



June 2018

CYBERSECURITY WORKFORCE

Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions

Accessible Version

GAO Highlights

Highlights of [GAO-18-466](#), a report to congressional committees

Why GAO Did This Study

A key component of mitigating and responding to cyber threats is having a qualified, well-trained cybersecurity workforce. The Federal Cybersecurity Workforce Assessment Act of 2015 requires OPM and federal agencies to take several actions related to cybersecurity workforce planning.

GAO is to monitor agencies' progress in implementing the act's requirements. For this report, GAO assessed whether: (1) OPM developed a coding structure and procedures for assigning codes to cybersecurity positions and submitted a progress report to Congress; (2) CFO Act agencies submitted complete, reliable baseline assessments of their cybersecurity workforces; and (3) CFO Act agencies established procedures to assign codes to cybersecurity positions. GAO examined OPM's coding procedures and progress report on the act's implementation, and baseline assessments and coding procedures from the 24 CFO Act agencies. GAO also interviewed relevant OPM and agency officials about efforts to address the act's requirements.

What GAO Recommends

GAO is making 30 recommendations to 13 agencies to fully implement two of the act's requirements on baseline assessments and coding procedures. Of the 12 agencies to which we made recommendations that provided comments on the report, 7 agreed with the recommendations made to them, 4 did not state whether they agreed or disagreed, and 1 did not agree with one of two recommendations made to it. GAO continues to believe that the recommendation is valid as discussed in this report.

View [GAO-18-466](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

June 2018

CYBERSECURITY WORKFORCE

Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions

What GAO Found

As required by the Federal Cybersecurity Workforce Assessment Act of 2015 (act), the Office of Personnel Management (OPM) developed a cybersecurity coding structure under the National Initiative for Cybersecurity Education (NICE) as well as procedures for assigning codes to federal civilian cybersecurity positions. However, OPM issued the coding structure and procedures 5 and 4 months later than the act's deadlines because OPM was working with the National Institute of Standards and Technology (NIST) to align the structure and procedures with the draft *NICE Cybersecurity Workforce Framework*, which NIST issued later than planned. OPM also submitted a progress report to Congress on the implementation of the act 1 month after it was due. The delays in issuing the coding structure and procedures have extended the expected time frames for implementing subsequent provisions of the act.

Most of the 24 agencies covered by the Chief Financial Officers (CFO) Act submitted baseline assessment reports to Congress but the results may not be reliable. As of March 2018, 21 of the 24 CFO Act agencies had conducted baseline assessments identifying the extent to which their cybersecurity employees held professional certifications and had submitted the assessment reports to Congress as required by the act. Three agencies had not conducted the assessments for various reasons, such as a lack of resources and tools to do so. Of the 21 agencies that did, 4 did not address all of the reportable information, such as the extent to which personnel without professional certifications were ready to obtain them or strategies for mitigating any gaps. Additionally, agencies were limited in their ability to obtain complete or consistent information about their cybersecurity employees and the certifications they held. This was because agencies had not yet fully identified all members of their cybersecurity workforces or did not have a consistent list of appropriate certifications for cybersecurity positions. As a result, the agencies had limited assurance that their assessment results accurately reflected all relevant employees or the extent to which those employees held appropriate certifications. This diminishes the usefulness of the assessments in determining the certification and training needs of these agencies' cybersecurity employees.

Most of the 24 CFO Act agencies established coding procedures, but 6 agencies only partially addressed certain activities required by OPM in their procedures. Of the 24 agencies reviewed, 23 had established procedures to identify their civilian cybersecurity positions and assign the appropriate employment codes to the positions as called for by the act. However, 6 of the 23 agencies did not address one or more of 7 activities required by OPM in their procedures, such as the activities to review all filled and vacant positions and annotate reviewed position descriptions with the appropriate employment code. These 6 agencies cited a variety of reasons for not addressing all of the required activities in their coding procedures. For example, these agencies stated that they addressed the activities in existing guidance or did not include activities that their components did not have the responsibility to perform. By not addressing all of the required activities in their coding procedures, the 6 agencies lack assurance that the activities will be performed or performed consistently throughout their agency.

Contents

Letter	1
Background	4
OPM Issued a Cybersecurity Position Coding Structure, Procedures, and Progress Report Later Than the Deadlines Established in the Act	11
Most CFO Act Agencies Submitted Baseline Assessments, but the Results May Not Be Reliable	17
Most CFO Act Agencies Established Coding Procedures, but Six Agencies' Procedures Only Partially Addressed Activities Required by OPM	28
Conclusions	34
Recommendations for Executive Action	35
Agency Comments and Our Evaluation	39

Appendix I: Objectives, Scope, and Methodology	45
Appendix II: Comments from the Department of Commerce	48
Appendix III: Comments from the Department of Education	50
Appendix IV: Comments from the Department of Energy	51
Appendix V: Comments from the Department of Homeland Security	53
Appendix VI: Comments from the Department of the Interior	56
Appendix VII: Comments from the Small Business Administration	57
Appendix VIII: Comments from National Aeronautics and Space Administration	58
Appendix IX: Comments from the Nuclear Regulatory Commission	60
Appendix X: Comments from the United States Agency for International Development	61
Appendix XI: Comments from the Social Security Administration	64
Appendix XII: GAO Contact and Staff Acknowledgments	65
Appendix XIII: Accessible Data	66
Agency Comment Letter	66

Tables

Table 1: Office of Personnel Management Cybersecurity Employment Codes for “Securely Provision” Category (aligned with NICE Cybersecurity Workforce Framework, NIST SP 800-181)	12
Table 2: Submission Status of Reports on Cybersecurity Workforce Baseline Assessments by Agencies Covered by the Chief Financial Officers Act, as of March 2018	18
Table 3: Information Reported by 21 Chief Financial Officers (CFO) Act Agencies in Their Cybersecurity Workforce Baseline Assessments	21
Table 4: Extent That Chief Financial Officers Act Agencies with Procedures Have Addressed Activities Required by OPM	

in Their Procedures (Civilian Positions),^a as of March
201831

Figures

Figure 1: National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NIST SP 800-181), Categories and Specialty Areas	7
Figure 2: Specialty Areas and Work Roles Defined in the “Securely Provision” Cybersecurity Workforce Framework Category	8
Figure 3: Timeline of Recent Efforts by OPM, NIST, and Other Agencies to Assess the Cybersecurity Workforce	10
Figure 4: Prior Delays Resulting in Later Implementation of the Provisions of the Federal Cybersecurity Workforce Assessment Act of 2015, as of March 2018	16

Abbreviations

CFO	Chief Financial Officers
CIO	chief information officer
CISO	chief information security officer
DHS	Department of Homeland Security
DOD	Department of Defense
HR	human resources
IT	information technology
NASA	National Aeronautics and Space Administration
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



June 14, 2018

Congressional Committees

The security of federal information systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. However, the federal government faces an ever-evolving array of cyber-based threats to its systems and information. Further, federal systems and networks are inherently at risk because of their complexity, technological diversity, and geographic dispersion, among other reasons.

