United States Government Accountability Office

Report to Congressional Committees

February 2018

CYBERSECURITY WORKFORCE

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

Accessible Version

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.

Contents

Letter 1

Background 5
DHS Has Not Fully Identified Cybersecurity Positions or Assigned Employment Codes in a Complete and Reliable Manner 12
DHS Has Not Identified or Reported Its Department-wide Cybersecurity Workforce Areas of Critical Need 21
Conclusions 26
Recommendations for Executive Action 27
Agency Comments and Our Evaluation 28

Appendix I: Objectives, Scope, and Methodology 31

Appendix II: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Categories and Specialty Areas 35

Appendix III: Comments from the Department of Homeland Security 40

Appendix IV: GAO Contacts and Staff Acknowledgments 45

GAO Contacts 45
Staff Acknowledgments 45

Appendix V: Accessible Data 46

Data Tables 46
Agency Comment Letter 48

Tables

Table 1: Missions and Cybersecurity Functions of Selected Department of Homeland Security Components 9
Table 2: Activities and Due Dates Required of the Department of Homeland Security by the *Homeland Security Cybersecurity Workforce Assessment Act of 2014* 11
Table 3: Performance of the Department of Homeland Security in Establishing Procedures, Identifying Cybersecurity Positions, and Assigning Codes, as Required by the

Homeland Security Cybersecurity Workforce Assessment Act of 2014, as of December 2017 13
Table 4: Examples of Components' Cybersecurity Coding Progress Reflected in the Department of Homeland Security's Dashboard Report, as of August 2017 20
Table 5: Performance of the Department of Homeland Security in Meeting Due Dates for Activities Required by the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, as of December 2017 21
Table 6: National Initiative for Cybersecurity Education Cybersecurity Workforce Framework Categories and Specialty Areas Definition and Corresponding Office of Personnel Management (OPM) Codes 35

Figures

Figure 1: Department of Homeland Security Components, Including Six Selected for GAO's Review 9
Figure 2: Department of Homeland Security Positions Coded for Cybersecurity Functions, June 2016-August 2017 19
Accessible Data for Figure 1: Department of Homeland Security Components, Including Six Selected for GAO's Review 46
Accessible Data for Figure 2: Department of Homeland Security Positions Coded for Cybersecurity Functions, June 2016-August 2017 47

Abbreviations

CBP	United States Customs and Border Protection
DCI	data collection instrument
DHS	Department of Homeland Security
DMO	Departmental Management and Operations
HSCWAA	*Homeland Security Cybersecurity Workforce Assessment Act of 2014*
IT	information technology
NICE	National Initiative for Cybersecurity Education

NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OCHCO	Office of the Chief Human Capital Officer
OPM	Office of Personnel Management
S&T	Science and Technology Directorate
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

February 6, 2018

Congressional Committees

The Department of Homeland Security's (DHS's) mission is to safeguard the American people and the homeland. It also serves a critical role in securing the nation's cyberspace. As such, in addition to being responsible for protecting the confidentiality, integrity, and availability of its own computer systems and information, it is also the lead federal department for coordinating 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.

Having an effective cybersecurity workforce is essential to helping ensure the security of the department's information and systems. However, achieving a resilient, well-trained, and dedicated cybersecurity workforce to help protect our information and infrastructure has been a long-standing challenge for the federal government. Since 1997, we have designated federal information security as a governmentwide high-risk area and, in 2003, expanded this area to include computerized systems supporting the nation's critical infrastructure. In 2003, we designated *Implementing and Transforming DHS* as a high-risk area, and in 2013, we renamed that area to *Strengthening DHS Management Functions,* which included information technology and human capital.[1]

In December 2014, Congress passed the *Homeland Security Cybersecurity Workforce Assessment Act of 2014* (HSCWAA).[2] This law requires 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 data element

[1] GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 2015).

[2] 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.

employment code to each cybersecurity position.[3] After completing these activities, DHS was to identify its cybersecurity work categories and specialty areas of critical need within a year of identifying and assigning employment codes, and report these needs annually to the Office of Personnel Management (OPM).

HSCWAA also contained a provision for GAO to analyze and monitor the status of DHS's efforts to address the act's requirements. For this report, our specific objectives were to determine 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 address the first objective, we reviewed the provisions of HSCWAA to identify the specific implementation activities DHS was to perform for its cybersecurity workforce and the time frames by which it was to complete the activities. In addition, we reviewed *Standards for Internal Control in the Federal Government* and then compared the cybersecurity workforce internal controls and project management processes that DHS implemented to address the act to the selected standard.[4]

We examined department-level procedures and guidance disseminated to DHS's components for their use in identifying cybersecurity positions and assigning employment codes, and compared the procedures and guidance to HSCWAA requirements and leading practices.[5] We also analyzed department-level cybersecurity workforce data from the DHS Office of Chief Human Capital Officer (OCHCO), the Department of Agriculture's National Finance Center, dashboard reports, and DHS progress reports to OPM and Congress, to identify the status of the department's efforts in fulfilling mandated requirements to identify, categorize, and code cybersecurity positions. We found the data sufficiently reliable for the purposes of reporting DHS's cybersecurity workforce identification and coding progress. However, the National

[3] Data element employment codes are standard codes developed by the Office of Personnel Management (OPM), in alignment with the *National Initiative for Cybersecurity Education*'s (NICE) National Cybersecurity Workforce Framework, and set forth in OPM's guide to data standards. Office of Personnel and Management, *The Guide to Data Standards* (Washington, D.C.: November 15, 2014).

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

[5] GAO-14-704G.

Finance Center data are limited in that only filled federal civilian positions were reported in the National Finance Center system. Vacancies, contractors, and military were not included in those data. Additionally, DHS reported data may be estimated by components, data may not cover the breadth of components, and data may be measured at different intervals.

Further, we chose a nonprobability sample of DHS components and examined their procedures for identifying cybersecurity positions and applying employment codes to the positions. The results of our assessments of these six components are not generalizable to all DHS components.

To identify the components, we considered their reported number of cybersecurity personnel and their cybersecurity functions. To select the components, we segmented the 15 DHS components into 3 groups, based on their reported total number of cybersecurity personnel in DHS. We classified these groups as “high,” “medium,” and “low.” From each group, we selected the two DHS components with the highest number of cybersecurity functions, as reported by DHS. This resulted in the selection of six components:

- U.S. Customs and Border Protection (CBP),
- Departmental Management and Operations (DMO),
- National Protection and Programs Directorate (NPPD),
- U.S. Secret Service (USSS),
- Science and Technology Directorate (S&T), and
- U.S. Citizenship and Immigration Services (USCIS).

We then collected and reviewed the cybersecurity coding progress reports from the six selected DHS components. We also administered a questionnaire and data collection instrument (DCI) to officials representing each of the six selected components to collect information and obtain their views on the status of the components’ efforts to identify and code cybersecurity positions. We administered the questionnaire and DCI from July through September 2017.

All six components responded to the questionnaire and DCI, although not all six components answered every question. We reviewed the responses and clarified and validated them, as necessary, through interviews with, or additional written responses received from the six component officials that oversaw cybersecurity workforce activities. Again, the results of our assessments of these six components are not generalizable.

To address the second objective, we analyzed documentation discussing DHS's planned actions for identifying its cybersecurity workforce areas of critical need, including its data calls to components and progress reports to OPM and Congress. We also examined cybersecurity workforce data and documentation from OCHCO and the six selected components and compared the documentation to the act's requirements, DHS-wide and component-specific workforce planning processes, the *National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework* categories and specialty areas, and *Standards for Internal Control in the Federal Government.*[6] We found the data sufficiently reliable for the purposes of reporting DHS's identification of cybersecurity workforce areas of critical need. However, the data are limited in that DHS reported data may be estimated by components, and component responses may be from a particular program or office and not cover the breadth of the program.

For both objectives, we supplemented the information and knowledge obtained from our analyses by conducting interviews with relevant officials from DHS OCHCO and the six selected components regarding the status of the department's efforts to implement the provisions of HSCWAA. Additional details on our objectives, scope, and methodology are provided in appendix I.

We conducted this performance audit from March 2017 to February 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit 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 a reasonable basis for our findings and conclusions based on our audit objectives.

[6] According to NICE, categories are high-level groupings of common cybersecurity functions, and specialty areas represent an area of concentrated work, or function, within cybersecurity and related work. GAO-14-704G.

Background

Federal agencies and our nation’s critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. The information systems and networks that support federal operations are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the myriad of operating systems, applications, and devices comprising the systems and networks.

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. This includes federal and contractor employees who use the systems in the course of their work, as well as the designers, developers, programmers, and administrators of the programs and systems.

However, 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 protections to combat cyber threats.[7] This shortage of cybersecurity professionals makes securing the nation’s networks more challenging and may leave federal IT systems vulnerable to malicious attacks. Having experienced and qualified cybersecurity professionals is important for DHS to help mitigate vulnerabilities in its own and other agencies’ computer systems as a result of cyber threats.

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

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.

- **The National Initiative for Cybersecurity Education (NICE):** This initiative, which began in March 2010, is a partnership among government, academia, and the private sector. It is coordinated by the National Institute of Standards and Technology (NIST) to help improve cybersecurity education. According to NICE, its mission includes promoting cybersecurity education, training, and workforce development, and coordinating with government, academic, and industry partners to build on existing successful programs and facilitate change and innovation. The initiative's goal is to increase the number of skilled cybersecurity professionals in order to boost national IT security.
- ***National Cybersecurity Workforce Framework*****:** In April 2013, NICE published the *National Cybersecurity Workforce Framework*, which is intended to provide a consistent way to define and describe cybersecurity work at any public or private organization, including federal agencies.[8] The initial framework defined 31 cybersecurity-related specialty areas that were organized into 7 categories. In August 2017, the framework was revised to include 33 cybersecurity-related specialty areas. The 7 categories are: securely provision, operate and maintain, protect and defend, investigate, collect and operate, analyze, and oversee and govern. For example, in the oversee and govern category, a specialty area is cybersecurity management, which covers the management of personnel, infrastructure, policy, and security awareness. Further, in the protect and defend category, the vulnerability assessment and management specialty area covers conducting assessments of threats and vulnerabilities and recommending appropriate mitigation countermeasures in order to protect information systems from threats.

  In August 2017, NIST also revised the framework to define work roles within each specialty area and describe cybersecurity tasks for each

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

work role.[9] The revision also described the knowledge, skills, and abilities that a person should have in order to perform each work role.[10] The revised framework is intended to enable agencies to examine specific IT and cybersecurity-related work roles and identify personnel skills gaps.

