

**OFFICE OF INSPECTOR GENERAL**

# **DHS Needs to Improve Cybersecurity Workforce Planning**



Homeland  
Security

**September 23, 2019**

**OIG-19-62**



# DHS OIG HIGHLIGHTS

## *DHS Needs to Improve Cybersecurity Workforce Planning*

September 23, 2019

### Why We Did This Audit

In December 2014, Congress enacted the *Cybersecurity Workforce Assessment Act*, which required the Department of Homeland Security to assess its cybersecurity workforce and develop a strategy for addressing workforce gaps. We performed this audit to assess DHS' progress in fulfilling the requirements of the Act.

### What We Recommend

We recommend the Chief Human Capital Officer assign staff resources, establish a centralized approach, and ensure cross-component commitment needed for DHS' implementation of the *Cybersecurity Workforce Assessment Act*.

#### For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov)

### What We Found

DHS has not fully met requirements in the *Cybersecurity Workforce Assessment Act* to assess its cybersecurity workforce and develop a strategy to address workforce gaps. The Department did not submit annual workforce assessments to Congress by the statutorily defined due dates for the past four years. DHS also did not include all required information in the assessments once they were submitted. Further, the Department did not submit an annual cybersecurity workforce strategy to Congress, as required, between 2015 and 2018. As of February 2019, DHS only submitted one workforce strategy in 2016, but it did not include all required information.

DHS' lack of progress in meeting the requirements of the Act can be attributed to both external and internal factors. Legislation passed in 2014 and 2015 created overlapping and new requirements for cybersecurity workforce planning and reporting. DHS fell behind in responding to these mandates because it did not have consistent and detailed information on its cybersecurity workforce readily available to comply with the new reporting requirements.

Without a complete workforce assessment and strategy, DHS is not well positioned to carry out its critical cybersecurity functions in the face of ever-expanding cybersecurity threats. Lacking an assessment, DHS cannot provide assurance that it has the appropriate skills, competencies, and expertise positioned across its components to address the multifaceted nature of DHS' cybersecurity work. In addition, the Department may not have an understanding of its future hiring or training needs to maintain a qualified and capable workforce to secure the Nation's cyberspace.

### Management Response

The Department concurred with all three recommendations and initiated corrective actions to address them.

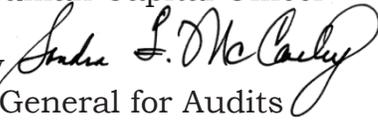


**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

Washington, DC 20528 / [www.oig.dhs.gov](http://www.oig.dhs.gov)

September 23, 2019

MEMORANDUM FOR: Angela Bailey  
Chief Human Capital Officer  
Office of the Chief Human Capital Officer

FROM: Sondra F. McCauley   
Assistant Inspector General for Audits

SUBJECT: *DHS Needs to Improve Cybersecurity Workforce Planning*

Attached for your action is our final report, *DHS Needs to Improve Cybersecurity Workforce Planning*. We have incorporated the formal comments from the Department.

The report contains three recommendations aimed at improving the Department's Cybersecurity Workforce. Your office concurred with all three recommendations. Based on information provided in your response to the draft report, we consider recommendations 1, 2, and 3 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions.

Please send your response or closure request to [OIGAuditsFollowup@oig.dhs.gov](mailto:OIGAuditsFollowup@oig.dhs.gov). Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination

Please call me with any questions, or your staff may contact Kristen Bernard, Deputy Assistant Inspector General for Technology Audits & Analytics Support, at (202) 981-6000.

Attachment



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

**Table of Contents**

**Background** ..... 1

**Results of Audit**..... 4

    DHS Has Not Met Requirements to Assess Its Cybersecurity Workforce  
    and Develop a Strategy ..... 5

    Multiple Factors Contributed to Lack of Progress in DHS Cybersecurity  
    Workforce Planning..... 12

    DHS Cannot Ensure Readiness and Capacity to Carry Out Its Critical  
    Cybersecurity Functions ..... 15

**Recommendations**..... 17

**Appendixes**

    Appendix A: Objective, Scope, and Methodology ..... 20

    Appendix B: Management Comments to the Draft Report..... 21

    Appendix C: Office of Audits Major Contributors to This Report ..... 24

    Appendix D: Report Distribution..... 25

**Abbreviations**

CHCO	Chief Human Capital Officer
CISA	Cybersecurity and Infrastructure Security Agency
CS&C	Office of Cybersecurity and Communications
GAO	Government Accountability Office
ICE	U.S. Immigration and Customs Enforcement
IT	Information Technology
OCHCO	Office of the Chief Human Capital Officer
Secret Service	United States Secret Service



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

### **Background**

Federal agencies are dependent upon computerized (cyber) information technology (IT) systems and electronic data to carry out operations and process, maintain, and report essential information. Hence, the security of these systems and data is vital to public confidence and the Nation's safety, prosperity, and well-being. However, safeguarding sensitive data and information systems from unauthorized access and potential exploits is becoming a major challenge. In the last several decades, advances in IT and the proliferation of mobile devices have introduced new cybersecurity risks across all industries; researchers predict that more than 20 billion devices will be connected to the internet by 2020. Our National security and our economy depend on a stable, safe, and resilient cyber space.

The Department of Homeland Security plays a critical role in protecting the Nation's cyber space, which includes not only DHS' own computer systems and information, but also those belonging to other Federal civilian agencies. For example, DHS coordinates and integrates information among Federal cyber-operations centers, state and local governments, and the private sector. Approximately 14,000 DHS employees perform a diverse range of cybersecurity functions across at least 18 DHS components and in 96 different operational programs. In supporting these missions, the workforce performs a variety of cybersecurity functions, including incident response, digital forensics, cybercrime investigation, and cybersecurity threat analysis. Three DHS components employ approximately 70 percent of DHS' total cybersecurity workforce, as described in table 1.<sup>1</sup>

---

<sup>1</sup> Several additional DHS components perform cybersecurity work, such as U.S. Customs and Border Protection, U.S. Customs & Immigration Services, Office of the Chief Information Officer, Federal Law Enforcement Training Centers, Transportation Security Administration, and Science & Technology Directorate.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

**Table 1: Missions and Cybersecurity Functions of Selected DHS Components**

<b>DHS Component</b>	<b>Description</b>
Cybersecurity and Infrastructure Security Agency (CISA)	CISA is primarily responsible for fulfilling DHS’ national, non-law enforcement cybersecurity missions. It also provides crisis management, incident response, and defense against cyber-attacks for Federal civil executive branch networks (.gov). The National Cybersecurity and Communications Integration Center, which is a part of CISA, serves as a central location for operational components involved in cyber response activities to share information between the public and private sector.
U.S. Immigration and Customs Enforcement (ICE)	ICE focuses on internet-related criminal activities and cross-border cybercrimes, such as domestic and international investigations into cross-border smuggling of people and guns, and investigations of narcotics, financial, cyber, and immigration-related crimes.
U.S. Secret Service (Secret Service)	Secret Service investigates criminal organizations and individuals targeting critical financial infrastructure and payment systems. Secret Service is to safeguard designated protectees and help secure the Nation’s banking and finance infrastructure. Secret Service’s cybersecurity workforce conducts criminal investigations and protects its systems, networks, and data.