A key component of the government's ability to mitigate and respond to cyber threats is having a qualified, well-trained cybersecurity workforce. 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 IT systems depends on the knowledge, skills, and abilities of the federal workforce that uses, implements, secures, and maintains these systems. This includes federal 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.

We and other organizations previously have reported that agencies faced challenges in ensuring that they have an effective cybersecurity workforce. In 1997, we designated the security of federal information systems as a government-wide high-risk area and cited the shortage of information security personnel with technical expertise required to manage controls in these systems. In 2001, we added strategic human capital management to our high-risk list.¹ In our 2017 update to the high-risk list, we reported that the federal government continues to be challenged in addressing mission critical skills gaps, including cybersecurity skills gaps.²

¹GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997); and GAO, *High-Risk Series: An Update*, [GAO-01-263](#) (Washington, D.C.: January 2001).

²GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, [GAO-17-317](#) (Washington, D.C.: February 2017).

To address these and other challenges, the Federal Cybersecurity Workforce Assessment Act of 2015 requires the Office of Personnel Management (OPM), the National Institute of Standards and Technology (NIST), and other federal agencies to take several actions related to cybersecurity workforce planning.³ Among other things, the act requires:

- OPM, in coordination with NIST, to develop an employment coding structure⁴ for cybersecurity positions.⁵
- OPM, in coordination with NIST, the Department of Homeland Security (DHS), and the Office of the Director of National Intelligence (ODNI), to establish procedures to implement the coding structure for civilian cybersecurity positions.
- OPM to submit a progress report on the implementation of the act to the appropriate congressional committees.
- Agencies to report on the baseline assessments of their existing cybersecurity workforces and establish procedures for identifying cybersecurity positions and assigning codes to such positions.

The Federal Cybersecurity Workforce Assessment Act of 2015 also includes a provision calling for us to analyze and monitor agencies' implementation of the act's requirements and report on this assessment to Congress no later than December 2018. Our objectives for this first report were to determine whether (1) OPM developed a coding structure and procedures for assigning codes to cybersecurity positions and submitted a progress report to Congress, (2) Chief Financial Officers

³The Federal Cybersecurity Workforce Assessment Act of 2015 was enacted as part of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title III, sec. 303 (Dec. 18, 2015); 129 Stat. 2242, 2975-77.

⁴The act requires the development of an employment coding structure under the National Initiative for Cybersecurity Education (NICE). NIST, which heads NICE, issued the *NICE Cybersecurity Workforce Framework* to describe cybersecurity roles and positions. The employment coding structure identifies unique numeric codes for each of 52 work roles and 33 specialty areas defined in the NICE Framework. The codes are intended to allow OPM and agencies to identify and categorize all federal cybersecurity positions.

⁵The act generally refers to the cybersecurity workforce as those positions requiring the performance of IT, cybersecurity, or other cyber-related job functions. Because the *NICE Cybersecurity Workforce Framework* focuses on cybersecurity work roles, for the purposes of this report, we refer to positions that require the performance of IT, cybersecurity, or other cyber-related functions as cybersecurity positions.

(CFO) Act agencies⁶ submitted complete and reliable baseline assessment reports of their cybersecurity workforces, and (3) CFO Act agencies established procedures to identify and assign codes to cybersecurity positions.

To address the first objective, we examined OPM guidance, memorandums, and reports to assess whether OPM had developed a coding structure and procedures for assigning codes to all federal civilian cybersecurity positions and submitted a progress report to Congress on the implementation of the act. We also interviewed OPM and NIST officials about their efforts to develop these documents and the reasons for any delays.

To address the second objective, we reviewed and compared the contents of the 24 CFO Act agencies' baseline assessment reports to the reporting requirements defined in the act. We also interviewed cognizant officials at the 24 agencies to (1) identify the process by which agencies collected and reported baseline assessment information on the certifications held by their cybersecurity personnel and (2) obtain their views on the reliability of the information reported in their agency's baseline assessment.

To address the third objective, we assessed the completeness of the 24 agencies' procedures for identifying and assigning codes to cybersecurity positions by determining whether the procedures addressed the required coding activities defined in OPM guidance. We also compared the issuance date of the procedures to the deadline established in OPM's coding guidance for agencies to issue the procedures, and interviewed agency officials about their efforts to complete the procedures by the required deadline and the reasons for any delays. A more complete description of our objectives, scope, and methodology is provided in appendix I.

⁶The 24 agencies covered by the Chief Financial Officers Act are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development (31 U.S.C. § 901(b)).

We conducted this performance audit from October 2016 to June 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.

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 IT systems. The ability to secure federal systems depends on the knowledge, skills, and abilities of the federal and contractor workforce that uses, implements, secures, and maintains these systems.

Nevertheless, the Office of Management and Budget (OMB) 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. In addition, the RAND Corporation⁷ and the Partnership for Public Service⁸ have reported that there is a nationwide shortage of cybersecurity experts, in particular, in the federal government. According to these reports, this shortage of cybersecurity professionals makes securing the nation's networks more

⁷RAND Corporation, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (2014).

⁸The Partnership for Public Service and Booz Allen Hamilton, *Cyber-In-security: Strengthening the Federal Cybersecurity Workforce* (July 2009) and *Cyber In-Security II: Closing the Federal Talent Gap* (April 2015).

challenging and may leave federal IT systems vulnerable to malicious attacks. The persistent shortage of cyber-related talent has given rise to efforts to identify and assess the federal cybersecurity workforce.

