
U.S. Secret Service (USSS)	USSS is to protect designated protectees, investigate threats against protectees, as well as investigate financial and computer-based crimes; it is also expected to help secure the nation's banking and finance critical infrastructure. USSS's cybersecurity workforce primarily conducts criminal investigations and protects its systems, networks, and data.
Science and Technology Directorate (S&T)	S&T is to conduct basic and applied research, development, demonstration, testing and evaluation activities relevant to DHS. S&T's cybersecurity workforce is expected to conduct cybersecurity research and development for the Homeland Security Enterprise, and protect its systems, networks, and data.
U.S. Citizenship and Immigration Services (USCIS)	USCIS is responsible for overseeing lawful immigration to the United States. Its mission is to provide accurate and useful information to USCIS customers, grant immigration and citizenship benefits, promote an awareness and understanding of citizenship, and ensure the integrity of national immigration system. USCIS's cybersecurity workforce primarily protects its systems, networks, and data.

Source: GAO analysis of DHS information. | GAO-18-430T

DHS Is Required to Assess Its Cybersecurity Workforce

The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* required DHS to perform workforce assessment-related activities to identify and assign employment codes to its cybersecurity positions. Specifically, the act called for DHS to:

1. Establish procedures for identifying and categorizing cybersecurity positions and assigning codes to positions (within 90 days of law's enactment).
2. Identify all filled and vacant positions with cybersecurity functions and determine the work category and specialty area of each.
3. Assign OPM 2-digit employment codes to all filled and vacant cybersecurity positions based on the position's primary cybersecurity work category and specialty areas, as set forth in OPM's *Guide to Data Standards*.[15]

In addition, after completing the aforementioned activities, the act called for the department to take steps to identify and report its cybersecurity workforce areas of critical need. Specifically, DHS was to:

4. Identify the cybersecurity work categories and specialty areas of critical need in the department's cybersecurity workforce and report to Congress.
5. Submit to OPM an annual report through 2021 that describes work categories and specialty areas of critical need and substantiates the critical need designations.

The act required DHS to complete the majority of these activities by specific due dates between March 2015 and September 2016.

Within DHS, OCHCO is responsible for carrying out these provisions, including the coordination of the department's overall efforts to identify, categorize, code, and report its cybersecurity workforce assessment progress to OPM and Congress.

[15] At the time the *Homeland Security Cybersecurity Workforce Assessment Act of 2014* was enacted, DHS was to use OPM's 2014 data standards guide (Office of Personnel Management, *The Guide to Data Standards* (Washington, D.C.: November 2014). The purpose of the guide is to help agencies identify and code their cybersecurity positions. Employment codes can be used in human capital systems to measure areas of critical need.

DHS Has Not Fully Identified Cybersecurity Positions or Assigned Employment Codes in a Complete and Reliable Manner

The act required DHS to establish procedures to identify and assign the appropriate employment code, in accordance with OPM's *Guide to Data Standards*, to all filled and vacant positions with cybersecurity functions by March 2015.[16] In addition, DHS's April 2016 *Cybersecurity Workforce Coding* guidance states that components should ensure procedures are in place to monitor and to update the employment codes as positions change over time.[17]

Further, the Standards for I*nternal Control in the Federal Government* recommends that management assign responsibility and delegate authority to key roles and that each component develop individual procedures to implement objectives. The standards also recommend that management periodically review such procedures to see that they are developed, relevant, and effective.[18]

DHS OCHCO developed departmental procedures in May 2014 and recommended implementation steps for coding positions with cybersecurity functions for the department's components. However, OCHCO did not update its procedures to include information on identifying positions and assigning codes until April 2016—13 months after the due date specified by the act.

In addition, the procedures were not complete because they did not include information related to identifying and coding vacant positions, as the act required. Moreover, the departmental procedures did not identify the individual within each DHS component who was responsible for

[16] Office of Personnel Management, The Guide to Data Standards (Washington, D.C.: November 15, 2014). OPM guidance created unique 2-digit employment codes for categories and specialty areas identified in the NICE framework.

[17] U.S. Department of Homeland Security, Office of the Chief Human Capital Officer, *Cybersecurity Workforce Coding* (Washington, D.C.: April 22, 2016).

[18] GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: Sep 10, 2014).

leading and overseeing the identification and coding of the component's cybersecurity positions.

Further, although components were able to supplement the departmental procedures by developing their own component-specific procedures for identifying and coding their cybersecurity positions, OCHCO did not review those procedures for consistency with departmental guidance. The department could not provide documentation that OCHCO had verified or reviewed component-developed procedures. In addition, OCHCO officials acknowledged that they had not reviewed the components' procedures and had not developed a process for conducting such reviews.