Source: DHS components’ mission and responsibilities

The supply of cybersecurity talent to meet the Federal Government’s increasing demand is not sufficient. Competition in the marketplace to recruit and retain the same workforce grows as the demand for cyber defense experts to protect our Nation’s networks and information systems increases. The Government Accountability Office (GAO) reported in February 2018 that achieving a resilient, well-trained, and dedicated cybersecurity workforce to help protect Federal government information and infrastructure has been a longstanding challenge.<sup>2</sup> During a congressional hearing, “Examining DHS’s Cybersecurity Mission,” on October 3, 2017, it was estimated that 24 percent of DHS’ Cybersecurity and Communications positions remained unfilled. At the hearing, a member of the U.S. House of Representatives raised specific concerns regarding unfilled positions in CISA’s Office of Cybersecurity and Communications, which is a central hub for cyber defense activities.<sup>3</sup>

<sup>2</sup> *Cybersecurity Workforce, Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirement*, GAO-18-175, February 6, 2018

<sup>3</sup> The National Protection and Programs Directorate was reorganized as CISA in November 2018. Congressional hearing transcript of National Protection and Programs Directorate’s Office Cybersecurity and Communications Assistant Secretary Jeanette Manfra for a House



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

Further, according to a non-profit organization's global study, 80 percent of respondents said it was likely or very likely their enterprises would experience cyberattacks in 2018. Almost daily, we learn of nefarious attempts by nation states to impact our information systems, including election systems and critical infrastructure. However, organizations continue to experience shortage of and difficulty in recruiting qualified personnel to fill cybersecurity positions. Specifically:

- Fifty-nine percent of enterprises reported that they have open (unfilled) cybersecurity positions.
- Fifty-four percent reported it takes, on average, 3 months or longer to fill open positions.
- Thirty percent of those surveyed reported that fewer than 25 percent of applicants are qualified.
- Thirty-one percent reported that only 25 to 50 percent of applicants are sufficiently qualified for the positions enterprises hope to fill.

Funding limitations and a lengthy hiring process also inhibit the Federal government's hiring and retention of cybersecurity professionals. According to senior Federal IT and cybersecurity officials, they lack the money, organizational flexibility, and culture to close the workforce gap.<sup>4</sup> Specifically, in fiscal year 2019, Federal cyber programs requested \$477 million but received only \$432 million. Agencies are further constrained by the lengthy security clearance process, as most IT or cybersecurity jobs require candidates to possess a clearance. For example, from the time they are hired, it takes 224 days on average for individuals to receive a Top Secret/Sensitive Compartmented Information clearance.

In the face of ever-increasing and more sophisticated cyber-incidents, the President and Congress have raised concerns about whether DHS and other agencies are hiring and retaining the quantity and quality of IT employees needed to perform cybersecurity functions. On December 18, 2014, Congress enacted the *Cybersecurity Workforce Assessment Act* ("the Act").<sup>5</sup> The Act is meant to position DHS to improve workforce planning capabilities to carry out critical cybersecurity functions. Specifically, the Act requires the DHS Secretary to (1) assess the readiness of DHS' cybersecurity workforce to meet its mission, and (2) develop a comprehensive workforce strategy to enhance the

---

Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection hearing titled *Examining DHS's Cybersecurity Mission (October 3, 2017)*.

<sup>4</sup> *Cybersecurity Federal Efforts are Under Way that May address Workforce Challenges*, (GAO-17-533T, April 4, 2017)

<sup>5</sup> Public Law 113-246



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

Department's recruitment, retention, and training of the cybersecurity workforce. The DHS Office of Chief Human Capital Officer (OCHCO), located within the DHS Management Directorate, is responsible for DHS-wide human capital policy development and workforce planning and has the lead in ensuring compliance with this Act.

In addition, Congress enacted the following Federal cybersecurity workforce legislation in 2014 and 2015.

- *Border Patrol Agent Pay Reform Act of 2014* grants DHS authority to create a cybersecurity-focused personnel system exempt from many civil service restrictions.<sup>6</sup> Section 4 of this legislation, the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, requires DHS to (1) identify all cybersecurity workforce positions within the Department, (2) determine the cybersecurity work category and specialty area of such positions, and (3) assign the corresponding data element employment code to each cybersecurity position.
- *Federal Cybersecurity Workforce Assessment Act of 2015* requires Federal agencies to identify all cyber-related positions and assign employment codes.<sup>7</sup> Specifically, each agency was required to conduct and report a baseline assessment of its existing workforce to Congress by December 2016, and complete a revised coding of IT, cybersecurity, and cyber-related positions and vacancies by September 2018.

As threats to DHS become more and more sophisticated, DHS must have a cybersecurity workforce that is well trained, resilient, and dedicated to the mission. Our audit objective was to assess DHS' progress in fulfilling requirements of the *Cybersecurity Workforce Assessment Act*, including the Department's cybersecurity workforce readiness, and developing a workforce strategy to maintain its capacity, training, recruitment, and retention.

### Results of Audit

DHS has not fully met requirements in the *Cybersecurity Workforce Assessment Act* to assess its cybersecurity workforce and develop a strategy to address workforce gaps. The Department did not submit annual workforce assessments to Congress by the statutorily defined due dates for the past four years. DHS also did not include all required information in assessments once they were submitted. Further, the Department did not submit an annual

---

<sup>6</sup> Public Law 113-277

<sup>7</sup> Public Law 114-113



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

cybersecurity workforce strategy to Congress, as required, between 2015 and 2018. As of February 2019, OCHCO was still developing DHS' second strategy, which was due approximately two years earlier, in December 2016.