- **OPM Guidance for Assigning Employment Codes to Cybersecurity Positions**: OPM sets data standards for federal job classifications, including cybersecurity positions. The data standards, issued by OPM in November 2014 created a 2-digit employment code for each work category and specialty area defined in the initial 2013 NICE cybersecurity workforce framework.[11] Federal agencies use the codes to identify cybersecurity positions in personnel systems, such as the National Finance Center's personnel and payroll system.[12] According to OPM, assigning codes to federal cybersecurity positions is intended to lay the groundwork for a consistent governmentwide count of the federal cybersecurity workforce. Use of these codes is intended to enable OPM and federal agencies to more effectively identify the cybersecurity workforce; determine baseline capabilities; examine hiring trends; identify skill gaps; and recruit, hire, train, develop, and retain an effective cybersecurity workforce. (See appendix II for a description of the specialty areas defined in the *NICE Cybersecurity Workforce Framework* and their corresponding OPM codes).

  In January 2017, OPM issued new guidance to agencies for assigning employment codes to cyber-related positions. This guidance created a unique 3-digit employment code for each cybersecurity work role identified in a draft version of the 2017 NICE cybersecurity workforce framework. To enhance the recruiting and hiring of workers with needed skills, agencies are to use the new 3-digit employment codes

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

[10] According to NIST, 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.

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

[12] The Department of Agriculture's National Finance Center personnel and payroll system is a system used by DHS and other agencies for processing personnel and payroll information. In addition, it is DHS's system of record for employment codes assigned to cybersecurity employees.

to identify critical needs, and provide training and development opportunities for cybersecurity personnel.[13] In October 2017, NIST issued guidance, which reflected the finalized 2017 NICE framework and included a crosswalk of the 2-digit employment codes to the 3-digit employment codes.[14]

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

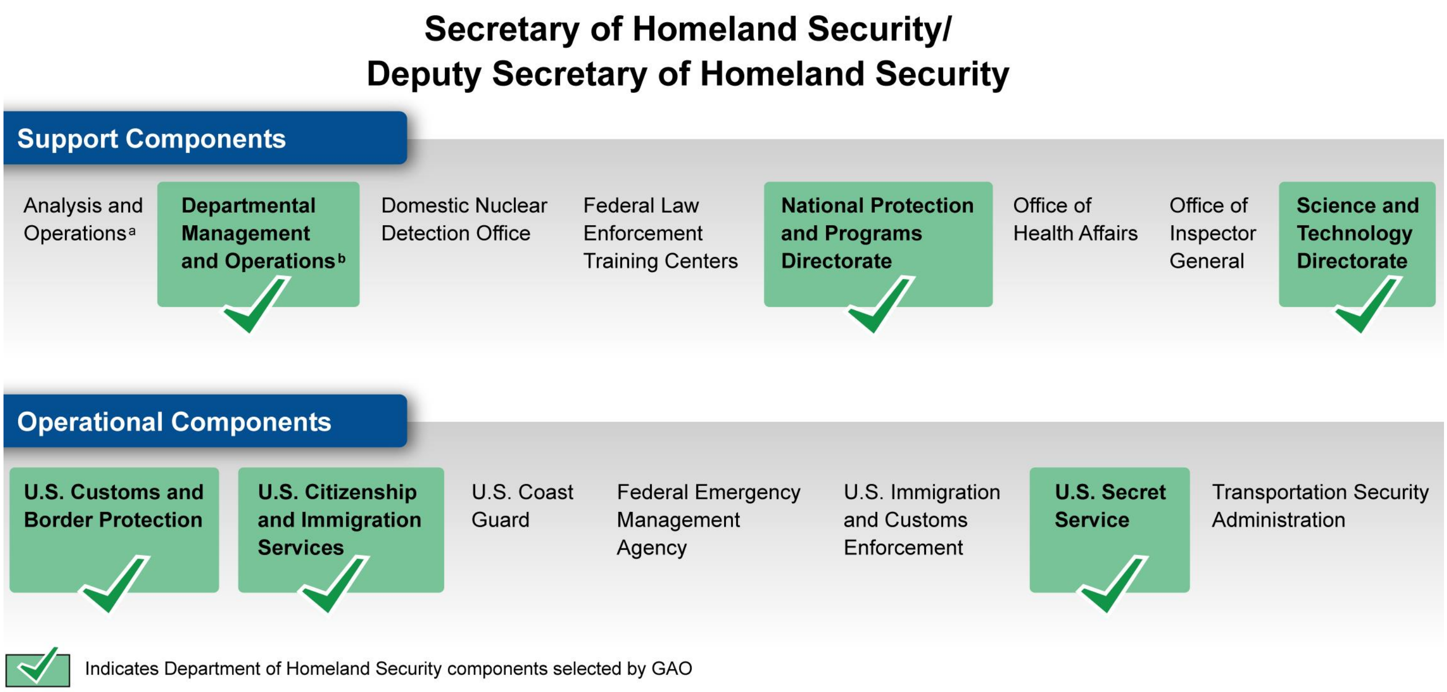
DHS is the third largest department in the federal government, employing approximately 240,000 people and with an annual budget of about $60 billion—$6.4 billion of which was spent on IT in fiscal year 2017. The department leads the federal government's efforts to secure our nation's public and private critical infrastructure information systems. For example, DHS 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.

DHS is made up of 15 components: 7 front-line, or operational, components, and 8 support components. The operational components lead the department's front-line activities to protect the nation, while the support components are to provide the resources, analysis, equipment, services, and other support to ensure that the operational components have the tools and resources to accomplish the department's mission. The 15 operational and support components, including the 6 that we reviewed, are identified in figure 1.

[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).

Figure 1: Department of Homeland Security Components, Including Six Selected for GAO's Review


Secretary of Homeland Security/
Deputy Secretary of Homeland Security
Support Components
Analysis and Operations[a]
Departmental Management and Operations[b] ✓
Domestic Nuclear Detection Office
Federal Law Enforcement Training Centers
National Protection and Programs Directorate ✓
Office of Health Affairs
Office of Inspector General
Science and Technology Directorate ✓
Operational Components
U.S. Customs and Border Protection ✓
U.S. Citizenship and Immigration Services ✓
U.S. Coast Guard
Federal Emergency Management Agency
U.S. Immigration and Customs Enforcement
U.S. Secret Service ✓
Transportation Security Administration
✓ Indicates Department of Homeland Security components selected by GAO

Source: GAO analysis of DHS information. | GAO-18-175

[a] Analysis and Operations includes the Office of Intelligence and Analysis and the Office of Operations Coordination.

[b] Departmental Management and Operations (DMO) is a group of 18 offices under a common budgeting structure that includes the Offices of the Chief Human Capital Officer, Chief Information Officer, and General Counsel.

The components perform a diverse range of cybersecurity functions. These functions include combating cybercrime; responding to cyber incidents; sharing cyber-related information, including threats and best practices; providing cybersecurity training and education; and securing both privately owned critical infrastructure and non-military federal networks. The missions and cybersecurity functions for the six components selected for our review are described in table 1.

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 its systems, networks, and data.

DHS Component	Description
Departmental Management and Operations (DMO)	DMO is to provide support to the Secretary and Deputy Secretary in the overall leadership, direction, and management of the DHS and all of its components. DMO is responsible for the 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 the Chief Human Capital Officer (OCHCO) is responsible for coordinating the department's overall efforts to identify categorize, code, and report its cybersecurity workforce progress to OPM and Congress. The Office of Chief Information Officer and Office of the General Counsel, among other things, are to develop and implement information security programs and give legal advice on cybersecurity issues, respectively.
National Protection and Programs Directorate (NPPD)	NPPD is expected to protect and enhance the resilience of the nation's physical and cyber infrastructure. It is to work with partners at all levels of government and the private and nonprofit sectors to share information and build greater trust to make national cyber and physical 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 cyber-attacks 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 the national immigration system. USCIS's cybersecurity workforce primarily protects its systems, networks, and data.

Source: GAO analysis of DHS information. | GAO-18-175

Federal Laws Require DHS to Assess Its Cybersecurity Workforce

HSCWAA required DHS to perform several workforce assessment-related activities. Specifically, the department was to:

1. Establish procedures for identifying and categorizing cybersecurity positions and assigning codes to those positions. This was to be done within 90 days of the law's enactment.
2. Identify all positions with cybersecurity functions and determine the work category and specialty areas of each position. DHS was required to identify all cybersecurity positions—both filled and vacant—within the department. In addition, it was to determine the cybersecurity work category and specialty areas for each such position. Work categories

and specialty areas are defined in the *NICE Cybersecurity Workforce Framework*.[15]

3. Assign codes to all filled and vacant cybersecurity positions. The department was to assign the appropriate 2-digit employment code, as set forth in OPM's *Guide to Data Standards,*[16] to each position based on the position's primary cybersecurity work category and specialty areas.

In addition, after completing the aforementioned activities, the department 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 the work categories and specialty areas of critical need and substantiates the critical need designations.

The act required DHS to complete the majority of the activities by specific due dates between March 2015 and September 2016 (see table 2).

Table 2: Activities and Due Dates Required of the Department of Homeland Security by the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*

Required activity		Due date
1.	Establish procedures to identify, categorize, and code cybersecurity positions.	Mar. 2015
2.	Identify all positions with cybersecurity functions and determine the work category and specialty areas of each position.	Sept. 2015[a]
3.	Assign codes to all filled and vacant cybersecurity positions.	Sept. 2015
4.	Identify and report on critical needs in specialty areas to Congress.	Jun. 2016
5.	Report critical needs annually to the Office of Personnel and Management.	Sept. 2016

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

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

[16] At the time HSCWAA 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 are to be used in human capital systems to measure areas of critical need.

[a] Although the requirement to identify and categorize all cybersecurity positions does not have a specific due date, this requirement would need to be completed before the September 2015 requirement to code the positions. Therefore, we used the coding deadline as the deadline for identifying and categorizing these positions.

Beyond HSCWAA, the *Federal Cybersecurity Workforce Assessment Act of 2015* was enacted in December 2015.[17] It assigned specific workforce planning-related activities to all federal agencies, including DHS. Specifically, the law requires all federal agencies to identify all positions that perform information technology, cybersecurity, or other cyber-related functions and assign the appropriate employment code to each position.[18] Similar to HSCWAA, the federal act also requires all federal agencies, including DHS, to identify and report to OPM on its cybersecurity work roles of critical need; each agency also is to submit a progress report on identifying cyber-related work roles of critical need to Congress.[19] According to OPM officials within Employee Services, which oversees the federal cybersecurity workforce activities and implementation, agencies are not expected to continue coding to the 2-digit data standard and, instead, are to adopt the 3-digit data standard and complete coding the 3-digit standard by April 2018.