OCHCO officials stated that several factors had limited their ability to develop the procedures and to review component-developed procedures in a timely and complete manner. These factors were (1) a delayed departmental decision until April 2016 as to whether certain positions should be considered cybersecurity positions; (2) a belief that each component had the best understanding of their human capital systems, so procedure development was best left up to each component; (3) a condition where each of the six selected DHS components recorded and tracked vacant positions differently; and (4) cybersecurity specialty areas for vacant positions were not known until a position description was developed or verified and a hiring action was imminent. Without assurance that procedures are timely, complete, and reviewed, DHS cannot be certain that its components have the procedures to identify and code all positions with cybersecurity functions, as required by the act.

Accordingly, our February 2018 report included recommendations that DHS 1) develop procedures on how to identify and code vacant cybersecurity positions, 2) identify the individual in each component who is responsible for leading that component's efforts in identifying and coding cybersecurity positions, and 3) establish and implement a process to periodically review each component's procedures for identifying component cybersecurity positions and maintaining accurate coding.[19] DHS concurred with the recommendations and stated that it would implement them by April 30, 2018.

[19] GAO-18-175.

DHS Has Not Yet Completed Required Identification Activities

The act required DHS to identify all of its cybersecurity positions, including vacant positions, by September 2015. Further, the act called for the department to use OPM's *Guide to Data Standards* to categorize the identified positions and determine the work category or specialty area of each position.[20]

As of December 2016, the department reported that it had identified 10,725 cybersecurity positions, including 6,734 federal civilian positions, 584 military positions, and 3,407 contractor positions.[21] Nevertheless, as of November 2017, the department had not completed identifying all of its cybersecurity positions and it had not determined the work categories or specialty areas of the positions. In explaining why the department had not identified all its positions, OCHCO officials stated that components varied in reporting their identified vacant positions because the department did not have a system to track vacancies.

Of the 7 work categories and 33 specialty areas in the NICE framework, DHS reported that its 3 most common work categories were "protect and defend", "securely provision," and "oversight and development;" and its 2 most common specialty areas were "security program management" and "vulnerability assessment and management." However, DHS could not provide data to show the actual numbers of positions in each of these categories and specialty areas.

According to OCHCO officials, the department was still in the process of identifying positions for the 2-digit codes and would continue this effort until the 3-digit codes were available in the National Finance Center personnel and payroll system in December 2017. At that time, OCHCO officials stated that the department intends to start developing procedures for identifying and coding positions using the 3-digit codes.

[20] Office of Personnel Management, *The Guide to Data Standards* (Washington, D.C.: November 15, 2014). OPM guidance outlined categories and specialty areas in alignment with the NICE framework.

[21] Department of Homeland Security, *Comprehensive Cybersecurity Workforce Update: 2016 Report* (Washington, D.C.: March 16, 2017).

DHS Has Not Completely and Accurately Assigned Employment Codes

The act also required DHS to assign 2-digit employment codes to all of its identified cybersecurity positions. This action was to be completed by September 2015.[22]

However, as of August 2017—23 months after the due date—the department had not completed the coding assignment process. Although, in August 2017, OPM provided a progress report to Congress containing DHS data which stated that 95 percent of DHS-identified cybersecurity positions had been coded,[23] our analysis determined that the department had assigned cybersecurity position codes to approximately 79 percent of its identified federal civilian cybersecurity positions.[24] The primary reason for this discrepancy was that DHS did not include the coding of vacant positions, as required by the act. Further, OCHCO officials stated they did not verify the accuracy of the components' cybersecurity workforce data. Without coding cybersecurity positions in a complete and accurate manner, DHS will not be able to effectively examine its cybersecurity workforce; identify skill gaps; and improve workforce planning.

Thus, in our recently issued report, we recommended that OCHCO collect complete and accurate data on all filled and vacant cybersecurity positions when it conducts its cybersecurity identification and coding efforts. DHS concurred with the recommendation and stated that, by June 29, 2018, it intends to issue memorandums to its components that provide instructions for the components to periodically review compliance and cybersecurity workforce data concerns to ensure data accuracy.

[22] Identification and code assignment is inclusive of both filled and vacant positions with cybersecurity functions.

[23] Office of Personnel Management, *Progress Report on the National Cybersecurity Workforce Measurement Initiative* (Washington, D.C.: August 3, 2017). This report was 20 months late. OPM officials stated that they did not meet the December 2015 deadline because DHS had not provided sufficient data at that point.

[24] Per DHS's August 2017 coding progress dashboard, 5,298 of 6,734 identified positions had been coded. Vacant position coding progress was not provided.

DHS Has Not Identified or Reported Its Cybersecurity Workforce Areas of Critical Need

According to the act, DHS was to identify its cybersecurity work categories and specialty areas of critical need in alignment with the NICE framework and to report this information to the appropriate congressional committees by June 2016. In addition, a DHS directive required the DHS Chief Human Capital Officer to provide guidance to the department's components on human resources procedures, including identifying workforce needs.[25]

As of February 2018, the department had not fulfilled its requirements to identify and report its critical needs. Although DHS identified workforce skills gaps in a report that it submitted to congressional committees in March 2017, the department did not align the skills gaps to the NICE framework's defined work categories and specialty areas of critical need.