DHS' lack of progress in meeting the requirements of the Act can be attributed to both external and internal factors. Numerous legislation was enacted in 2014 and 2015 that created new requirements for cybersecurity workforce planning and reporting. DHS fell behind in responding to these mandates because it did not have consistent and detailed information on its cybersecurity workforce readily available to comply with the new reporting requirements.

Without a complete workforce assessment and strategy, DHS is not well positioned to carry out its critical cybersecurity functions in the face of ever-expanding cybersecurity threats. Lacking an assessment, DHS cannot provide assurance that it has the appropriate skills, competencies, and expertise positioned across its components to address the multifaceted nature of DHS cybersecurity work. In addition, the Department may not have an understanding of its future hiring or training needs to maintain a qualified and capable workforce to secure the Nation's cyberspace.

### **DHS Has Not Met Requirements to Assess Its Cybersecurity Workforce and Develop a Strategy**

DHS was mandated in 2014 to assess its cybersecurity workforce and develop a comprehensive strategy to ensure sufficient staffing to perform cybersecurity functions. In response, OCHCO began various workforce planning activities to identify and assess the Department's cybersecurity positions. However, the Department has not met the statutorily defined due dates for completing the annual workforce assessments. Further, the assessments reported to Congress were incomplete, as DHS did not fully identify the readiness, capacity, and training needs of its cybersecurity workforce. Additionally, DHS did not complete a comprehensive strategy for cybersecurity on time and it did not include all required elements in the submission to Congress.

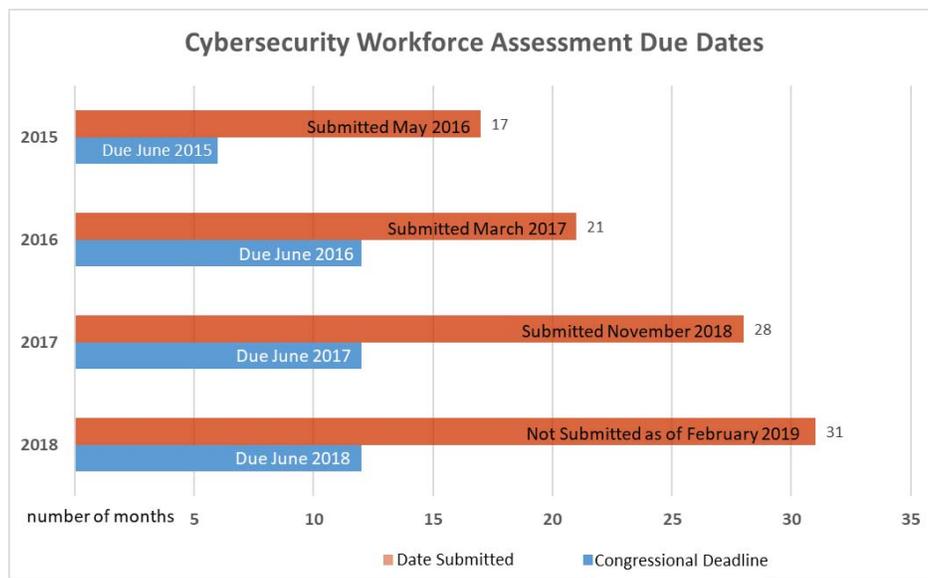


## OFFICE OF INSPECTOR GENERAL Department of Homeland Security

### DHS Has Not Fully Complied with Cybersecurity Workforce Assessment Requirements

DHS has not submitted a cybersecurity workforce assessment each year, as required by the *Cybersecurity Workforce Assessment Act*. The Department was required to submit a workforce assessment to Congress within 180 days after enactment, by June 2015, and annually thereafter for 3 years. However, OCHCO submitted each assessment, on average, 12 months late. For example, OCHCO submitted the first cybersecurity workforce assessment to Congress in May 2016, 11 months past the June 2015 due date. Each subsequent assessment was submitted well beyond the required date, as depicted in figure 1. As of February 2019, DHS had not yet completed the fourth assessment, which was due in June 2018.

**Figure 1: Submission Dates and Status of DHS' Cybersecurity Workforce Assessment to Congress**



Source: OIG analysis of DHS documentation and the *Cybersecurity Workforce Assessment Act*

### Workforce Assessments Did Not Include All Required Information

DHS did not include essential required data in the three workforce assessments it submitted to Congress. Specifically, none of the assessments DHS submitted contained information pertaining to the readiness, capacity, recruitment, and training of its cybersecurity workforce. According to the Act, the workforce assessments should have included the following key elements:



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

1. An assessment of the readiness and capacity of the DHS workforce to meet its cybersecurity mission.
2. Information on the location of cybersecurity workforce positions in the Department.
3. Information on which cybersecurity workforce positions are:
  - o permanent full-time equivalent DHS employees (including, to the greatest extent practicable, demographic information about such employees),
  - o independent contractors,
  - o individuals employed by other Federal agencies, or
  - o vacant.
4. Information on the percent of individuals in each cybersecurity category and specialty area who received essential training to perform their jobs, and reasons why training was not received, as applicable.<sup>8</sup>

#### *DHS' 2016 Cybersecurity Workforce Assessment*

DHS' first cybersecurity workforce assessment, submitted in 2016, was a 3-page document that did not include any of the four elements required by the Act.<sup>9</sup> OCHCO reported on its challenges in recruiting, retaining, and filling the gaps of its cybersecurity workforce and the high-level actions underway to address these challenges. However, OCHCO did not include a detailed assessment of the readiness and capacity of its workforce to meet its cybersecurity mission, as required. Specifically, OCHCO did not identify its cybersecurity workforce positions and vacancies, including which positions are filled by full-time equivalent employees, contractors, or employees from other Federal agencies. In addition, OCHCO did not identify the percent of individuals within each cybersecurity category who received essential training to perform their jobs. OCHCO officials acknowledged that their first assessment fell short of meeting requirements of the *Cybersecurity Workforce Assessment Act* because of a DHS leadership decision to address multiple similar requirements from other legislation in its first assessment, such as the *Homeland Security Cybersecurity Workforce Assessment Act*.<sup>10</sup>

---

<sup>8</sup> The National Institute of Standards and Technology organizes cybersecurity and related work into its National Initiative for Cybersecurity Education Framework (Special Publication 800-181, August 2017). As such, cybersecurity and related work can be organized into 7 categories and 31 specialty areas.