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

As defined in OPM's guidance and required by HSCWAA, DHS has begun activities related to identifying, categorizing, and assigning the appropriate employment codes to its cybersecurity positions. However, DHS has not completed all of these activities, as required. Specifically, the department did not develop timely and complete procedures or review

[17] *Federal Cybersecurity Workforce Assessment Act of 2015*, *Consolidated Appropriations Act*, 2016, Pub. L. No. 114-113, Div. N, Title III (Dec. 18, 2015), 129 Stat. 2242, 2975-77.

[18] In January 2017, OPM issued a revised employment coding structure to address the requirements in the *Federal Cybersecurity Workforce Assessment Act of 2015.* OPM's revised coding structure created a new unique 3-digit employment code for each work role identified in the revised NICE cybersecurity workforce framework. See Office of Personnel and Management, *Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions* (Washington D.C.: January 4, 2017).

[19] GAO is reviewing federal agencies' implementation of the *Federal Cybersecurity Workforce Assessment Act of 2015*, including DHS, as a separate engagement.

its components' procedures. In addition, it did not completely and reliably identify and assign employment codes because its processes were manual, undocumented, and resource-intensive.

As indicated in table 3, the department did not complete any of the activities associated with establishing procedures and identifying and assigning employment codes to positions by the statutorily defined due dates, and two of these efforts are still ongoing.

Table 3: Performance of the Department of Homeland Security in Establishing Procedures, Identifying Cybersecurity Positions, and Assigning Codes, as Required by the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, as of December 2017

Required activity		Due date	Actual 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[a]	Ongoing
3.	Assign codes to all filled and vacant cybersecurity positions.	Sept. 2015	Ongoing

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

[a] Although the requirement to identify and categorize all cybersecurity positions does not have a specific due date, this requirement would need to be completed before the September 2015 requirement to code the positions. Therefore, we used the coding deadline as the deadline for identifying and categorizing these positions.

DHS Did Not Ensure Cybersecurity Workforce Procedures Were Timely, Complete, or Reviewed

HSCWAA required DHS to establish procedures to identify and assign the appropriate employment code to all of the department's filled and vacant positions with cybersecurity functions, in accordance with OPM's *Guide to Data Standards* by March 2015.[20] In addition, DHS's April 2016 *Cybersecurity Workforce Coding* guidance stated that components should ensure procedures are in place to monitor and to update the employment

[20] 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.

codes as positions change over time.[21] Further, *Standards for Internal 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 standard also recommends that management periodically review such procedures to see that they are developed, relevant, and effective.[22]

Toward this end, OCHCO has developed procedures and recommended implementation steps for coding positions with cybersecurity functions for the department's components. The procedures include criteria to be used in identifying cybersecurity positions. For example, the procedures state that any position that performs cybersecurity work at least 25 percent of the time should be identified as a cybersecurity position. The procedures also include information on how components are to select the appropriate data element codes.

Nevertheless, although OCHCO developed procedures for identifying positions and assigning codes, the procedures were not timely.[23] Specifically, DHS did not include in its procedures information on identifying positions and assigning codes to address the act's requirements until April 2016—13 months after the due date.

In addition, the procedures were not complete in that they did not include information related to identifying and coding vacant positions, as the act required. For example, while the National Finance Center system, which is DHS's system of record for employment codes assigned to cybersecurity employees, was modified to capture the codes for filled positions, the system was not modified to capture data on vacant positions. (For an explanation of National Finance Center's system and how DHS relates to it, see footnote 12.) In addition, the department's procedures did not address how to identify or code vacant positions, or where such information should be reported in a standardized manner across the department.

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

[22] GAO-14-704G.

[23] Under an earlier OPM cybersecurity workforce initiative, DHS had established procedures for identifying its cybersecurity positions in May 2014. Office of Personnel Management, *Special Cybersecurity Workforce Project* (Washington, D.C.: July 8, 2013).

Moreover, the departmental procedures did not identify the individual within each DHS component who was responsible for leading and overseeing the identification and coding of the component’s cybersecurity positions. For example, the procedures did not identify a responsible individual for leading the effort to identify and code CBP’s cybersecurity positions. Because there was no identified individual responsible for the entirety of the CBP cybersecurity workforce identification efforts, CBP officials told us they were unable to comment on, or provide a status update on, where they were on the cybersecurity coding process.

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

OCHCO officials identified several factors that they said limited their ability to develop timely and complete procedures for identifying and coding cybersecurity positions, and to review the supplemental procedures developed by the components. For example, they stated that:

- DHS did not complete its update of the procedures for identifying cybersecurity positions and assigning codes until April 2016 because the department could not decide whether or not certain positions within the department should be considered cybersecurity positions;
- each component had the best understanding of their human capital systems and processes, so the development of tailored procedures was best left up to each component;
- each of the six selected DHS components recorded and tracked vacant positions differently; therefore, the department’s human capital office could not issue department-wide guidance on vacant positions;
- the cybersecurity specialty areas for vacant positions were not known until a position description was developed or verified and a hiring action was imminent; and
- DHS did not assign responsibilities for, or review, components’ procedures because, as noted previously, the department believed that its components had the best understanding of their specific

human capital systems; thus, what the components included in their own procedures was best left up to them.

OCHCO officials said that they plan to work with their internal accountability team to review component-developed procedures, but they had not established a time frame for doing so. Without assurance that procedures are timely, complete, and reviewed, DHS cannot be certain that components are effectively prepared to identify and code all positions with cybersecurity functions, as required by the act.

DHS Has Not Yet Completed Required Identification Activities

HSCWAA required DHS to identify all cybersecurity positions, including vacant positions, by September 2015 in order to meet the act's other deadlines. 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.[24]

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.[25] However, as of November 2017, the department had not completed identifying all of its cybersecurity positions or determining the work categories or specialty areas of the positions. For example, three of the six DHS components we reviewed had not identified their vacant cybersecurity positions. OCHCO officials stated that components varied in reporting their identified vacant positions because the department did not have a system to track vacancies.

DHS also reported that it most commonly determined that the work category or specialty area of its cybersecurity positions were in the "protect and defend," "securely provision," and "oversight and development" work categories, and in the "security program management" and "vulnerability assessment and management" specialty areas of the NICE framework. DHS reported at least 12 of 15 DHS

[24] 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.

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

components as having cybersecurity positions in these categories and specialty areas. 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.

DHS Has Not Completely and Accurately Assigned Employment Codes

In addition to identifying all of its positions with cybersecurity functions and determining the work categories and specialty areas of each position consistent with the NICE framework, HSCWAA required DHS to assign positions codes to all such identified positions by September 2015.[26] According to the Office of Management and Budget, having complete data consistent with the framework will help agencies to effectively examine the cybersecurity workforce; identify skill gaps; and improve workforce planning.[27] Further, *Standards for Internal Control in the Federal Government* states that agencies should obtain relevant data from reliable sources that are accurate.[28]

DHS has not completely and accurately assigned employment codes to its cybersecurity workforce. As of August 2017—23 months after the due date—the department had not completed the process of assigning the 2-digit employment codes to all of its identified cybersecurity positions. For example, five of the six components we selected for review had not completed the coding of their cyber positions.

In addition, DHS did not completely or accurately assign codes to all filled and vacant cybersecurity positions as required by the act. In August 2017, OPM provided a progress report to Congress containing DHS data

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

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

[28] GAO-14-704G.

that stated that 95 percent of DHS-identified cybersecurity positions had been coded.[29] However, our analysis determined that the department had assigned cybersecurity position codes to approximately 79 percent, rather than the reported 95 percent, of identified federal civilian cybersecurity positions.[30] See figure 2 below. DHS could not demonstrate that it had assigned codes to 95 percent of its positions, as reported, since its coding progress data never indicated such a percentage.

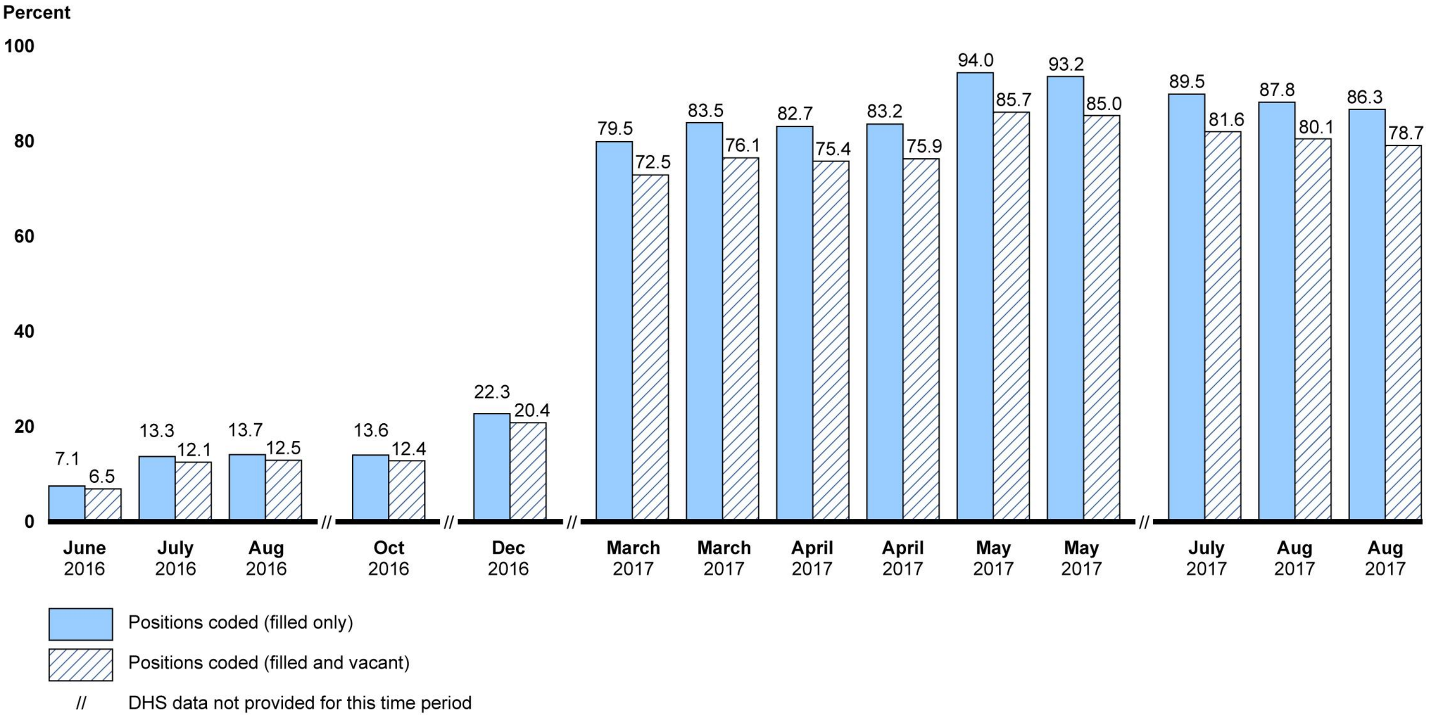
The percentage of coded positions reported for DHS was overstated because it was not based on complete information. Specifically, the percentage reflected information on the progress of filled federal civilian cybersecurity positions, but excluded vacant positions, even though the act required DHS to report these positions. Among the six components that we selected for our review, five of them had not yet completed the coding of their positions.