In September 2017, OCHCO developed a draft document that attempted to crosswalk identified department-wide cybersecurity skills gaps to one or more specialty areas in the NICE framework. However, the document did not adequately help components identify their critical needs by aligning their gaps with the NICE framework because it did not provide clear guidance to help components determine a critical need in cases in which a skills gap is mapped to multiple work categories.

According to OCHCO officials, DHS had not identified department-wide cybersecurity critical needs that aligned with the framework partly because OPM did not provide DHS with guidance for identifying cybersecurity critical needs. In addition, OCHCO officials stated that the components did not generally view critical skills gaps in terms of the categories or specialty areas as defined in the NICE framework, but instead, described their skills gaps using position titles that are familiar to them. In the absence of relevant guidance to help components identify their critical needs, DHS and the components are hindered from effectively identifying and prioritizing workforce efforts to recruit, hire, train, develop, and retain cybersecurity personnel.

[25] Department of Homeland Security, *Human Capital Line of Business Integration and Management*, Directive No. 258-01 (Feb. 6, 2014).

DHS also did not report cybersecurity critical needs to OPM in September 2016 or September 2017, as required. Instead, the department first reported its cybersecurity coding progress and skills gaps in a March 2017 report that it sent to OPM and Congress to address several of the act's requirements.[26] However, the report did not describe or substantiate critical need designations because DHS has not yet identified them.

Additionally, DHS had not developed plans or time frames to complete priority actions—developing a DHS cybersecurity workforce strategy and completing its initial cybersecurity workforce research— that OCHCO officials said must be completed before it can report its cybersecurity critical needs to OPM. According to OCHCO officials, the report that the department submitted to Congress in March 2017 had contained plans and schedules. However, we found that the March 2017 report did not capture and sequence all of the activities that DHS officials said must be completed in order to report critical needs. Until DHS develops plans and schedules with time frames for reporting its cybersecurity critical needs, DHS may not have insight into its needs for ensuring that it has the workforce necessary to carry out its critical role of helping to secure the nation's cyberspace.

In our report, we recommended that DHS 1) develop guidance to assist DHS components in identifying their cybersecurity work categories and specialty areas of critical need that align to the NICE framework and 2) develop plans with time frames to identify priority actions to report on specialty areas of critical need.[27] DHS concurred with the recommendations and stated that it plans to implement them by June 2018.

In summary, DHS needs to act now to completely and accurately identify, categorize, and assign codes to all of its cybersecurity positions, and to identify and report on its cybersecurity workforce areas of critical need. Implementing the six recommendations we made in our February 2018 report should better position the department to meet the requirements of the 2014 act. Further, doing so will help DHS understand its needs for recruiting, hiring, developing, and retaining a cybersecurity workforce with the skills necessary to accomplish the department's varied and essential

[26] Department of Homeland Security, *Comprehensive Cybersecurity Workforce Update: 2016 Report* (Washington, D.C.: March 16, 2017).

[27] GAO-18-175.

cybersecurity mission.[28] Until DHS implements our recommendations, it will not be able to ensure that it has the necessary cybersecurity personnel to help protect the department's and federal networks and the nation's critical infrastructure from cyber threats.

Chairmen Ratcliffe and Perry, Ranking Members Richmond and Correa, and Members of the Subcommittees, this concludes my statement. I would be pleased to respond to your questions.

GAO Contact and Staff Acknowledgments

If you or your staffs have any questions about this testimony, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Chris P. Currie at (404) 679-1875 or curriec@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

GAO staff who made key contributions to this testimony are Alexander Anderegg, Ben Atwater, David Blanding, Jr., Chris Businsky, Wayne Emilien, Jr., Nancy Glover, David Hong, Tammi Kalugdan, David Plocher, Luis E. Rodriguez, and Priscilla Smith.

[28] GAO-18-175.

Related GAO Products

GAO, *Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges*, GAO-17-533T (Washington, D.C.: Apr. 4, 2017).

GAO, *Information Security: DHS Needs to Continue to Advance Initiatives to Protect Federal Systems*, GAO-17-518T (Washington, D.C.: Mar. 28, 2017).

GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

GAO, *Cybersecurity: Actions Needed to Strengthen U.S. Capabilities*, GAO-17-440T (Washington, D.C.: Feb. 14, 2017).

GAO *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

GAO, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686 (Washington, D.C.: Aug. 26, 2016).

GAO, *Federal Hiring: OPM Needs to Improve Management and Oversight of Hiring Authorities*, GAO-16-521 (Washington, D.C.: Aug. 2, 2016).

GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

GAO, *Federal Workforce: OPM and Agencies Need to Strengthen Efforts to Identify and Close Mission-Critical Skills Gaps*, GAO-15-223 (Washington, D.C.: Jan. 30, 2015).

GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, GAO-12-8 (Washington, D.C.: Nov. 29, 2011).

GAO’s Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO’s commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO’s website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select “E-mail Updates.”

Order by Phone

The price of each GAO publication reflects GAO’s actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO’s website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: https://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548