The National Initiative for Cybersecurity Education (NICE) Created a Framework for Defining Cybersecurity Workforce Positions

NICE, led by NIST, is a partnership among government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals that are helping to keep our nation secure. NICE issued an initial draft of the *National Cybersecurity Workforce Framework* (National Framework) for public comment in September 2011 and the final version 1.0 in April 2013. The National Framework was intended to help identify, describe, and assess all cybersecurity roles within an organization. The National Framework organized cybersecurity job functions into 7 categories and 31 specialty areas:

- **Category:** a high-level grouping of common cybersecurity functions. Categories group together work and workers that share common major functions, regardless of job titles or other occupational terms.
- **Specialty area:** an area of concentrated work, or function, within cybersecurity and related work. Related specialty areas are grouped together into categories. In version 1.0 of the National Framework, each specialty area was also associated with a distinct set of cybersecurity related tasks and knowledges, skills, and abilities.

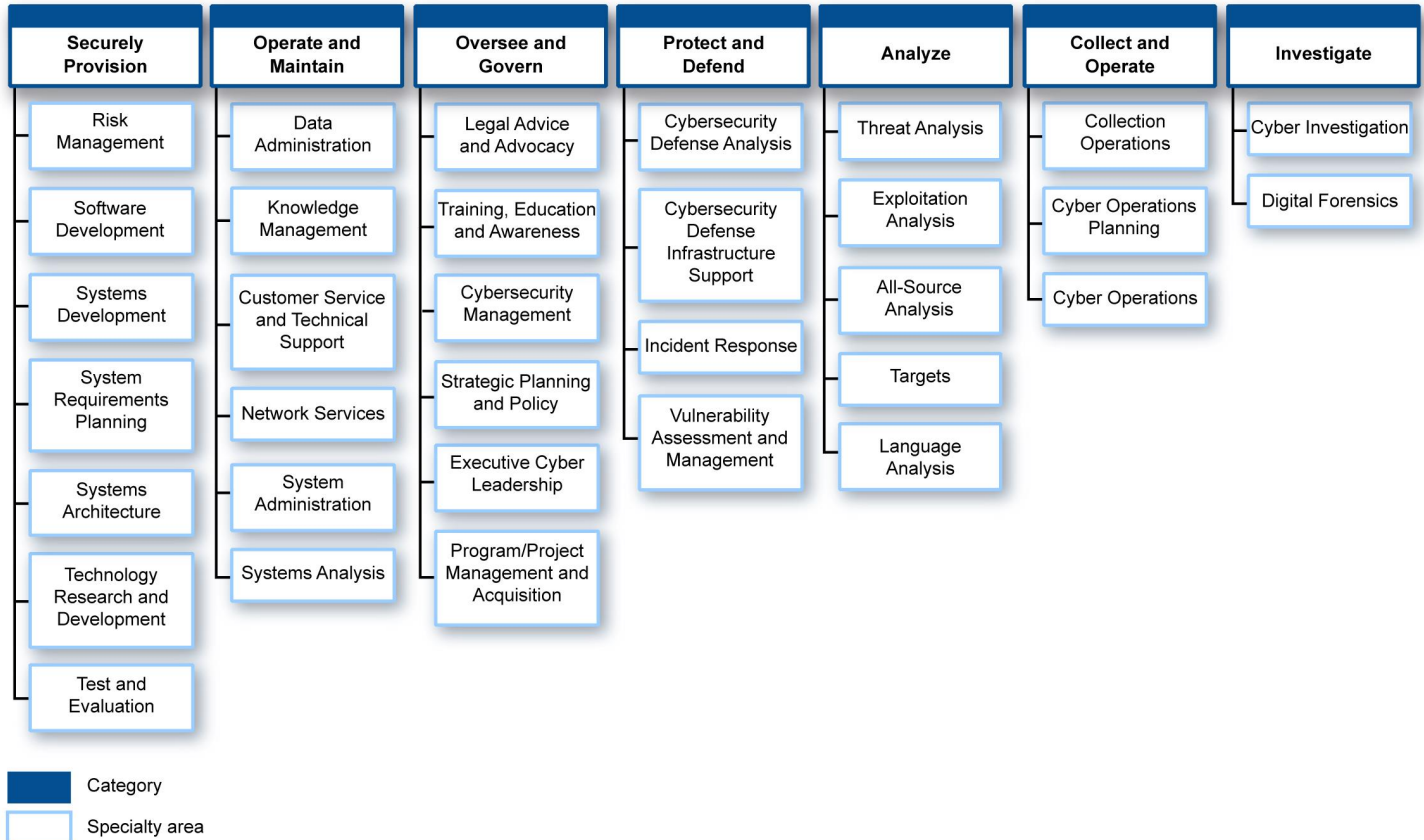
In November 2016, NIST issued draft special publication 800-181 which revised and replaced earlier versions of the National Framework. The draft was co-authored by NIST, DOD, and DHS and was renamed the

NICE Cybersecurity Workforce Framework (NICE Framework). In August 2017, NIST published the final version of the special publication.⁹

The NICE Framework is intended to help the federal government better identify cybersecurity workforce needs by enabling agencies to examine specific cybersecurity work roles, and identify personnel skills gaps, rather than merely examine the number of vacancies by job series. The NICE Framework added 2 additional specialty areas within the 7 categories. Figure 1 identifies the 7 categories and the 33 specialty areas in the NICE Framework.

⁹National Institute of Standards and Technology, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, SP 800-181 (Gaithersburg, Md.: August 2017).