<sup>9</sup> *Annual Report, Usage of Cybersecurity Human Capital Authorities Granted by 6 United States Code 147*, May 3, 2016

<sup>10</sup> *Border Patrol Agent Pay Reform Act of 2014*, Section 4, Public Law 113-277

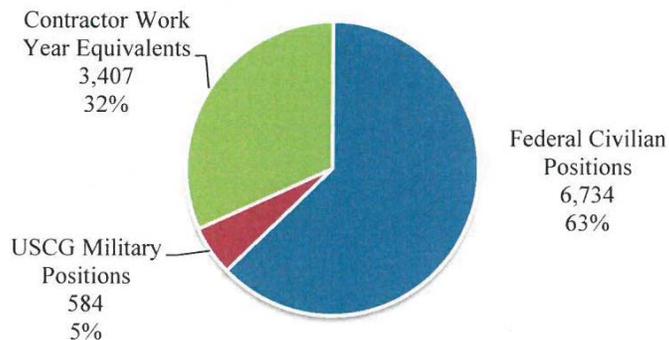


**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

*DHS' 2017 Cybersecurity Workforce Assessment*

DHS submitted its second assessment to Congress in March 2017.<sup>11</sup> While we found DHS' second assessment was, at 41 pages, more comprehensive, OCHCO still did not include all required elements. The assessment provided an overview of all current DHS employees and discussed the readiness of the cybersecurity workforce to meet mission requirements. Specifically, OCHCO identified DHS-wide cybersecurity positions and vacancies, as depicted in figure 2, showing a total of 10,725 civilian employees, military personnel, and contractors.

**Figure 2: Total DHS Cybersecurity Workforce by Position Type**



Source: DHS *Comprehensive Cybersecurity Workforce Update to Congress*, March 16, 2017<sup>12</sup>

In addition, OCHCO documented a partial breakdown of its cybersecurity workforce, such as demographics for occupational series, and grade levels of positions. OCHCO also provided background information on the Department's cybersecurity personnel planning program and outlined its ongoing efforts to code certain high-tech positions. However, OCHCO's assessment did not include the percentage of individuals within each cybersecurity category who had received essential training to perform their jobs, as required.

Moreover, OCHCO did not identify training completed or essential training that had not been received. In the assessment, OCHCO stated that the variation in DHS cybersecurity work leads components to develop unique approaches to training employees to ensure their mission readiness. Although 9 of the 14

<sup>11</sup> *Comprehensive Cybersecurity Workforce Update to Congress*, March 16, 2017

<sup>12</sup> A Contractor Work Year Equivalent is the equivalent of 2,080 hours of compensated Federal employment in a fiscal year.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

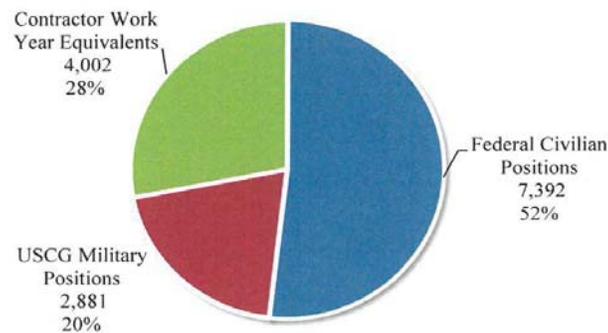
DHS components indicated they had processes to track employee certifications over time, OCHCO could not view or easily produce consolidated reports on this information.

A message by the Under Secretary for Management at the beginning of DHS' 2017 submission stated that the workforce assessment was compiled in response to numerous 2014 and 2015 mandates.<sup>13</sup> As it had done in 2016, DHS presented its 2017 assessment as a comprehensive report to Congress on its cybersecurity workforce planning efforts without fully addressing all data requirements of the *Cybersecurity Workforce Assessment Act*.

### *DHS' 2018 Cybersecurity Workforce Assessment*

DHS submitted its third assessment to Congress in November 2018.<sup>14</sup> In this 54-page assessment, OCHCO provided a broad overview of meeting the requirements of numerous 2014 and 2015 mandates.<sup>15</sup> OCHCO identified cybersecurity positions across DHS components and provided a breakdown of its total cybersecurity workforce. Specifically, as of December 2017, the Department had increased this workforce by approximately 20 percent from the previous year, to a total of 14,000 civilian, military, and contract employees as depicted in figure 3.<sup>16</sup>

**Figure 3: Total DHS Cybersecurity Workforce Position Types**



Source: DHS *Comprehensive Cybersecurity Workforce Update to Congress*, November 1, 2018

<sup>13</sup> *Border Patrol Agent Reform Act of 2014*, Public Law 113-277; *Cybersecurity Workforce Assessment Act*, Public Law 113-246; and *Federal Cybersecurity Workforce Assessment Act of 2015*, Public Law 114-113

<sup>14</sup> *Comprehensive Cybersecurity Workforce Update to Congress*, November 1, 2018

<sup>15</sup> *Border Patrol Agent Reform Act of 2014*, Public Law 113-277; *Cybersecurity Workforce Assessment Act*, Public Law 113-246; and *Federal Cybersecurity Workforce Assessment Act of 2015*, Public Law 114-113

<sup>16</sup> The numbers reported in the assessment were estimates and not exact numbers.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

OCHCO identified Federal civilian positions in DHS' cybersecurity workforce by component, with Secret Service (3,044), CISA (1,086), and ICE (1,026) employing the most positions. Criminal investigators and IT management specialists are among the most common positions. OCHCO also identified the demographics and locations for each position, as required by the Act. The assessment outlined cybersecurity training efforts across DHS, as well as the current state of cybersecurity training within each of the six components employing cybersecurity professionals.

While this submission was more detailed than its 2017 predecessor, OCHCO still did not provide all the information required by the Act. Primarily, OCHCO did not include an account of essential training that had not been received, nor an overview of challenges encountered in providing training. Nonetheless, OCHCO highlighted a number of difficulties DHS faced to accurately track and report on positions and training. In the 2018 assessment, OCHCO stated that its existing Human Resources systems did not contain all data required for complete and accurate workforce analysis. Therefore, the numbers in the assessment had been extracted and compiled from numerous systems and data reported from various DHS components.