Figure 2 shows the results of our analysis of DHS's progress in coding its cybersecurity positions, which considered both filled and vacant federal civilian cybersecurity positions, in comparison to what the department identified, which considered incomplete data—using only filled positions.

[29] 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.

[30] 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.

Figure 2: Department of Homeland Security Positions Coded for Cybersecurity Functions, June 2016-August 2017



Source: GAO analysis of DHS documentation. | GAO-18-175

Notes: Data for all months were not provided by DHS. Data for June through December 2016 were reported by DHS in the DHS *Comprehensive Cybersecurity Workforce Update*. Data for January 2017 through June 2017, and August 2017 were reported in DHS Office of the Chief Human Capital Officer cybersecurity workforce dashboards based on National Finance Center data. July 2017 data were provided by a DHS report of National Finance Center data.

DHS reported data twice during March 2017, April 2017, May 2017, and August 2017. DHS did not provide data for September 2016, November 2016, January 2017, February 2017, or June 2017.

The baseline for the total identified federal civilian cybersecurity positions was 6,734 as reported in the *Comprehensive Cybersecurity Workforce Update* and coding progress dashboards. DHS estimated it had 7,000 identified positions for months prior to December 2016. Therefore, for the purpose of this figure, we used 6,734 as the baseline for all months. For reporting purposes, DHS used a baseline of 6,139 representing filled positions only and did not include vacant positions.

According to DHS officials the percentage decrease of positions coded from May 2017 to August 2017 was caused by system errors and workforce turnover in which new cybersecurity employees had not been assigned position codes.

In addition to being incomplete, DHS's results were not accurate. Specifically, OCHCO developed a bi-monthly dashboard to monitor and report coding progress; however, the office did not have assurance that its data were accurate. OCHCO officials stated they did not verify the components' data for accuracy. For example, while no more than 100 percent of identified positions should be coded, OCHCO reported 122.7

percent of positions as being coded for the Office of the Chief Information Officer. Such anomalies were due to DHS components reporting the total number of identified cybersecurity positions on a semi-annual basis, while OCHCO determined positions coded on a bi-monthly basis using data from the National Finance Center personnel and payroll system.[31] Yet, OCHCO analyzed and reported these numbers together, even though they were representative of different time periods. This produced unreliable results that were not representative of actual progress.

Table 4 provides examples of components' coding progress, as reflected in DHS's August 29, 2017 dashboard report, which showed one component that had more cybersecurity positions coded than were identified.

Table 4: Examples of Components' Cybersecurity Coding Progress Reflected in the Department of Homeland Security's Dashboard Report, as of August 2017

Component	Percentage of filled and vacant positions coded
Customs and Border Protection	45.9
Office of the Chief Information Officer[a]	122.7
Office of the General Counsel[a]	0[b]
National Protection and Programs Directorate	59.5
U.S. Secret Service	71.2
Science and Technology Directorate	100.0
U.S. Citizenship and Immigration Services	85.7

Source: GAO analysis of DHS documentation. | GAO-18-175

[a] Subcomponent of Departmental Management and Operations (DMO).

[b] DHS's August 2017 dashboard and previous monthly versions reported that no OGC filled and vacant cybersecurity positions were coded; but data obtained from the National Finance Center as of July 2017 showed 211.9 percent of identified positions were coded for OGC.

OCHCO officials reported several factors related to their processes and systems that had limited their ability to collect and use data that were complete and accurate. Specifically, the officials stated that OCHCO did not have documented processes to collect and verify data from the components. The officials also stated that the components did not report vacancies consistently, and that the department does not have a system

[31] DHS used the National Finance Center personnel and payroll system to record codes for positions with identified cybersecurity functions.

to track the vacancies. The officials further stated that the cybersecurity workforce amounts frequently changed, and that they could not review workforce data for reliability, as such a review was a resource-intensive activity.

However, if DHS does not assure that processes are in place to obtain and use data that are complete, including vacant positions, and accurate, then the department cannot be assured that it will have an accurate understanding of its internal coding progress. Without the ability to code its cybersecurity positions in a complete and accurate manner, DHS will not be able to effectively examine the cybersecurity workforce; identify skill gaps; and improve workforce planning.

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

While DHS has identified workforce capacity and capability gaps, it has not identified or reported to Congress its department-wide cybersecurity critical needs that align with the NICE framework. Additionally, the department has not reported its critical needs to OPM or developed plans and time frames for completing priority actions for reporting critical needs annually to OPM. Further, as indicated in table 5, the department did address any required activities by the statutorily defined due dates.

Table 5: Performance of the Department of Homeland Security in Meeting Due Dates for Activities Required by the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, as of December 2017

Required activity	Due date	Actual completion date
1. Identify and report on critical needs in specialty areas to Congress.	Jun. 2016	Not addressed
2. Report critical needs annually to the Office of Personnel Management.	Sept. 2016	Not addressed

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

DHS Has Not Identified Critical Needs in Alignment with the NICE Framework or Provided Guidance to Components

HSCWAA required DHS 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, according to a DHS directive, the DHS Chief Human Capital Officer is responsible for providing guidance to the department's components on human resources standards, such as identifying workforce needs.[32] According to GAO's leading practices on strategic workforce planning, developing and providing guidance could help agencies identify their critical needs in order to effectively recruit, hire, train, and retain cybersecurity personnel.[33]

Although required to do so by June 2016, DHS has not yet identified its cybersecurity work categories and specialty areas of critical need in alignment with the NICE framework. The department identified workforce skills gaps and included this information in a report that it submitted to congressional committees in March 2017. However, the department did not align the workforce skills gaps report to the NICE framework's work categories and specialty areas as required by HSCWAA.[34] (The categories and specialty areas are described in appendix II.)

Specifically, although the framework required that critical needs be align with a specific specialty area, DHS did not align the skills gaps to a particular specialty area in the NICE framework. For example, DHS identified a skill gap called development operations, which is related to 12 different specialty areas in the NICE framework. This skill gap also overlaps with other DHS skill gaps and creates the potential for double-counting critical needs. Furthermore, although three selected components reported in our questionnaires that they were able to identify their critical

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

[33] *GAO, Key Principles for Effective Strategic Workforce Planning,* GAO-04-39 *(*Washington, D.C.: December 2003*)*.

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

needs that aligned to the framework, they did not report this information to OCHCO.

According to OCHCO officials, DHS has not identified department-wide cybersecurity critical needs that align with the framework partly because OPM had not provided DHS with guidance for identifying cybersecurity critical needs. According to OPM officials, however, they provided oral guidance to DHS on using the 2-digit codes for identifying its critical needs during four meetings in 2016 and 2017. The OPM officials also stated that they had plans to develop governmentwide guidance for using the 3-digit codes to identify cybersecurity critical needs by March 2018 to fulfil the requirements of the *Federal Cybersecurity Workforce Assessment Act of 2015*.[35] According to OPM, agencies such as DHS are required to identify critical needs for the 3-digit codes by April 2019. DHS OCHCO officials said that DHS plans to transition to identifying cyber-related work roles of critical need once they have completed the 3-digit coding efforts under the 2015 federal act mentioned previously.

Further, DHS has not developed and provided guidance to help its component-level agencies to identify their critical needs that align to the NICE framework. Specifically, DHS did not include guidance in its procedures that instructed components on how to report on their critical needs or to align to the NICE framework work categories and specialty areas.[36] Two selected components' officials told us they required guidance from OCHCO on how best to identify critical needs.

According to OCHCO officials, they did not provide components guidance on critical needs that align with the NICE framework because the components were in the best position to determine their critical needs. Further, OCHCO officials stated that the components do not generally

[35] The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* required OPM to provide DHS with timely guidance for identifying cybersecurity work categories and specialty areas of critical need. In addition, the *Federal Cybersecurity Workforce Assessment Act of 2015* requires OPM to provide federal agencies with timely guidance for identifying information technology, cybersecurity, or other cyber-related roles of critical need beginning 1 year after they have coded employees.

[36] The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* required DHS to identify work categories and specialty areas of critical need in the department's cybersecurity workforce. In addition, the act stated that DHS is to use work categories and specialty areas defined in OPM's *Guide to Data Standards*, which is aligned with the NICE framework. Thus to comply with the requirements of the act, DHS would need to identify its critical needs in alignment with the NICE framework.

view critical skills gaps in terms of the categories or specialty areas as defined in the NICE framework, but instead, describe their skills gaps using position titles that are familiar to them. For example, one selected component identified security engineering as a skills gap familiar to them. However, according to OCHCO officials, this gap may align to five different specialty areas in the NICE framework's securely provision work category. As mentioned previously, the framework required that critical needs be align with a specific specialty area.

In September 2017, OCHCO developed a draft document that crosswalks identified department-wide cybersecurity skills gaps to one or more specialty areas in the NICE framework. However, the document does not adequately help components identify their critical needs by aligning their gaps with the NICE framework. Half of the DHS skills gaps overlap with two or more work categories, but the National Finance Center payroll system allows components to enter only one code per position. Further, the document does not provide additional decision rules to help components determine a critical need in cases in which a skills gap is mapped to multiple work categories.

Without providing 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 across the department.

DHS Did Not Report Critical Needs Annually to OPM or Develop Plans and Time Frames for Completing Priority Actions

HSCWAA required that, annually from September 2016 through September 2021, DHS, in consultation with OPM, submit a report to OPM that describes and substantiates critical need designations. In addition, *Standards for Internal Control in the Federal Government* states that management should develop plans to achieve objectives.[37] Developing plans to report critical needs is a control activity that could help capture and sequence all of the activities that DHS must complete in order to report critical needs. This involves clearly defining what is to be achieved,

[37] GAO-14-704G.

who is to achieve it, how it will be achieved, and the time frames for achievement.[38]

DHS did not report cybersecurity critical needs to OPM in September 2016 or September 2017 as required.[39] Instead, the department first reported its cybersecurity coding progress and skills gaps in the March 2017 report that it sent to OPM and Congress addressing several of the HSCWAA requirements.[40] The report did not describe or substantiate critical need designations because DHS has not yet identified them. OCHCO officials stated that the department plans to submit another report to OPM; however, they did not indicate whether critical needs will be included in the report, and did not have a time frame for when they plan to submit the report to OPM.