Figure 1: National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NIST SP 800-181), Categories and Specialty Areas



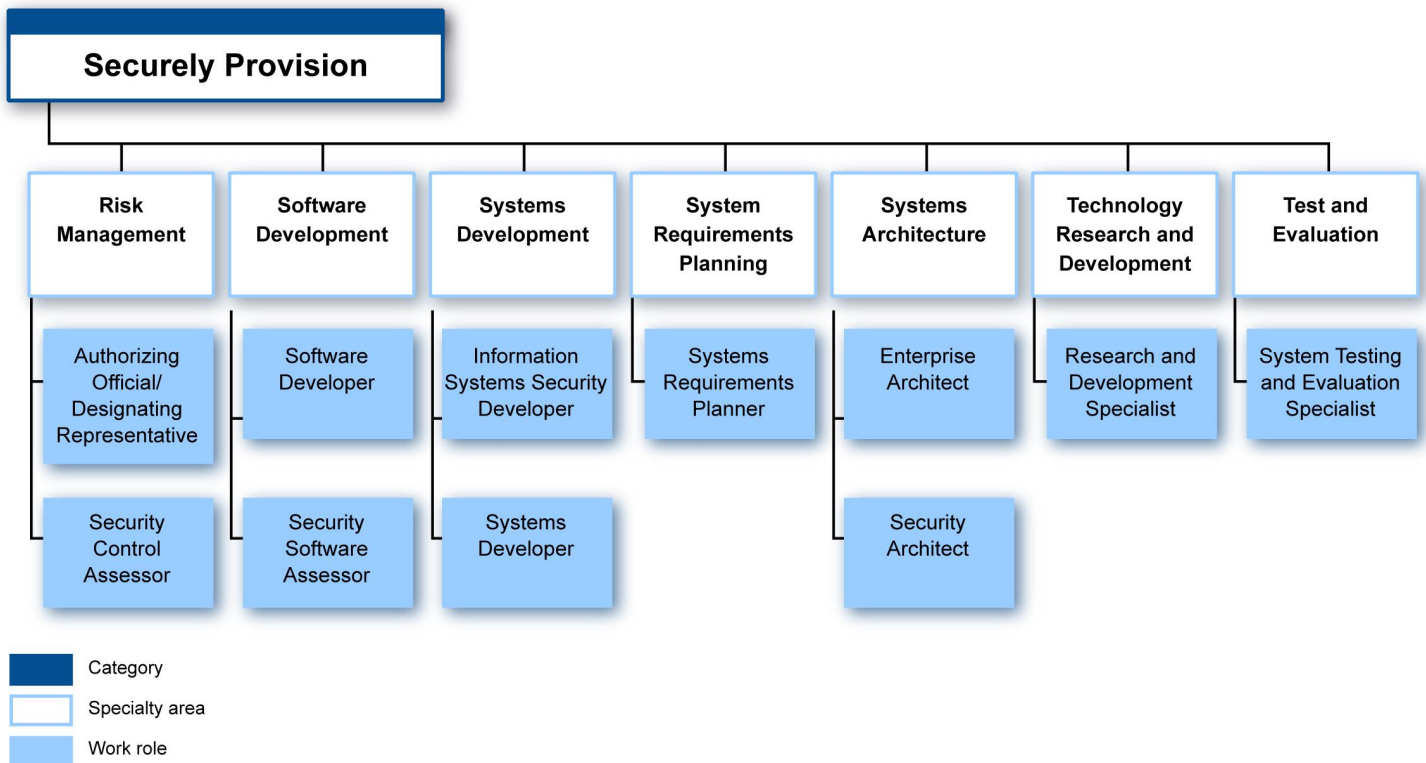
Source: GAO analysis of National Institute of Standards and Technology, *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*, SP-800-181. | GAO-18-466

The NICE Framework also introduced the concept of work roles as the third component of cybersecurity job functions. Work roles provide a more detailed description of the roles and responsibilities of cybersecurity job functions than do the category and specialty area components of the NICE Framework. The NICE Framework defines one or more work roles within each specialty area.¹⁰ For example, as depicted in figure 2, the

¹⁰The NICE Framework defines a total of 52 work roles across the 33 specialty areas.

NICE Framework defined 11 work roles within the 7 specialty areas in the “Securely Provision” category.¹¹

Figure 2: Specialty Areas and Work Roles Defined in the “Securely Provision” Cybersecurity Workforce Framework Category



Source: GAO analysis of National Institute of Standards and Technology, *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*, SP-800-181. | GAO-18-466

¹¹The NICE Framework states that the specialty areas and work roles in the “Securely Provision” category conceptualize, design, procure, and/or build secure information technology systems, with responsibility for aspects of system and/or network development.

OPM Has Led Several Efforts to Assess the Federal Cybersecurity Workforce

In October 2012, in coordination with a NICE interagency working group, OPM published a cybersecurity employment coding structure that aligned with the initial draft version of the *National Cybersecurity Workforce Framework*. The coding structure assigned a unique 2-digit cybersecurity employment code to each category and specialty area in the NICE Framework. According to OPM, the coding of federal positions with cybersecurity functions was intended to enhance agencies' ability to identify critical cybersecurity workforce needs, recruit and hire employees with needed skills, and provide appropriate training and development opportunities to cybersecurity employees.

In July 2013, OPM initiated the Special Cybersecurity Workforce Project to support federal efforts to reduce the cybersecurity workforce skills gaps across agencies.¹² Agencies were to use the definitions of cybersecurity work, as described in the *National Cybersecurity Workforce Framework*, along with OPM's cybersecurity coding structure, to code positions performing cybersecurity work by the end of fiscal year 2014. The project was intended to enable agencies to identify and address their needs for cybersecurity skill sets to meet their missions.

In July 2016, OPM and the Office of Management and Budget (OMB) issued the Federal Cybersecurity Workforce Strategy.¹³ The strategy details government-wide actions to identify, expand, recruit, develop, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats. The strategy identifies a number of actions intended to address cybersecurity workforce challenges in: (1) identifying cybersecurity workforce needs, (2) expanding the cybersecurity workforce through education and training, (3) recruiting and hiring highly skilled talent, and (4) retaining and developing highly skilled talent.

The strategy states that OPM is to expand cybersecurity position coding and agencies are to conduct strategic workforce planning. These actions

¹²Office of Personnel Management, *Memorandum for Heads of Executive Departments and Agencies: Special Cybersecurity Workforce Project* (Washington, D.C.: July 8, 2013).

¹³Office of Management and Budget and Office of Personnel Management, *Federal Cybersecurity Workforce Strategy*, M-16-15 (Washington, D.C.: July 12, 2016).

are related to the requirements of the Federal Cybersecurity Workforce Assessment Act of 2015, under which OPM is to establish an employment coding structure and agencies are to identify and report on cybersecurity workforce critical needs.

Figure 3 depicts a timeline of recent efforts to assess the federal cybersecurity workforce.