More concerning, OCHCO reported that 862 (12 percent) of its 7,392 civilian cybersecurity positions were vacant, as compared to a 9 percent vacancy rate in 2017. Some components indicated they had a shortage of candidates and not enough cybersecurity workforce. Specifically, 17 of 18 components indicated that they needed to increase the number of their cybersecurity positions. As of February 2019, OCHCO was working on its fourth assessment, originally due in June 2018. The Department did not provide an estimate on when the fourth assessment is expected to be completed.

### **DHS Did Not Fully Comply with Cybersecurity Workforce Strategy Requirements**

To ensure the Department maintains adequate and well-trained personnel to meet its cyber mission, the *Cybersecurity Workforce Assessment Act* required DHS to develop a comprehensive workforce strategy within one year of enactment, by December 2015. In addition, the Act required that DHS maintain and update its strategy each year thereafter.

DHS has not timely met this workforce strategy requirement for any year since the law was passed. OCHCO did not complete its first comprehensive strategy until May 2016, approximately 5 months later. As of February 2019, OCHCO was still developing DHS' second strategy, which was due two years earlier, in

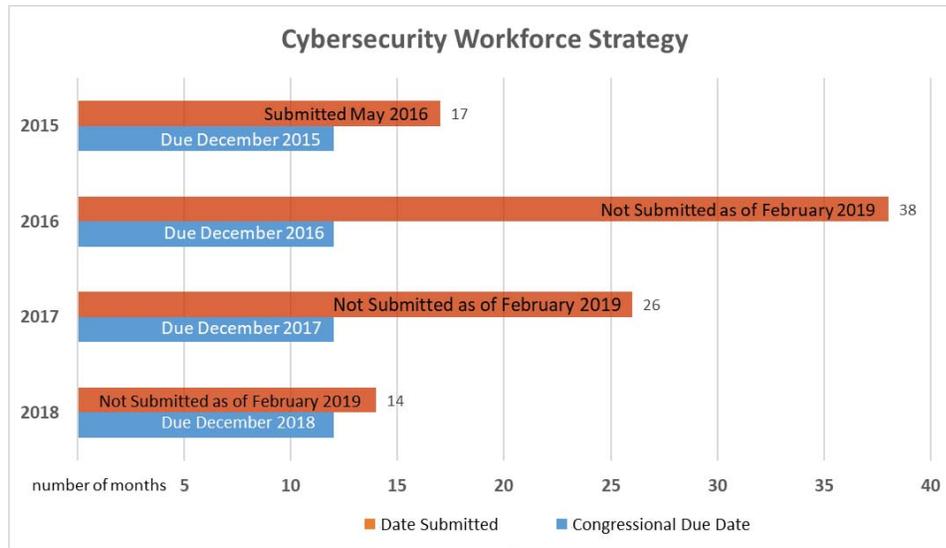


## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

December 2016. OCHCO also did not develop the third and fourth strategies, due to Congress in December 2017 and December 2018, respectively. Figure 4 illustrates the status of the Department’s cybersecurity workforce strategies for the past four years.

**Figure 4: Status of DHS’ Required Workforce Strategy to Congress**



Source: OIG analysis of DHS documentation and the *Cybersecurity Workforce Assessment Act*

### Workforce Strategy Did Not Include All Required Information

As with the Workforce Assessments, each Workforce Strategy DHS submitted to Congress did not fully meet requirements of the *Cybersecurity Workforce Assessment Act*. The Act required DHS to develop a comprehensive strategy to enhance the readiness, capacity, training, recruitment, and retention of its cybersecurity workforce, including the following:

- description of a multi-phased recruitment plan identifying:
  - experienced professionals,
  - members of disadvantaged or underserved communities,
  - unemployed, and
  - veterans;
- five-year implementation plan;
- ten-year projection of DHS’ cybersecurity workforce needs;
- obstacles impeding hiring and developing a cybersecurity workforce; and
- gaps in the existing DHS cybersecurity workforce and a plan to fill gaps.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

The 15-page cybersecurity workforce strategy that DHS submitted to Congress in May 2016 did not include all elements required by the Act.<sup>17</sup> Specifically, OCHCO did not include a required multi-phased recruitment plan, a 5-year implementation plan, or a 10-year projection of cybersecurity workforce. OCHCO also did not identify specific gaps in the existing workforce, a plan to fill the gaps, or obstacles to hiring and developing a cybersecurity workforce. Instead, OCHCO focused on the Department's plan for executing the requirements of different cybersecurity workforce legislation, which granted DHS additional authority to conduct recruiting and hiring for cybersecurity positions.<sup>18</sup> Also, OCHCO included in the strategy a discussion of DHS' effort to comply with requirements of the Office of Management and Budget and the Office of Personnel Management to review and code cybersecurity positions.<sup>19</sup>

DHS did not timely submit the subsequent annual workforce strategies as required by the Act, which were due in December of 2016, 2017, and 2018. As of February 2019, OCHCO was working with components to finalize a *DHS Cybersecurity Workforce Strategy, Fiscal Years 2018 – 2023, Version 3*. We reviewed the draft strategy and the 5-year implementation plan and found these still did not include all required elements, such as a cyber workforce projection or obstacles to hiring and developing DHS' cybersecurity workforce.

### **Multiple Factors Contributed to Lack of Progress in DHS Cybersecurity Workforce Planning**

DHS' lack of progress in meeting the requirements of the Act can be attributed to multiple external and internal factors. Legislation passed in 2014 and 2015 created new requirements for cybersecurity workforce planning and reporting. DHS fell behind in responding to these mandates because it did not have consistent and detailed information about its cybersecurity workforce readily available. Specifically, OCHCO lacked sufficient, centralized data for all components on cybersecurity workforce recruiting, hiring, and training to comply with the new reporting requirements.