Additionally, DHS has not developed plans or time frames to complete priority actions that OCHCO officials said must be completed before it can report its cybersecurity critical needs to OPM. DHS's *Comprehensive Cybersecurity Workforce Update* reported two priority actions to identify, describe, and substantiate cybersecurity critical needs—developing a DHS cybersecurity workforce strategy and completing its initial cybersecurity workforce research—by the end of fiscal year 2017.[41] However, DHS did not complete the priority actions by the end of fiscal year 2017, as planned.

As of September 2017, the department was still in the process of finalizing the DHS cybersecurity workforce strategy and had not yet

[38] GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, GAO-16-89G (Washington, D.C.: Dec. 22, 2015).

[39] The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* also required OPM to submit a progress report on DHS's cybersecurity coding progress to the appropriate congressional committees by December 2015. In addition, the *Federal Cybersecurity Workforce Assessment Act of 2015*, required OPM to submit a progress report by June 2016. OPM submitted the report in August 2017.

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

[41] Department of Homeland Security, *Comprehensive Cybersecurity Workforce Update*: 2016 Report (Washington, D.C.: March 16, 2017). DHS's cybersecurity workforce research includes psychometric research, which is research by psychologists that involves measuring the knowledge, skills, and abilities of persons. DHS is conducting the psychometric research to determine the critical knowledge, skills, and abilities, and competencies needed by DHS's cybersecurity workforce to meet its cybersecurity mission requirements.

completed the initial cybersecurity workforce research. OCHCO officials said that the strategy is to be influenced by ongoing efforts to finalize the DHS comprehensive cybersecurity mission strategy, provide DHS reports required by the May 2017 cybersecurity-related presidential executive order, and finalize and implement the new cybersecurity-focused personnel system.[42] According to OCHCO officials, the department plans to conduct additional interviews and focus groups in fiscal year 2018.[43]

According to DHS OCHCO officials, the department did not develop plans or schedules with time frames to report cybersecurity critical needs. These officials stated that the report that the department submitted to Congress in March 2017 had contained plans and schedules. However, it did not capture and sequence all of the activities that DHS officials said must be completed in order to report critical needs. For example, the report did not include a schedule for completing the cybersecurity workforce strategy or conducting additional interviews and focus groups to complete the initial cybersecurity workforce research.

Until DHS develops plans and schedules with time frames for reporting its cybersecurity critical needs, the department may not have important 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. Further, OPM may be hindered from using DHS's reports to understand critical needs consistently on a governmentwide basis.

Conclusions

DHS has begun the required workforce assessment activities to identify, categorize, and assign codes to its cybersecurity positions. However, the department did not complete the activities by their statutorily defined due dates and efforts are still ongoing. Specifically, the department did not develop timely and complete procedures or review its components' procedures. In addition, DHS's efforts to identify, categorize, and code cybersecurity positions were incomplete and unreliable. Without the ability

[42] The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017).

[43] OCHCO officials stated that industrial/organizational psychologists had conducted interviews with component cybersecurity subject matter experts in July, August, and September 2017, to identify the knowledge, skills, and abilities needed to meet DHS's cybersecurity mission requirements.

to identify, categorize, and code its cybersecurity positions in a complete and accurate manner, DHS will not be able to effectively examine the cybersecurity workforce, identify skill gaps, and improve workforce planning.

DHS has identified critical gaps in its cybersecurity workforce, but these gaps did not align with the NICE framework work categories and specialty areas of critical need, as required by the act. Specifically, DHS has not developed guidance to help its component agencies and offices identify their cybersecurity critical needs. Moreover, DHS lacks plans with defined time frames for completing its required annual reporting to OPM. Until the department addresses these issues, it may continue to miss reporting deadlines and be hindered from effectively identifying and prioritizing critical workforce efforts to recruit, hire, train, develop, and retain cybersecurity personnel across its multiple components. In addition, DHS may not have cybersecurity personnel with the required skills to better protect federal networks and national critical infrastructure from threats.

The commitment of DHS's leadership is essential to successfully addressing these issues and the associated management weaknesses. By taking urgent and diligent action now, DHS will be better positioned to fulfill the requirements of HSCWAA and to identify and code its filled and vacant cybersecurity positions accurately when it transitions to using the revised NICE framework.

Recommendations for Executive Action

We are making the following six recommendations to DHS:

The Secretary of Homeland Security should develop procedures on how to identify and code vacant cybersecurity positions. (Recommendation 1)

The Secretary of Homeland Security should identify the individual in each component who is responsible for leading that component's efforts in identifying and coding cybersecurity positions. (Recommendation 2)

The Secretary of Homeland Security should establish and implement a process to periodically review each component's procedures for identifying component cybersecurity positions and maintaining accurate coding. (Recommendation 3)

The Secretary of Homeland Security should ensure OCHCO collects complete and accurate data from its components on all filled and vacant cybersecurity positions when it conducts its cybersecurity identification and coding efforts. (Recommendation 4)

The Secretary of Homeland Security should develop guidance to assist DHS components in identifying their cybersecurity work categories and specialty areas of critical need that align to the NICE framework. (Recommendation 5)

The Secretary of Homeland Security should develop plans with time frames to identify priority actions to report on specialty areas of critical need. (Recommendation 6)

Agency Comments and Our Evaluation

We received written comments on a draft of this report from DHS. In the comments (reprinted in appendix III), the department concurred with our six recommendations and provided estimated completion dates for implementing each of them.

With regard to recommendations 1 and 2, DHS stated that, by February 28, 2018, it plans to finalize and disseminate an updated version of its cybersecurity position identification and coding guidance to address vacant positions, as well as issue a memorandum requiring its components to designate a lead for reporting progress to OCHCO. Further, by April 30, 2018, the department said it plans to address recommendation 3 by disseminating a memorandum that includes a process for periodically reviewing component procedures and instructions for components to report related data and documents.

DHS also stated that, by June 29, 2018, it plans to issue memorandums to its components that provide instructions, guidance, and plans to address recommendations 4 through 6. The department added that it intends to (1) periodically review compliance and cybersecurity workforce data concerns with component leads to ensure data accuracy; (2) disseminate a reporting schedule for identifying cybersecurity critical needs; and (3) develop and disseminate a project plan with milestones, due dates, and responsibilities for reviewing progress and reporting on workforce planning actions in fiscal years 2018 and 2019.

The aforementioned actions, if implemented effectively, should help DHS address the intent of our recommendations. In addition, we received technical comments from the department, which we have incorporated, as appropriate.

We also provided a draft of this report for OPM’s review and comments. In response, an OPM program analyst stated, via email, that the agency had no edits, comments, or revisions to the draft report.

We are sending copies of this report to appropriate congressional committees, the Secretary of Homeland Security, and the Director of the Office of Personnel Management. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Chris 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 report. GAO staff who made key contributions to this report are listed in appendix IV.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Chris P. Currie

Chris P. Currie
Director, Homeland Security and Justice

List of Congressional Committees

The Honorable Ronald Johnson
Chairman
The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Michael T. McCaul
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Gregg Harper
Chairman
The Honorable Robert Brady
Ranking Member
Committee on House Administration
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to identify the extent to which DHS has:

1. identified, categorized and assigned employment codes to cybersecurity positions and
2. identified its cybersecurity workforce areas of critical need.

To address both objectives, we examined Department of Homeland Security (DHS) Office of Chief Human Capital Officer (OCHCO) and component cybersecurity workforce data and documentation and interviewed OCHCO and component officials. In addition, we reviewed *Standards for Internal Control in the Federal Government* and *Key Principles for Effective Strategic Workforce Planning,* and then compared the cybersecurity workforce internal controls and project management processes that DHS implemented to address the act to the selected standard.[1]

We also administered a questionnaire and data collection instrument (DCI) to a nonprobability sample of 6 of 15 DHS components. To select the 6 components we used OPM's Enterprise Human Resources Integration-Statistical Data Mart data on DHS civilian positions. We segmented the 15 components into 3 groups, based on their reported total number of cybersecurity personnel in DHS—high, medium, and low. From each group, we selected 2 DHS components with the highest number of cybersecurity functions,[2] as reported by DHS. Where components or offices in the same tier have equivalent cybersecurity functions, we selected the DHS component or office with the highest

[1] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014) and GAO, *Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: December 2003).

[2] For example, one of the selected components is the National Protection and Programs Directorate (NPPD), which has the second highest number of cybersecurity functions. 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 networks.

share of cybersecurity employees. This approach resulted in the selection of the following DHS components:

- U.S. Customs and Border Protection,
- Departmental Management and Operations,
- National Protection and Programs Directorate,
- U.S. Secret Service,
- Science & Technology Directorate, and
- U.S. Citizenship and Immigration Services.

The results of this analysis are not generalizable to all DHS components.

In both the questionnaire and DCI, we asked questions related to the status of DHS's identification, categorization and assignment of employment codes to cybersecurity positions, and identification of its cybersecurity workforce areas of critical need. To minimize errors that might occur from respondents interpreting our questions differently from our intended purpose, we performed a preliminary review of the questionnaire and DCI with OCHCO officials.

The selection of OCHCO officials for preliminary review was based on OCHCO's oversight role in the implementation of the *Homeland Security Cybersecurity Workforce Assessment Act of 2014* (HSCWAA). During this review, we interviewed the officials to ensure that the questions were applicable, clear, unambiguous, and easy to understand. We then revised our questionnaire and DCI based on the feedback provided during the preliminary review. All respondents completed the final questionnaire and DCI, although not all survey respondents answered every question.[3] We then reviewed the responses and interviewed relevant component officials in order to get clarification and validation of their responses.

We determined that the data obtained from the questionnaire and DCI are sufficiently reliable for the purpose of reporting DHS' progress in assigning cybersecurity codes. However, these data have the following limitations: component responses may be from a particular program or office and not cover the breadth of the program, and component reported data may be estimated or unavailable.

[3] The questionnaire and data collection instrument were administered from July 2017 through September 2017.