Figure 3: Timeline of Recent Efforts by OPM, NIST, and Other Agencies to Assess the Cybersecurity Workforce

Efforts to assess the federal cybersecurity workforce

2011

September National Institute of Standards and Technology (NIST) posted draft *National Cybersecurity Workforce Framework* for public comment

2013

April NIST issued *National Cybersecurity Workforce Framework, Version 1.0*
July 8 OPM initiated Special Cybersecurity Workforce Project

2015

December 18 Federal Cybersecurity Workforce Assessment Act of 2015 enacted

2012

October 1 The Office of Personnel Management (OPM) published the new cybersecurity employment coding structure

2014

May NIST released draft *National Cybersecurity Workforce Framework, Version 2.0*
September 30 Special Cybersecurity Workforce Project deadline for federal agencies to assign 2-digit code to 90% of 2210 job series as well as other cyber-related positions

2016

July 12 OPM and Office of Management and Budget issued *Federal Cybersecurity Workforce Strategy* (OMB M-16-15)

Source: GAO analysis of federal laws and OPM, NIST, and OMB documentation. | GAO-18-466

OPM Issued a Cybersecurity Position Coding Structure, Procedures, and Progress Report Later Than the Deadlines Established in the Act

As required by the Federal Cybersecurity Workforce Assessment Act of 2015, OPM developed a cybersecurity coding structure under NICE, issued guidance to implement the coding structure to identify all federal civilian cybersecurity positions, and provided a progress report to Congress on the implementation of the act. However, the coding structure and procedures were issued later than the act's deadlines because OPM was working with the National Institute of Standards and Technology (NIST) to align the structure and procedures with the draft version of the *NICE Cybersecurity Workforce Framework*, which NIST issued later than planned. The delays in issuing the coding structure and procedures have extended the expected time frames for implementing subsequent provisions of the act.

OPM Developed a 3-digit Cybersecurity Coding Structure

The Federal Cybersecurity Workforce Assessment Act of 2015 (the act) required OPM, in coordination with NIST, to develop a cybersecurity coding structure by June 15, 2016.

OPM addressed this requirement by developing a 3-digit cybersecurity employment coding structure that fully aligns with the *NICE Cybersecurity Workforce Framework*.¹⁴ OPM issued version 1 of the coding structure on November 15, 2016, 5 months after the deadline established in the act.¹⁵

The coding structure assigns a unique 3-digit cybersecurity employment code to each work role outlined in the draft version of the *NICE Cybersecurity Workforce Framework*. Table 1 presents an example of the 3-digit employment codes associated with one category—"Securely Provision"—and its component specialty areas and work roles.

¹⁴Office of Personnel Management, *Memorandum for Human Resources Directors: Requirements of the Federal Cybersecurity Workforce Assessment Act* (Washington, D.C.: August 1, 2016).

¹⁵Office of Personnel Management, *Federal Cybersecurity Coding Structure Version 1.0* (November 15, 2016). Version 2 of the revised coding structure was issued on October 18, 2017.

Table 1: Office of Personnel Management Cybersecurity Employment Codes for “Securely Provision” Category (aligned with NICE Cybersecurity Workforce Framework, NIST SP 800-181)

Category	Specialty Area	Work Role	Employment Code
Securely Provision	Risk Management	Authorizing Official/Designating Representative	611
		Security Control Assessor	612
	Software Development	Software Developer	621
		Secure Software Assessor	622
	Systems Development	Information Systems Security Developer	631
		Systems Developer	632
	Systems Requirements Planning	Systems Requirements Planner	641
	Systems Architecture	Enterprise Architect	651
		Security Architect	652
	Technology Research and Development	Research & Development Specialist	661
	Test and Evaluation	System Testing and Evaluation Specialist	671

Source: GAO analysis of Office of Personnel Management, *Federal Cybersecurity Coding Structure Version 1.0* (Washington, DC: November 15, 2016). | GAO-18-466

Although the act had called for the coding structure to be established by June 15, 2016, OPM officials explained that the coding structure was issued 5 months later than the established deadline because the structure was to be aligned with the *NICE Cybersecurity Workforce Framework*. However, the draft version of the NICE Framework was not issued until November 2, 2016.¹⁶

According to NIST officials, the issuance of the draft NICE Framework was delayed because some of the knowledge, skills, and abilities (KSA) and task statements¹⁷ that had been originally developed by the intelligence community were marked as sensitive. NIST delayed publication of the draft NICE Framework until officials in the intelligence community had removed any sensitivity designations on the KSAs and task statements.

¹⁶National Institute of Standards and Technology, *(Draft) NICE Cybersecurity Workforce Framework*, Draft SP 800-181 (Gaithersburg, Md.: November 2, 2016).

¹⁷Knowledge, skills, and abilities—commonly known as KSAs—are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training. A task is a specific define piece of work that, combined with other identified tasks, composes the work in a specific specialty area or work role.

OPM Developed Government-wide Procedures for Assigning Codes to Civilian Cybersecurity Positions

The act required OPM, in coordination with NIST, DHS, and ODNI to establish procedures to assist agencies in implementing the cybersecurity coding structure. OPM was to develop the procedures no later than September 18, 2016.

In accordance with this requirement, OPM coordinated with NIST, DHS, and ODNI to develop its *Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions*.¹⁸ The guidance provides instructions on how agencies are to assign the 3-digit cybersecurity employment codes to filled and vacant positions, including required activities for identifying and assigning codes to cybersecurity positions. The guidance also referenced additional updates and guidance that were to be posted on OMB's MAX website.¹⁹

OPM posted the guidance on the Chief Human Capital Officers Council website on January 4, 2017, 4 months after the deadline established in the act. OPM officials said they delayed issuance of the guidance so that it could be released in coordination with the cybersecurity coding structure, which was dependent on the release of the draft NICE Framework.

OPM Submitted a Progress Report to Congress

The act required OPM to report on the progress of agencies' implementation of the act's requirements, as well as OPM's efforts to develop a coding structure and government-wide coding procedures.

¹⁸Office of Personnel Management, *Memorandum for Heads of Executive Departments and Agencies: Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions* (Washington, D.C.: January 4, 2017).