---

<sup>17</sup> *The Plan for Execution of Authorities, Fiscal Year 2015 Report to Congress*, May 3, 2016

<sup>18</sup> *Border Patrol Agent Reform Act of 2014*, Public Law 113-277

<sup>19</sup> *DHS Cybersecurity Workforce Coding Guidance*, April 2016



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### **Overlapping Federal Laws Hindered DHS' Ability to Adequately Assess Its Cybersecurity Workforce**

DHS' lack of progress can be attributed to the enactment of three new laws in a short timeframe that overburdened the Department's ability to assess the readiness and capacity of its cybersecurity workforce. The various laws required DHS to perform some similar, but also some different and specific workforce assessment-related activities. Legislation included:

- *Border Patrol Agent Reform Act of 2014*, Public Law 113-277;
- *Cybersecurity Workforce Assessment Act*, Public Law 113-246; and
- *Federal Cybersecurity Workforce Assessment Act of 2015*, Public Law 114-113.

The overlapping nature of new requirements created additional work for those OCHCO personnel responsible for consolidating the associated data. An OCHCO official stated that, due to insufficient staff resources in 2016 (four full-time positions and eight contractor staff in March 2016), DHS management decided to consolidate the Department's multiple cybersecurity workforce legislative reporting requirements into a single report to Congress. As a result, DHS did not include all the information required under the Act, such as full-time employees' demographics, information on individuals employed by other Federal agencies, and a 10-year projection of the cybersecurity workforce.

### **DHS Did Not Have Data Readily Available to Respond to Cybersecurity Mandates**

Given overlapping legislation and a lack of consistent and detailed information on the cybersecurity workforce across all components, OCHCO officials have not been able to meet the required timeframes and reporting associated with the various mandates. In its 2016 report to Congress, the Department highlighted the complexities associated with conducting workforce planning and analysis across its 14,000 employees who execute a complex set of cybersecurity responsibilities.<sup>20</sup> For example, DHS' cybersecurity positions include more than 50 potential job titles and nearly 20 different occupational series across at least 12 components.<sup>21</sup> As such, it was difficult for the OCHCO to gain a consolidated view of the breadth of cybersecurity work performed across the Department. OCHCO noted that establishing an inventory of cybersecurity positions, and the myriad of personnel codes and occupation

---

<sup>20</sup> *Plan for Execution of Authorities, Fiscal Year 2015 Report to Congress*, May 3, 2016

<sup>21</sup> As reported in *Comprehensive Cybersecurity Workforce Update to Congress*, November 1, 2018



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

series associated with each, would be an essential first step for compiling the data necessary to report on workforce distribution within each component.<sup>22</sup> An initial inventory of DHS' cybersecurity work and workforce was completed in July 2016.

Despite this effort, OCHCO officials still lacked detailed information on the wide range of skills and experience of the cybersecurity workforce across all components in its 2016 and 2017 workforce assessment reports. For example, in its July 2016 Cybersecurity Workforce Analysis, OCHCO stated that the diversity of cyber missions, work, and positions made it challenging to create an overarching structure to describe DHS' work and workforce in a meaningful and accurate way. Moreover, information on the number of cybersecurity positions hired by each component, as well as the exact vacancy and attrition rates across each component was not centrally managed or readily available within DHS. The underlying factors that posed significant challenges for OCHCO to complete cybersecurity workforce planning efforts and reporting to Congress included:

- Cybersecurity work is not associated with a single occupational series or position title within DHS. DHS' Human Resources systems do not capture or maintain all the data required for cybersecurity-specific workforce analysis.
- DHS has not established department-wide certification requirements or training curriculum for Cybersecurity work. Also, Cybersecurity training is not centrally tracked, meaning it is not possible to ensure that employees receive the training necessary to perform their work.
- DHS does not have a department-wide position management capability allowing for the automated tracking of vacancies and filled positions.
- DHS does not have a centralized system for counting or coding contractor employees.

Until the Department addresses these issues, OCHCO officials will continue to rely on manual coordination with each component for information. For example, OCHCO officials had to conduct data calls to request training records in an attempt to identify the percent of individuals within each component who received essential training to perform their jobs. OCHCO officials stated they planned to coordinate with components to identify ways to overcome the

---

<sup>22</sup> The 2014 DHS Cybersecurity Workforce Inventory defined positions in the cybersecurity workforce as any performing at least one mission critical task.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

complexities associated with tracking cybersecurity training. In addition, OCHCO officials stated they planned to work with components to define cybersecurity positions and associated coding procedures over time.

### **DHS Cannot Ensure Readiness and Capacity to Carry Out Its Critical Cybersecurity Functions**

Given the lack of data to assess fully its cyber workforce, DHS cannot ensure readiness or capacity to carry out its critical cybersecurity functions in the face of ever-expanding cybersecurity threats. The risks to IT systems supporting the Federal Government are increasing as security threats continue to evolve and become more sophisticated. These risks include escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks. In FY 2017 alone, Federal agencies faced approximately 35,000 information security incidents involving threats such as web-based attacks, phishing attacks, and the loss or theft of computer equipment, among others.<sup>23</sup> These incidents pose a serious challenge to DHS to protect our National security and personal privacy. The potential impact of cybersecurity incidents includes loss or theft of critical data, compromised files related to millions of individuals, and degraded network or system performance, to name a few. These possibilities make it imperative that the Department intensify its efforts to retain current and recruit prospective cybersecurity employees to help manage this threat.

Until DHS completes a detailed and updated workforce assessment and strategy, it cannot take steps toward ensuring it has the appropriate skills, competencies, and expertise positioned across its components to address the multifaceted nature of cybersecurity work. The cyber-related work of each component varies greatly, ranging from unique and highly specialized technical cybersecurity knowledge to fulfill job requirements, to other work only warranting familiarity with cybersecurity to accomplish ad hoc or administrative tasks and support functions. In December 2017, DHS identified 18 components with a combined total of 96 individual programs performing cybersecurity work. Figure 5 shows support components in light grey, operational components in dark grey, and the 96 programs identified for each noted in blue.