To address our first objective, we reviewed and analyzed DHS's department-level cybersecurity workforce procedures and communications and organizational documents for identifying cybersecurity positions and assigning work-position codes in accordance with the act. Further, we examined department-level data from the Department of Agriculture's National Finance Center, DHS dashboard reports, and DHS progress reports to the Office of Personnel Management (OPM) and Congress. To assess the reliability of OCHCO and component cybersecurity workforce data, we compared them with data from OPM's Enterprise Human Resources Integration-Statistical Data Mart data on DHS civilian positions and against the National Finance Center personnel and payroll system data on the cybersecurity coding of DHS civilian positions as appropriate. In addition, we reviewed and analyzed component-level cybersecurity workforce procedures, as well as cybersecurity workforce data and documentation, including data calls to selected component-level offices in DHS. We evaluated these documents against the act's requirements and *Standards for Internal Control in the Federal Government* to ensure that DHS's processes addressed leading practices.

To address our second objective, we reviewed and analyzed DHS's planned actions for identifying its cybersecurity workforce areas of critical need, including data calls to components, and DHS progress reports to OPM and Congress. We also examined OCHCO and component cybersecurity workforce data and department-level workforce planning documentation to evaluate the status of the department's efforts to identify its cybersecurity workforce areas of critical need. We compared these documents against the act's requirements, DHS-wide and component-specific workforce planning processes, the National Initiative for Cybersecurity Education (NICE) framework categories and specialty areas, and *Standards for Internal Control in the Federal Government* to ensure DHS met its requirements.

To assess the reliability of OPM's Enterprise Human Resources Integration-Statistical Data Mart data on DHS civilian positions, we reviewed the data for obvious errors as well as compared OPM's written responses to our data reliability questionnaire regarding the generation and use of the data. We determined that the data were sufficiently reliable for the purpose of helping inform our selection of a nonprobability sample of 6 DHS components as described above.

To assess the reliability of National Finance Center personnel and payroll system data on the cybersecurity coding of DHS civilian positions, we examined the data for outliers and obvious errors and compared those data to data and documentation from DHS components. In addition, we interviewed and observed DHS officials generate and use the National Finance Center data. We determined that the data were sufficiently reliable for the purposes of reporting DHS cybersecurity workforce coding progress. The data are limited in that only filled federal civilian positions were reported in the National Finance Center system. Vacancies, contractors, and military were not included in those data.

To assess the reliability of DHS's OCHCO and component human capital systems data on the DHS civilian cybersecurity workforce, we reviewed the data for outliers and obvious errors, and compared them against data from the National Finance Center personnel and payroll system. We also interviewed officials from OCHCO and selected DHS components regarding the generation and use of the data. We determined that the data were sufficiently reliable for the purpose of reporting DHS' progress in assigning cybersecurity codes. However, the data have the following limitations: component responses may be from a particular program or office and not cover the breadth of the program, data may be estimated by components, and data may be measured at different intervals—for example, total cybersecurity workforce may be measured at a different point in time than cybersecurity workforce positions coded.

For both objectives, we supplemented the information and knowledge obtained from our assessments by holding discussions with relevant DHS OCHCO and the six components' officials to evaluate the status of the department's efforts to implement the act.

We conducted this performance audit from March 2017 to February 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit 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 a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Categories and Specialty Areas

Table 6: National Initiative for Cybersecurity Education Cybersecurity Workforce Framework Categories and Specialty Areas Definition and Corresponding Office of Personnel Management (OPM) Codes

Category	NICE Specialty Area	NICE Specialty Area definition	OPM code
Securely Provision category	Risk Management	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.	61
Securely Provision category	Software Development	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.	62
Securely Provision category	Systems Development	Works on the development phases of the systems development life cycle.	63
Securely Provision category	Systems Requirements Planning	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.	64
Securely Provision category	Systems Architecture	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.	65
Securely Provision category	Technology Research & Development	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.	66

Category	NICE Specialty Area	NICE Specialty Area definition	OPM code
Securely Provision category	Test and Evaluation	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.	67
Operate and Maintain category	Customer Service and Technical Support	Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).	41
Operate and Maintain category	Data Administration	Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.	42
Operate and Maintain category	Knowledge Management	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.	43
Operate and Maintain category	Network Services	Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.	44
Operate and Maintain category	Systems Administration	Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also, manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.	45
Operate and Maintain category	Systems Analysis	Conducts the integration/testing, operations, and maintenance of systems security.	46
Oversee and Govern category	Training, Education, and Awareness	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.	71
Oversee and Govern category	Acquisition and Program/Project Management[a]	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.	72

Category	NICE Specialty Area	NICE Specialty Area definition	OPM code
Oversee and Govern category	Acquisition and Program/Project Management[a]	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.	80
Oversee and Govern category	Legal Advice and Advocacy	Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.	73
Oversee and Govern category	Cybersecurity Management	Oversees the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.	74
Oversee and Govern category	Strategic Planning and Policy	Develops policies and plans and/or advocates for changes in policy that supports organizational cyberspace initiatives or required changes/enhancements.	75
Oversee and Govern category	Executive Cybersecurity Leadership	Supervises, manages, and/or leads work and workers performing cybersecurity work.	90
Protect and Defend category	Cybersecurity Defense Analysis	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.	51
Protect and Defend category	Cybersecurity Defense Infrastructure Support	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	52
Protect and Defend category	Incident Response	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	53

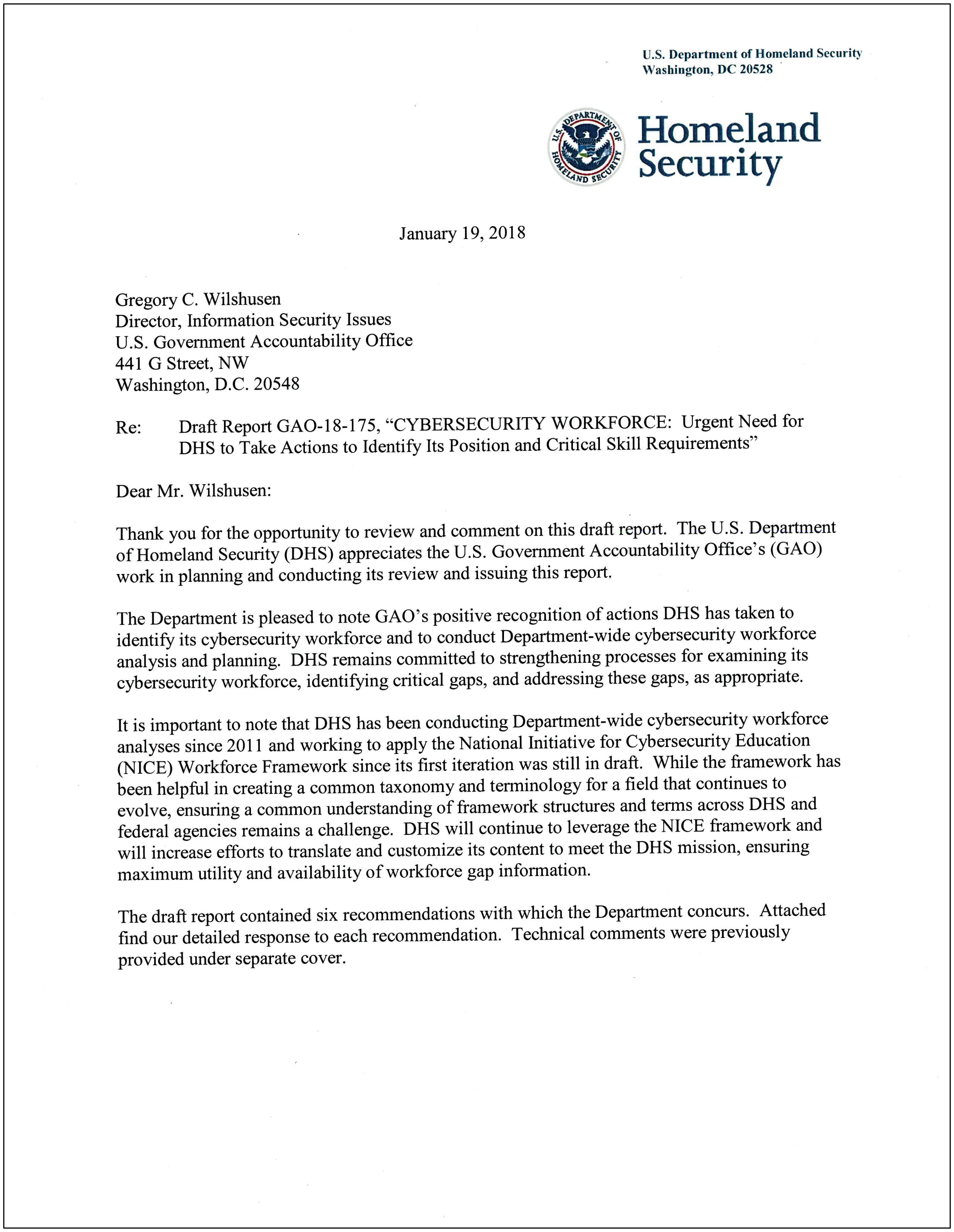
Category	NICE Specialty Area	NICE Specialty Area definition	OPM code
Protect and Defend category	Vulnerability Assessment and Management	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.	54
Analyze category	All-Source Analysis	Analyzes threat information from multiple sources, disciplines, and agencies across the intelligence community. Synthesizes and places intelligence information in context; draws insights about the possible implications.	11
Analyze category	Exploitation Analysis	Analyzes collected information to identify vulnerabilities and potential for exploitation.	12
Analyze category	Targets	Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.	13
Analyze category	Threat Analysis	Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.	14
Analyze category	Language Analysis	Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.	No code assigned
Collect and Operate category	Collection Operations	Executes collection using appropriate strategies and within the priorities established through the collection management process.	31
Collect and Operate category	Cyber Operations	Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.	32
Collect and Operate category	Cyber Operational Planning	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.	33
Investigate category	Digital Forensics	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.	21
Investigate category	Cyber Investigation	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.	22

Source: GAO analysis of NICE's framework and OPM's coding structure | GAO-18-175

[a] OPM guidance states that individuals primarily engaged in project or program management for cybersecurity projects or tasks should be coded with the Cybersecurity Program/Project Management value (80).