¹⁹OMB uses the MAX Information System to collect, validate, analyze, model, collaborate with agencies on, and publish information relating to its government-wide management and budgeting activities.

OPM was to submit the progress report to the appropriate congressional committees no later than June 15, 2016.²⁰

OPM prepared and submitted its progress report to the congressional committees identified in the act on July 12, 2016, about 1 month after the act's deadline. Among other things, the report stated the following:

- OPM was coordinating closely with NICE to revise the cybersecurity coding structure to align with the latest version of the NICE Framework, which was scheduled to be finalized in September 2016.
- OPM had begun an education campaign to inform the federal community of the act and its requirements and was collaborating with stakeholders and interagency partners on ideas for how to implement the requirements of the act.

An official in OPM's Employee Services division stated that OPM was delayed in completing and submitting the report to congressional committees due to the agency's internal review process.

OPM's Delays in Completing Required Activities Have Resulted in Later Implementation of Other Provisions of the Act

Because the deadlines for agencies to implement certain provisions of the act are contingent on the completion of earlier activities, delays by OPM in issuing the revised cybersecurity coding structure and the government-wide coding procedures have extended the due dates for agencies to implement other provisions of the act by about 4 months. Specifically:

- The act required agencies to establish procedures for identifying all IT or cybersecurity positions and for assigning the appropriate employment code to each position no later than 3 months after OPM issued the government-wide coding procedures. If OPM had issued the coding procedures by September 2016 as the act required, agencies would have been required to establish their coding

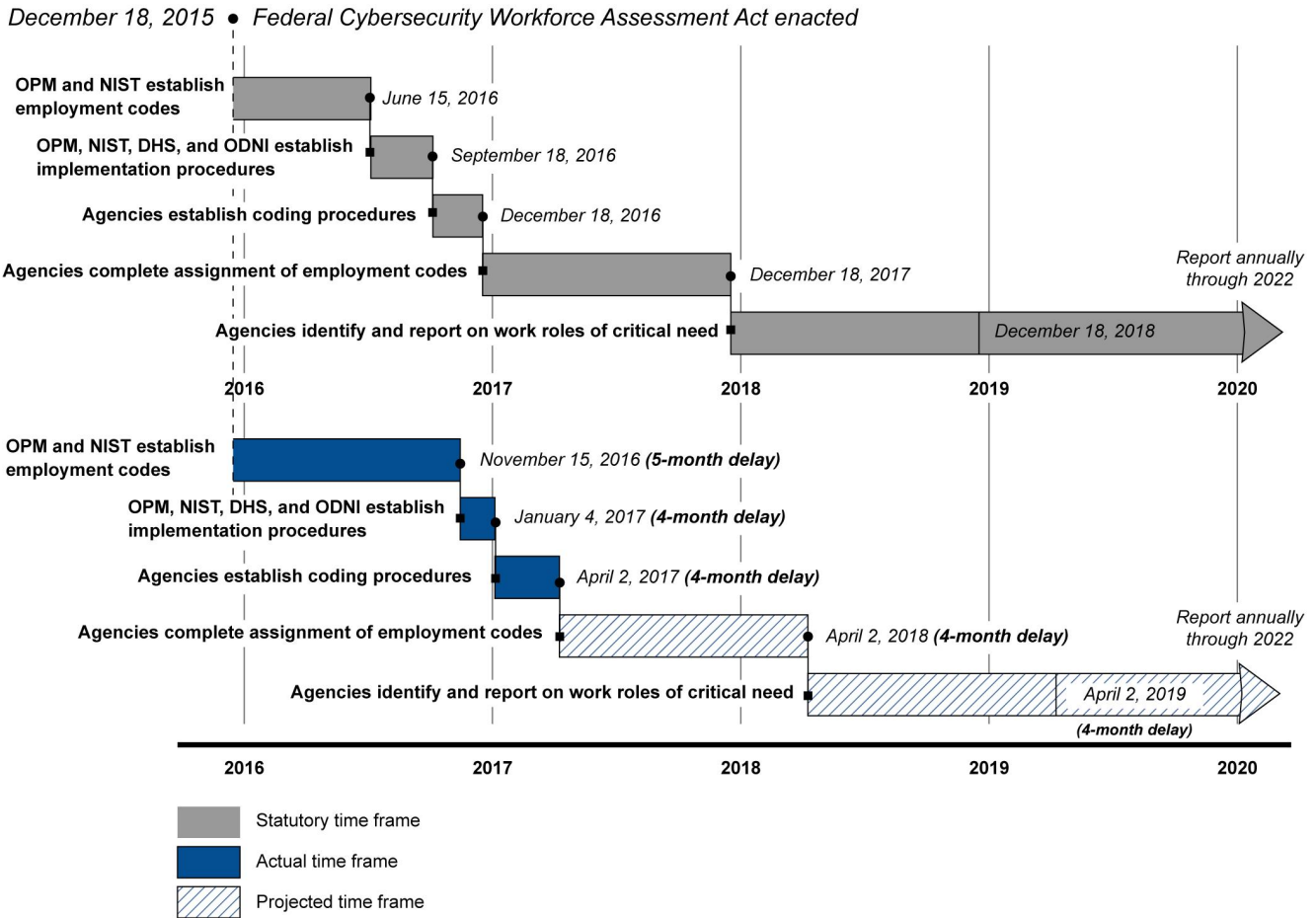
²⁰The Federal Cybersecurity Workforce Assessment Act defined appropriate congressional committees to mean: the House committees on Armed Services, Homeland Security, Oversight and Government Reform, and Intelligence; and the Senate committees on Armed Services, Homeland Security and Governmental Affairs, Commerce, Science, and Transportation, and Intelligence.

procedures by December 2016. However, because OPM did not issue the government-wide procedures until January 2017, agencies did not have to develop their coding procedures until April 2017.

- Similarly, agencies were to assign employment codes to all of their cybersecurity positions no later than 1 year after establishing their coding procedures. Had agencies been required to establish their procedures by December 2016, they would have been required to assign the employment codes by December 2017. However, because they did not have to develop coding procedures until April 2017, they were therefore required to complete the assignment of employment codes by April 2018.
- Further, agencies are required to identify and report on cybersecurity work roles of critical need beginning 1 year after the employment codes are assigned. If agencies had been required to assign employment codes by December 2017, they would have to begin reporting on their critical needs by December 2018. However, because they did not have to complete the assignment of employment codes until April 2018, they are therefore required to identify and begin reporting on critical needs by April 2019.