---

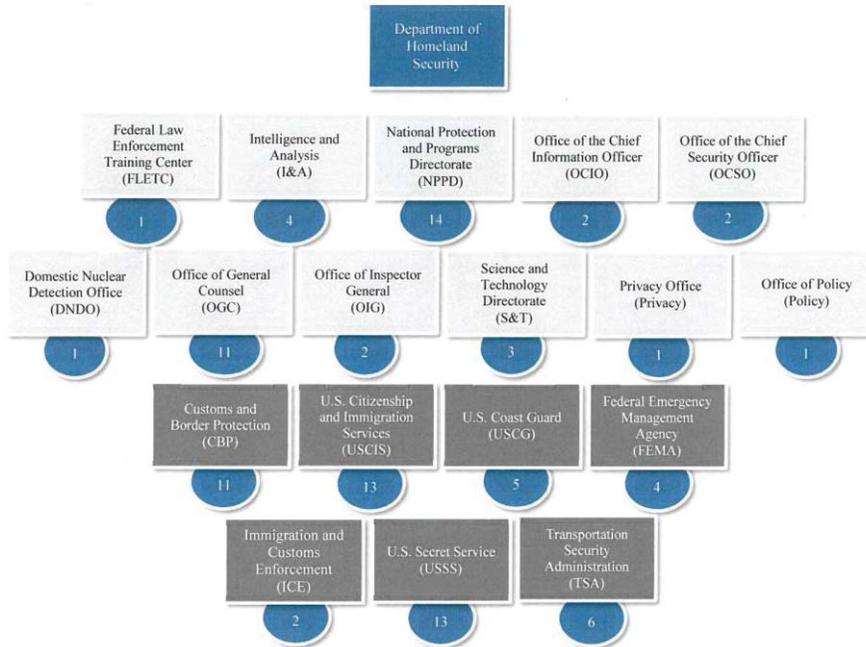
<sup>23</sup> Office of Management and Budget's 2018 annual Federal Information Security Modernization Act report to Congress



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

**Figure 5: DHS Cybersecurity Components and Number of Programs**



Source: DHS *Comprehensive Cybersecurity Workforce Update to Congress*, November 1, 2018

Without a thorough workforce assessment, DHS cannot be confident it has an adequate force of skilled cybersecurity professionals. Further, the Department cannot understand or plan for its future workforce needs to ensure it can secure the Nation’s cyberspace. These issues are exacerbated by the Department’s rising vacancy rate in civilian cybersecurity positions, which increased from 9 percent in March 2017 to 12 percent in November 2018. Hiring and recruiting efforts will become more critical as the Department faces a retirement surge in coming years. According to demographics reported in the most recent 2018 assessment, the average age for DHS’ cybersecurity workforce is 46, with 61 percent older than 40 years, and only 2 percent who are 30 years or younger.<sup>24</sup> DHS should complete its workforce strategy efforts to define fully the readiness, capacity, training, recruitment, and retention of its cybersecurity workforce.

<sup>24</sup> *Comprehensive Cybersecurity Workforce Update to Congress*, November 1, 2018



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### Recommendations

We recommend the DHS Chief Human Capital Officer:

**Recommendation 1:** Assign necessary staff resources to timely complete the required assessments and strategies regarding the DHS cyber workforce.

**Recommendation 2:** Establish a department-wide, coordinated approach to compiling centralized cybersecurity workforce data needed to fulfill reporting requirements in a timely manner.

**Recommendation 3:** Conduct oversight of component stakeholders to ensure department-wide commitment to addressing legislative reporting and data submission requirements.

### Management Comments and OIG Analysis

DHS OCHCO concurred with our three recommendations, and is taking steps or has implemented actions to address them. Appendix B contains DHS' management comments in their entirety. We also received technical comments to the draft report and revised the report as appropriate. We consider all recommendations resolved and open. A summary of DHS OCHCO's responses and our analysis follow.

**OCHCO Comments to Recommendation 1:** Concur. OCHCO has increased the size of its Cybersecurity Statutory Authority Program team from 4 federal staff and 8 contractors in 2016 to 16 federal staff and more than 100 contractors in 2019. OCHCO plans to have 35 federal personnel on-board and additional contract support by the end of fiscal year 2021.

**OIG Analysis of OCHCO Comments:** We believe that the steps OCHCO has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until OCHCO provides documentation to support that all planned corrective actions are completed, including documentation demonstrating that the Department, with additional resources, is assessing its cybersecurity workforce and developing the strategies as required.

**OCHCO Comments to Recommendation 2:** Concur. OCHCO has made significant progress in the collection and analysis of cybersecurity workforce data. During FY 2018, components completed coding of vacant and filled federal civilian positions in the Department's personnel payroll system. DHS



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

now has access to this data in a SharePoint site, a central system of record for workforce analysis and planning purposes. OCHCO is performing annual audits of component coding procedures and position descriptions to ensure workforce data is consistent and accurate.

**OIG Analysis of OCHCO Comments:** We believe that the steps OCHCO has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until OCHCO provides documentation to support that all planned corrective actions are completed. We ask OCHCO to provide documentation to support that the Department is collecting required information to fulfill the reporting requirements. For example, cybersecurity workforce positions include the following:

- permanent full-time equivalent DHS employees;
- independent contractors;
- individuals employed by other Federal agencies; or
- vacant positions.

In addition, OCHCO needs to provide documentation on the percentage of individuals in each cybersecurity category and specialty area who received essential training to perform their jobs, and reasons why training was not received. Using the data collected, OCHCO needs to provide support that it is incorporating the information to develop the Department's cyber workforce strategy, including projections or obstacles to hiring and developing DHS' cybersecurity workforce.

**OCHCO Comments to Recommendation 3:** Concur. DHS has made progress in consistently sharing reporting and data requirements with key component stakeholders. On March 3, 2018, OCHCO established the Lead Cybersecurity Workforce Official role in each component to oversee workforce analysis and reporting requirements. OCHCO continues to regularly share reporting and data submission requirements with component stakeholders through monthly meetings of the Cybersecurity Workforce Coordination Council and the Human Capital Leadership Council. OCHCO posts updates, new tasks for completion, and upcoming meetings on the dedicated SharePoint site.

**OIG Analysis of OCHCO Comments:** We believe that the steps OCHCO has taken satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until OCHCO provides documentation to support that planned corrective actions are completed. For example, we ask OCHCO to provide Cybersecurity Workforce Coordination Council monthly meeting minutes and components' data call responses to



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

show that the components are participating in department-wide efforts to address legislative reporting and data submission requirements.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### **Appendix A**

#### **Objective, Scope, and Methodology**

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

Our audit objective was to assess DHS' progress in fulfilling requirements of the *Cybersecurity Workforce Assessment Act*, including the Department's cybersecurity workforce readiness and development of a workforce strategy to maintain its capacity, training, recruitment, and retention.

We conducted our fieldwork at DHS Headquarters in Washington, DC. To answer our objective, we interviewed selected officials from DHS' OCHCO and Offices of the Chief Information Officer and Chief Security Officer. We also met with officials from CISA, ICE, and TSA.