Appendix III: Comments from the Department of Homeland Security

Appendix III: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

January 19, 2018

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Re: Draft Report GAO-18-175, "CYBERSECURITY WORKFORCE: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements"

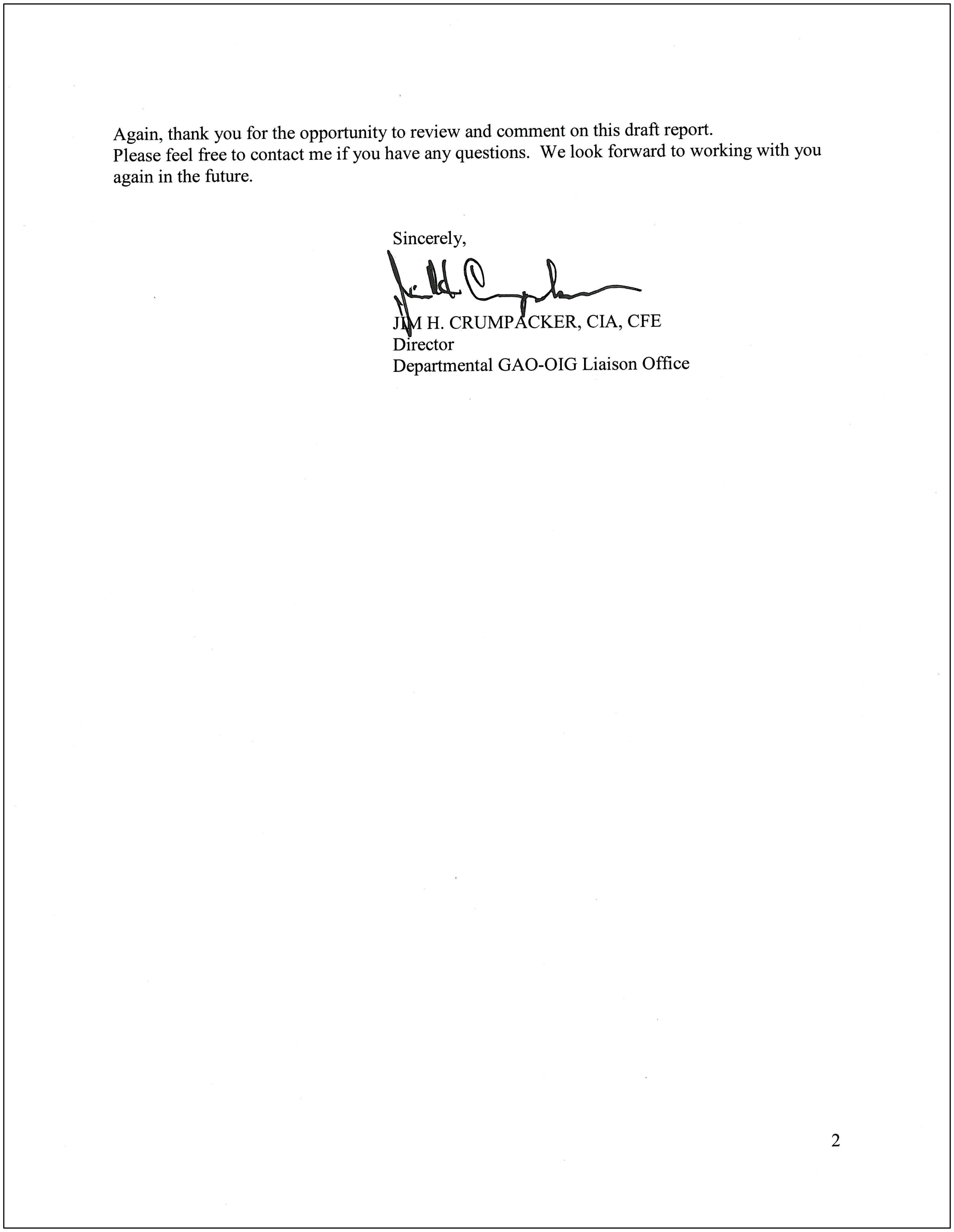
Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive recognition of actions DHS has taken to identify its cybersecurity workforce and to conduct Department-wide cybersecurity workforce analysis and planning. DHS remains committed to strengthening processes for examining its cybersecurity workforce, identifying critical gaps, and addressing these gaps, as appropriate.

It is important to note that DHS has been conducting Department-wide cybersecurity workforce analyses since 2011 and working to apply the National Initiative for Cybersecurity Education (NICE) Workforce Framework since its first iteration was still in draft. While the framework has been helpful in creating a common taxonomy and terminology for a field that continues to evolve, ensuring a common understanding of framework structures and terms across DHS and federal agencies remains a challenge. DHS will continue to leverage the NICE framework and will increase efforts to translate and customize its content to meet the DHS mission, ensuring maximum utility and availability of workforce gap information.

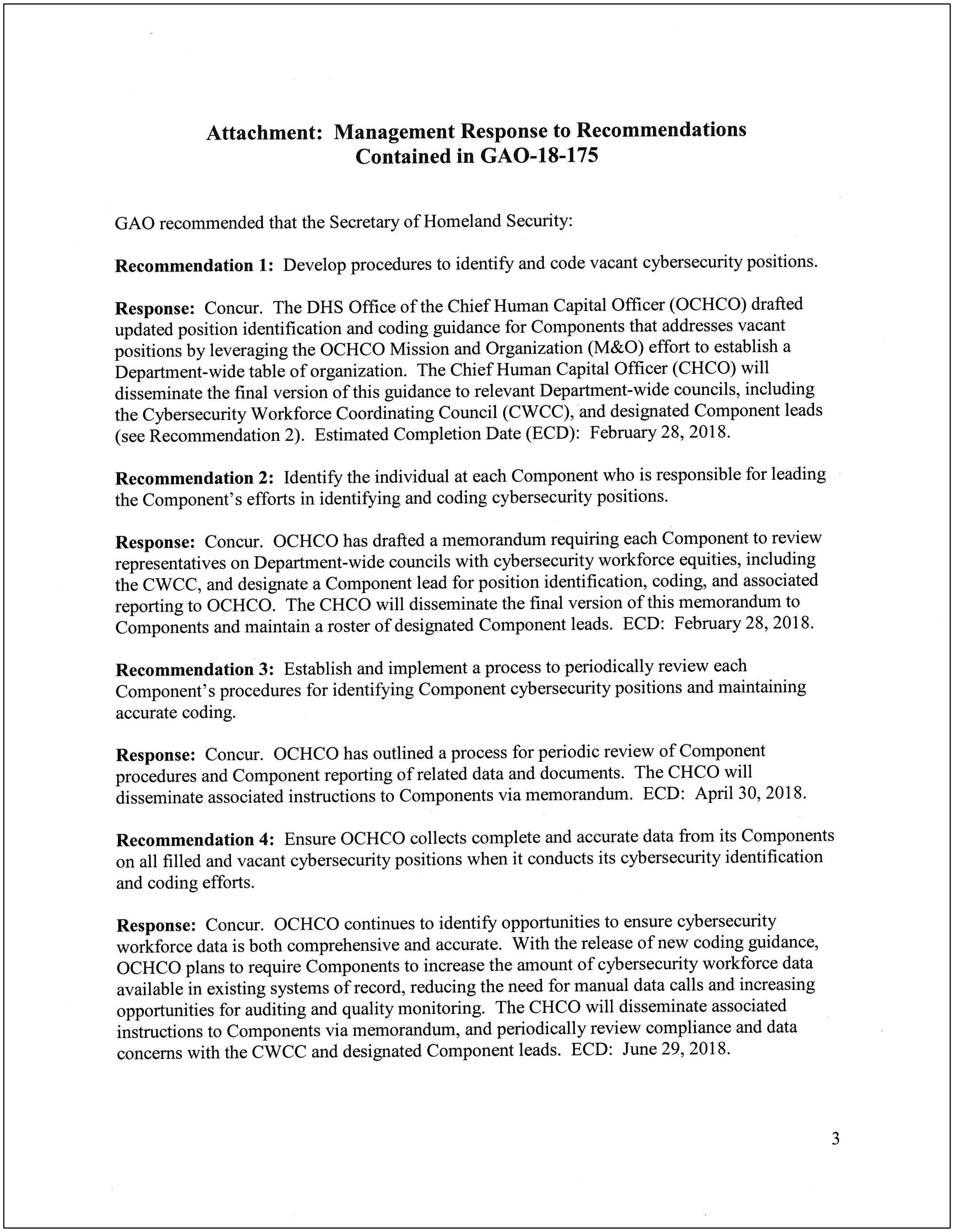
The draft report contained six recommendations with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.



Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office



Attachment: Management Response to Recommendations Contained in GAO-18-175

GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Develop procedures to identify and code vacant cybersecurity positions.

Response: Concur. The DHS Office of the Chief Human Capital Officer (OCHCO) drafted updated position identification and coding guidance for Components that addresses vacant positions by leveraging the OCHCO Mission and Organization (M&O) effort to establish a Department-wide table of organization. The Chief Human Capital Officer (CHCO) will disseminate the final version of this guidance to relevant Department-wide councils, including the Cybersecurity Workforce Coordinating Council (CWCC), and designated Component leads (see Recommendation 2). Estimated Completion Date (ECD): February 28, 2018.

Recommendation 2: Identify the individual at each Component who is responsible for leading the Component's efforts in identifying and coding cybersecurity positions.