Figure 4 depicts the delays in earlier activities which can result or have resulted in later implementation of subsequent provisions of the act.

Figure 4: Prior Delays Resulting in Later Implementation of the Provisions of the Federal Cybersecurity Workforce Assessment Act of 2015, as of March 2018



Source: GAO analysis of NIST and OPM information and of the Federal Cybersecurity Workforce Assessment Act of 2015. | GAO-18-466

Note: NIST = National Institute of Standards and Technology; OPM = Office of Personnel Management; DHS = Department of Homeland Security; ODNI = Office of the Director of National Intelligence.

Most CFO Act Agencies Submitted Baseline Assessments, but the Results May Not Be Reliable

Most of the 24 CFO Act agencies conducted baseline assessments identifying the extent to which their cybersecurity employees held certifications and submitted them to Congress as required by the act. However, 3 agencies did not complete the assessments for various reasons, such as a lack of resources and tools to do so. Further, of the 21 agencies that did complete the assessments, 4 agencies did not address all of the reportable information, such as the extent to which personnel without certifications were ready to obtain them or strategies for mitigating any gaps. In addition, the assessments conducted by the 21 agencies did not contain complete, comprehensive, or consistent information on the certifications held by agencies' cybersecurity employees due to limitations in the ability of the agencies to collect the needed information. As a result, the information collected and reported by most agencies about the certifications held by agency cybersecurity personnel may be of limited value for assessing the credentials and qualifications of their cybersecurity workforces.

Most CFO Agencies Conducted Baseline Assessments but Several Agencies Did Not Include All Reportable Information

The Federal Cybersecurity Workforce Assessment Act of 2015 required agencies to prepare baseline assessment reports identifying the extent to which their cybersecurity workforces held industry-recognized certifications as identified under NICE.²¹ OPM's August 2016 memorandum on the requirements and time frames of the act further stated that agencies were to report the results of the assessments to the appropriate congressional committees of jurisdiction by December 2016.²²

²¹Because NICE did not define a list of appropriate industry-recognized certifications, we evaluated only whether agencies identified personnel that held certifications.

²²Office of Personnel Management, *Memorandum for Human Resources Directors: Requirements of the Federal Cybersecurity Workforce Assessment Act* (Washington, D.C.: August 1, 2016).

In the absence of a NICE-defined list of appropriate industry-recognized certifications, 21 of the 24 agencies covered by the CFO Act had conducted baseline assessments of the certifications held by their cybersecurity workforces and submitted the baseline assessment reports to Congress as of March 2018.²³ Table 2 shows the status of the agencies' submissions of the baseline assessments as of March 2018.

Table 2: Submission Status of Reports on Cybersecurity Workforce Baseline Assessments by Agencies Covered by the Chief Financial Officers Act, as of March 2018

Agency	Submitted report to Congress
Department of Agriculture	checked
Department of Commerce	checked
Department of Defense	checked
Department of Education	checked
Department of Energy	checked
Department of Health and Human Services	checked
Department of Homeland Security	
Department of Housing and Urban Development	
Department of the Interior	checked
Department of Justice	checked
Department of Labor	checked
Department of State	checked
Department of Transportation	checked
Department of the Treasury	checked
Department of Veterans Affairs	checked
Environmental Protection Agency	checked
General Services Administration	checked
National Aeronautics and Space Administration	checked
National Science Foundation	checked
Nuclear Regulatory Commission	checked

²³The act required the baseline assessment to be submitted to the appropriate congressional committees of jurisdiction. Eight committees were identified as appropriate congressional committees, but the appropriate committees "of jurisdiction" were not specified. Fourteen agencies submitted the baseline assessment to the eight committees we previously mentioned. Two agencies submitted the assessment to their congressional committees of jurisdiction, but not to all of the committees listed in the act. Of the 21 assessments that were submitted to Congress, 6 were submitted by December 2016, 7 were submitted in January 2017, and 8 were submitted by January 2018.

Agency	Submitted report to Congress
Office of Personnel Management	checked
Small Business Administration	checked
Social Security Administration	checked
U.S. Agency for International Development	checked
Total	21

Legend: checked = agency submitted assessment report to Congress

Source: GAO analysis of the 24 Chief Financial Officers Act agencies' reports. | GAO-18-466

Three agencies did not conduct baseline assessments:

- Instead of conducting a baseline assessment as called for by the act, DHS submitted its 2016 *Comprehensive Cybersecurity Workforce Update*²⁴ to Congress in March 2017. However, this report did not include a baseline assessment of the department's workforce as called for by the act. The report noted that DHS's Office of the Chief Human Capital Officer lacked the ability to view or easily produce consolidated reports on employee certifications from all DHS components, and lacked consistent and detailed information about the readiness of additional employees to complete certification exams and specific certifications identified by components as being required for success in their positions. The report further noted that the department was working with cybersecurity subject matter experts from each component to revalidate the certifications most important to the work of their organizations and to organize the information according to the NICE Framework.
- The Department of Housing and Urban Development (HUD) prepared an assessment of IT specialist skills, but did not conduct a baseline assessment that identified the extent to which its cybersecurity workforce held industry-recognized certifications. Officials in HUD's Office of the Chief Information Officer (CIO) and Office of the Chief Human Capital Officer stated that the department intends to conduct a workforce assessment of its cybersecurity employees. The officials

²⁴DHS compiled this report in response to the Homeland Security Cybersecurity Workforce Assessment Act of 2014 (Pub. L. No. 113-277, sec. 4, Dec. 18, 2014); the Cybersecurity Workforce Assessment Act (Pub. L. No. 113-246, Dec. 18, 2014); and the Federal Cybersecurity Workforce Assessment Act of 2015. The report provided information on the Department's cybersecurity workforce planning program to date, the Department's efforts to code cybersecurity positions, an overview of the current cybersecurity workforce, and the readiness the cybersecurity workforce to meet mission requirements.

did not provide a time frame for when the assessment would be conducted.