As part of our evaluation, we assessed DHS' compliance with the Act's provisions. Specifically, we (1) examined and analyzed documentation received from DHS components; (2) reviewed the policies, procedures, and practices DHS implemented for the cybersecurity workforce at the program and component levels to assess readiness and capacity of the workforce and contractors; (3) investigated challenges, such as the security clearance process, that affect DHS' ability to recruit and retain cybersecurity professionals; and (4) examined several relevant audit reports from GAO.

While we reported information from the Department's assessments and strategies for informational and comparison purposes, we did not verify the accuracy of this data. We also did not rely on any computer-processed information from DHS components.

We conducted this compliance audit between November 2017 and February 2019, pursuant to the *Inspector General Act of 1978*, as amended. Accordingly, we followed generally accepted government auditing standards, with the exception of requirements related to the assessment of overall audit risk (6.11) and fraud (6.30), which, based on our professional judgment, were not significant in the context of the audit objective. The generally accepted government auditing 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

**Appendix B**  
**Management Comments to the Draft Report**

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



**Homeland  
Security**

August 21, 2019

MEMORANDUM FOR: Sondra McCauley  
Assistant Inspector General for Audits  
Office of Inspector General

FROM: Jim H. Crumacker, CIA, CFE  
Director  
Departmental GAO-OIG Liaison Office 

SUBJECT: Management Response to OIG Draft Report: "DHS Needs to  
Improve Cybersecurity Workforce Planning"  
(Project No. OIG 18-009-ITA-DHS)

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

The Department is pleased to note OIG's recognition of the critical role and related challenges DHS has in protecting the Nation's cyber space, including not only DHS's own computer systems and information but also those belonging to other Federal civilian agencies. DHS remains committed to:

- Protecting the confidentiality, integrity, and availability of its information systems and information, and
- Effectively serving as 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.

This includes strengthening processes from examining DHS' cybersecurity workforce to identifying critical gaps and addressing these gaps, as appropriate.

The draft report contained three 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.

Attachment



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

**Attachment: Management Response to Recommendations  
Contained in Project No. 18-009-ITA-DHS**

OIG recommended that the DHS Chief Human Capital Officer:

**Recommendation 1:** Assign necessary staff resources to timely complete the required assessments and strategies regarding the DHS cyber workforce.

**Response:** Concur. The Cybersecurity Statutory Authority Program (CSAP) team within the DHS Office of the Chief Human Capital Officer (OCHCO) has significantly increased in size since OIG announced this audit on October 24, 2017, up from four federal staff and eight contractors in 2016 to 16 federal staff and more than 100 contractors in 2019. CSAP’s staffing goal is to have 35 federal personnel on-board and additional contract support by the end of fiscal year (FY) 2021 (see table below). It is important to note achieving these staffing levels is dependent on FY 2020 and FY 2021 appropriations.

Table of Anticipated Staff and Contractor Personnel		
Federal	Contractor	Estimated Completion Date (ECD)
16	100+	Current
22	TBD	March 31, 2020
29	TBD	September 30, 2020
32	TBD	March 31, 2021
35	TBD	September 30, 2021

**Recommendation 2:** Establish a department-wide, coordinated approach to compiling centralized cybersecurity workforce data needed to fulfill reporting requirements in a timely manner.

**Response:** Concur. OCHCO has made significant progress in collection and analysis of cybersecurity workforce data. During FY 2018, Components completed coding of vacant and filled federal civilian positions in the Department’s personnel payroll system. DHS now has access to this data in a central system of record for workforce analysis and planning purposes. OCHCO is also performing annual audits of Component coding procedures and position descriptions to ensure workforce data is consistent and accurate. In addition, during FY 2018 OCHCO established a new SharePoint site for Component representatives that houses the latest coding and workforce analysis guidance and serves as a repository for all relevant Component documents and deliverables.

OCHCO has created and implemented the processes to fulfill this recommendation, and ongoing and future work will consist of monitoring and updating Component data to



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

ensure accuracy and consistency. DHS requests the OIG consider this recommendation resolved and closed as implemented.

**Recommendation 3:** Conduct oversight of Component stakeholders to promote department-wide commitment to addressing legislative reporting and data submission requirements.

**Response:** Concur. OCHCO has made significant progress in consistently sharing reporting and data requirements with key Component stakeholders. On March 3, 2018, OCHCO established the Lead Cybersecurity Workforce Official role in each Component to oversee workforce analysis and reporting requirements. OCHCO continues to regularly share reporting and data submission requirements with Component stakeholders through monthly meetings of the Cybersecurity Workforce Coordination Council and Human Capital Leadership Council. Updates – such as new tasks for completion and upcoming meetings – are posted to the dedicated SharePoint site.

OCHCO has created and implemented the processes to fulfill this recommendation, and ongoing and future work will consist of monitoring and updating Component data to ensure accuracy and consistency. DHS requests the OIG consider this recommendation resolved and closed as implemented.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

**Appendix C**  
**Office of Audits Major Contributors to This Report**

Chiu-Tong Tsang, Director  
Ann Brooks, Information Technology Auditor  
Corinn King, Independent Referencer  
Jane DeMarines, Communications Analyst  
Kelly Herberger, Communications Analyst



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

**Appendix D**  
**Report Distribution**

**Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
General Counsel  
Executive Secretary  
Director, GAO/OIG Liaison Office  
Assistant Secretary for Office of Policy  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs  
Office of the Chief Information Systems Officer  
Office of the Chief Information Security Officer  
DHS Privacy Office

**Office of the Chief Human Capital Officer**

Chief Human Capital Officer  
Executive Director Human Capital Policy and Programs  
Executive Director, Cyber Statutory Authority Program  
Audit Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees

## **Additional Information and Copies**

To view this and any of our other reports, please visit our website at:  
[www.oig.dhs.gov](http://www.oig.dhs.gov).

For further information or questions, please contact Office of Inspector General  
Public Affairs at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov).  
Follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).



### **OIG Hotline**

To report fraud, waste, or abuse, visit our website at [www.oig.dhs.gov](http://www.oig.dhs.gov) and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security  
Office of Inspector General, Mail Stop 0305  
Attention: Hotline  
245 Murray Drive, SW  
Washington, DC 20528-0305