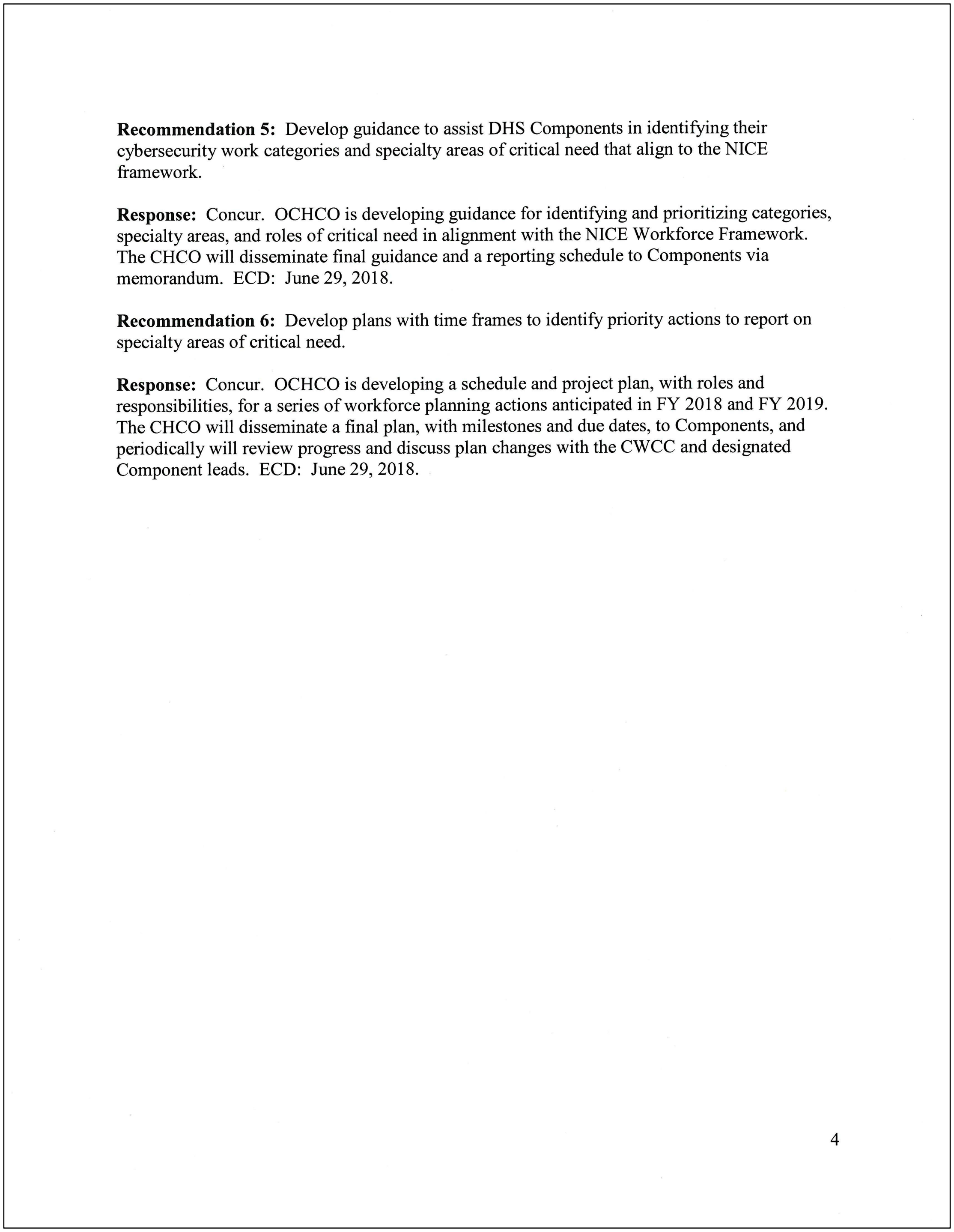
Response: Concur. OCHCO has drafted a memorandum requiring each Component to review representatives on Department-wide councils with cybersecurity workforce equities, including the CWCC, and designate a Component lead for position identification, coding, and associated reporting to OCHCO. The CHCO will disseminate the final version of this memorandum to Components and maintain a roster of designated Component leads. ECD: February 28, 2018.

Recommendation 3: Establish and implement a process to periodically review each Component's procedures for identifying Component cybersecurity positions and maintaining accurate coding.

Response: Concur. OCHCO has outlined a process for periodic review of Component procedures and Component reporting of related data and documents. The CHCO will disseminate associated instructions to Components via memorandum. ECD: April 30, 2018.

Recommendation 4: Ensure OCHCO collects complete and accurate data from its Components on all filled and vacant cybersecurity positions when it conducts its cybersecurity identification and coding efforts.

Response: Concur. OCHCO continues to identify opportunities to ensure cybersecurity workforce data is both comprehensive and accurate. With the release of new coding guidance, OCHCO plans to require Components to increase the amount of cybersecurity workforce data available in existing systems of record, reducing the need for manual data calls and increasing opportunities for auditing and quality monitoring. The CHCO will disseminate associated instructions to Components via memorandum, and periodically review compliance and data concerns with the CWCC and designated Component leads. ECD: June 29, 2018.



Recommendation 5: Develop guidance to assist DHS Components in identifying their cybersecurity work categories and specialty areas of critical need that align to the NICE framework.

Response: Concur. OCHCO is developing guidance for identifying and prioritizing categories, specialty areas, and roles of critical need in alignment with the NICE Workforce Framework. The CHCO will disseminate final guidance and a reporting schedule to Components via memorandum. ECD: June 29, 2018.

Recommendation 6: Develop plans with time frames to identify priority actions to report on specialty areas of critical need.

Response: Concur. OCHCO is developing a schedule and project plan, with roles and responsibilities, for a series of workforce planning actions anticipated in FY 2018 and FY 2019. The CHCO will disseminate a final plan, with milestones and due dates, to Components, and periodically will review progress and discuss plan changes with the CWCC and designated Component leads. ECD: June 29, 2018.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov
Chris P. Currie, (404) 679-1875 or curriec@gao.gov

Staff Acknowledgments

In addition to the contacts above, Ben Atwater (assistant director), Tammi Kalugdan (assistant director), David Hong (analyst-in-charge), Christy Abuyan, Alexander Anderegg, David Blanding, Jr., Chris Businsky, Wayne Emilien, Jr., David Plocher, Luis E. Rodriguez, and Priscilla Smith made significant contributions to this report.

Appendix V: Accessible Data

Data Tables

Accessible Data for Figure 1: Department of Homeland Security Components, Including Six Selected for GAO's Review

Support Components

- Analysis and Operations
- Departmental Management and Operations
- Domestic Nuclear Detection Office
- Federal Law Enforcement Training Centers
- National Protection and Programs Directorate
- Office of Health Affairs
- Office of Inspector General
- Science and Technology Directorate

Support Components Selected by GAO

- Departmental Management and Operations
- National Protection and Programs Directorate
- Science and Technology Directorate

Operational Components

- U.S. Customs and Border Protection
- U.S. Citizenship and Immigration Services
- U.S. Coast Guard

- Federal Emergency Management Agency
- U.S. Immigration and Customs Enforcement
- U.S. Secret Service
- Transportation Security Administration

Operational Components Selected by GAO

- U.S. Customs and Border Protection
- U.S. Citizenship and Immigration Services
- U.S. Secret Service

Accessible Data for Figure 2: Department of Homeland Security Positions Coded for Cybersecurity Functions, June 2016-August 2017

Month	Filled and Vacant (percent)	Filled ONLY (percent)
Jun	6.5	7.1
Jul	12.1	13.3
Aug	12.5	13.7
Oct	12.4	13.6
Dec	20.4	22.3
Mar	72.5	79.5
Mar	76.1	83.5
Apr	75.4	82.7
Apr	75.9	83.2
May	85.7	94.0
May	85	93.2
Jul	81.6	89.5
Aug	80.1	87.8
Aug	78.7	86.3

Agency Comment Letter

Accessible Text for Appendix III: Comments from the Department of Homeland Security

Page 1

U.S. Department of Homeland Security

Washington, DC 20528 •

Homeland Security

January 19, 2018

Gregory C. Wilshusen

Director, Information Security Issues

U.S. Government Accountability Office

441 G Street, NW

Washington, D.C. 20548

Re: Draft Report GAO-18-175, "CYBERSECURITY WORKFORCE: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements"

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive recognition of actions DHS has taken to identify its cybersecurity workforce and to conduct Department-wide cybersecurity workforce analysis and planning. DHS remains committed to strengthening processes for examining its cybersecurity workforce, identifying critical gaps, and addressing these gaps, as appropriate.

It is important to note that DHS has been conducting Department-wide cybersecurity workforce analyses since 2011 and working to apply the National Initiative for Cybersecurity Education (NICE) Workforce Framework since its first iteration was still in draft. While the framework has been helpful in creating a common taxonomy and terminology for a field that continues to evolve, ensuring a common understanding of framework structures and terms across DHS and federal agencies remains a challenge. DHS will continue to leverage the NICE framework and will increase efforts to translate and customize its content to meet the DHS mission, ensuring maximum utility and availability of workforce gap information.

The draft report contained six recommendations with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

Page 2

Again, thank you for the opportunity to review and comment on this draft report.

Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Director

Departmental GAO-OIG Liaison Office

Page 3

Attachment: Management Response to Recommendations

Contained in GAO-18-175

GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Develop procedures to identify and code vacant cybersecurity positions.

Response: Concur. The DHS Office of the Chief Human Capital Officer (OCHCO) drafted updated position identification and coding guidance for Components that addresses vacant positions by leveraging the OCHCO Mission and Organization (M&O) effort to establish a Department-wide table of organization. The Chief Human Capital Officer (CHCO) will disseminate the final version of this guidance to relevant Department-wide councils, including the Cybersecurity Workforce Coordinating Council (CWCC), and designated Component leads (see Recommendation 2). Estimated Completion Date (ECD): February 28, 2018.

Recommendation 2: Identify the individual at each Component who is responsible for leading the Component's efforts in identifying and coding cybersecurity positions.

Response: Concur. OCHCO has drafted a memorandum requiring each Component to review representatives on Department-wide councils with cybersecurity workforce equities, including the CWCC, and designate a Component lead for position identification, coding, and associated reporting to OCHCO. The CHCO will disseminate the final version of this memorandum to Components and maintain a roster of designated Component leads. ECD: February 28, 2018.

Recommendation 3: Establish and implement a process to periodically review each Component's procedures for identifying Component cybersecurity positions and maintaining accurate coding.

Response: Concur. OCHCO has outlined a process for periodic review of Component procedures and Component reporting of related data and documents. The CHCO will disseminate associated instructions to Components via memorandum. ECD: April 30, 2018.

Recommendation 4: Ensure OCHCO collects complete and accurate data from its Components on all filled and vacant cybersecurity positions when it conducts its cybersecurity identification and coding efforts.

Response: Concur. OCHCO continues to identify opportunities to ensure cybersecurity workforce data is both comprehensive and accurate. With the release of new coding guidance, OCHCO plans to require Components to increase the amount of cybersecurity workforce data available in existing systems of record, reducing the need for manual data calls and increasing opportunities for auditing and quality monitoring. The CHCO will disseminate associated instructions to Components via memorandum, and periodically review compliance and data concerns with the CWCC and designated Component leads. ECD: June 29, 2018.

Page 4

Recommendation 5: Develop guidance to assist DHS Components in identifying their cybersecurity work categories and specialty areas of critical need that align to the NICE framework.

Response: Concur. OCHCO is developing guidance for identifying and prioritizing categories, specialty areas, and roles of critical need in alignment with the NICE Workforce Framework. The CHCO will disseminate final guidance and a reporting schedule to Components via memorandum. ECD: June 29, 2018.

Recommendation 6: Develop plans with time frames to identify priority actions to report on specialty areas of critical need.

Response: Concur. OCHCO is developing a schedule and project plan, with roles and responsibilities, for a series of workforce planning actions anticipated in FY 2018 and FY 2019. The CHCO will disseminate a final plan, with milestones and due dates, to Components, and periodically will review progress and discuss plan changes with the CWCC and designated Component leads. ECD: June 29, 2018.

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 (http://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 http://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, http://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, LinkedIn, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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