- The CIO and Chief Human Capital Officer of the Small Business Administration (SBA) stated that the agency has been unable to complete a baseline assessment due to resource constraints. The officials added that the agency intends to conduct workforce planning efforts in the future. However, they did not provide a time frame for when the assessment would be conducted.

By not conducting baseline assessments, DHS, HUD, and SBA lack valuable information about the knowledge and skills of their cybersecurity employees. This lack of information limits the agencies' ability to effectively gauge the competency of individuals who are charged with ensuring the confidentiality, integrity, and availability of federal information and information systems. Additionally, by not conducting or reporting on the assessment, the agencies have not provided Congress the information it required in the act regarding existing credentials and certifications of personnel with information technology, cybersecurity, or other cyber-related job functions.

Not All Agencies That Prepared Baseline Assessment Reports Addressed Reportable Information

The act required agencies' baseline assessment reports to identify the following:

- the percentage of personnel with cybersecurity job functions who held the appropriate industry-recognized certifications as identified under NICE;²⁵
- the level of preparedness of cybersecurity personnel without existing credentials to take certification exams; and
- a strategy for mitigating any gaps in (1) personnel holding industry-recognized certifications and (2) the preparedness of personnel without existing credentials to take certification exams.

²⁵Certification is a voluntary process by which individuals are assessed (usually by application or exam) against pre-determined standards for knowledge, skills, and competency required to perform in a profession, occupation, or role, and granted a time-limited credential. It is typically awarded by a third-party, standard-setting organization.

In September 2016, OPM provided a template that agencies could use in reporting on their baseline assessments. Using the template, agencies could report on the number and percentage of surveyed staff with current certifications and the number and percentage of staff without such certifications that were planning to obtain them within the next year. Human resource strategists and program management officials in OPM’s Employee Services division stated that the template was a guide to help agencies with the reporting process; however, agencies were not required to use the template or report their results in the format described in the template.

The 21 CFO agencies that prepared baseline assessment reports did not always address the reportable information in their baseline assessments. Specifically, of the 21 assessments that the CFO agencies had prepared, all of the assessments included information on the percentage of cybersecurity personnel holding certifications; 17 assessments discussed the level of preparedness for personnel without certifications to take certification exams; and 20 included strategies for mitigating certification gaps. Table 3 shows the extent to which the 21 agencies’ assessments reported this information.

Table 3: Information Reported by 21 Chief Financial Officers (CFO) Act Agencies in Their Cybersecurity Workforce Baseline Assessments

Agency	Percentage of cybersecurity personnel holding certifications ^a	Level of preparedness of personnel without existing credentials to take certification exams	Strategies for mitigating any gaps identified
Department of Agriculture	checked	checked	checked
Department of Commerce	checked		
Department of Defense	checked	checked	checked
Department of Education	checked	checked	checked
Department of Energy	checked		checked
Department of Health and Human Services	checked	checked	checked
Department of the Interior	checked		checked
Department of Justice	checked	checked	checked
Department of Labor	checked	checked	checked
Department of State	checked	checked	checked
Department of Transportation	checked	checked	checked
Department of the Treasury	checked	checked	checked
Department of Veterans Affairs	checked	checked	checked

Agency	Percentage of cybersecurity personnel holding certifications ^a	Level of preparedness of personnel without existing credentials to take certification exams	Strategies for mitigating any gaps identified
Environmental Protection Agency	checked	checked	checked
General Services Administration	checked	checked	checked
National Aeronautics and Space Administration	checked		checked
National Science Foundation	checked	checked	checked
Nuclear Regulatory Commission	checked	checked	checked
Office of Personnel Management	checked	checked	checked
Social Security Administration	checked	checked	checked
U.S. Agency for International Development	checked	checked	checked
Total addressed	21	17	20
Total not addressed	0	4	1

Legend: checked = reportable information addressed in assessment report

Source: GAO analysis of the baseline assessment reports prepared by 21 Chief Financial Officers Act agencies. | GAO-18-466

^aBecause NICE did not define a list of appropriate industry-recognized certifications, we evaluated only whether agencies identified personnel that held certifications.

Note: This table does not include three CFO Act agencies—the Departments of Homeland Security and Housing and Urban Development and the Small Business Administration—because they had not conducted baseline assessments as of March 2018.

Moreover, 4 of the 21 agencies did not address all reportable information in their baseline assessments. Specifically:

- The Department of Commerce did not assess and did not report information on (1) the level of preparedness for personnel who did not hold certifications to take certification exams or (2) strategies for mitigating gaps. Officials in Commerce’s Office of Human Resources Management and Office of the CIO stated that information on the level of preparedness and gaps was not readily available because they have not fully identified and coded the department’s cybersecurity workforce, and there is no federal requirement for cybersecurity personnel to hold certifications. The officials stated that they did not have the time or resources to assess these reporting requirements.
- Officials in the Department of Energy’s Office of the Chief Human Capital Officer stated that they did not assess the level of preparedness for personnel without certifications to take certification exams because the department does not require its cybersecurity personnel to hold certifications. As a result, they did not have criteria for identifying personnel who are prepared to take certification exams.

- According to the Department of the Interior's Principal Deputy Assistant Secretary for Policy, Management, and Budget, the department did not assess the level of preparedness for personnel without certifications to take certification exams because neither OPM nor the department currently requires certifications for these cybersecurity positions. However, the department's Office of Human Resources and Office of the Chief Information Officer are exploring options to determine the level of preparedness across its IT workforce.
- According to the National Aeronautics and Space Administration's (NASA) baseline assessment report, the agency did not assess the level of preparedness for personnel without certifications to take certification exams because the agency does not require its cybersecurity personnel to maintain certifications. The agency did not know how many of its personnel were planning to seek certifications on their own.

Data regarding the number of cybersecurity employees that hold certifications and the level of preparedness of personnel without certifications can be a useful indicator of the skills and knowledge of an agency's cybersecurity workforce. In addition, strategies for addressing gaps can help an agency increase the skills and knowledge of its cybersecurity workforce. By not including all reportable information in the assessments, these four agencies may lack valuable information that could help them identify and meet the certification and training needs of their cybersecurity employees who are charged with protecting federal information and information systems from cyberattacks. However, as discussed later in this report, the absence of NICE identified appropriate industry-recognized certifications may have also contributed to uncertainty for agencies in their efforts to comply with the requirements of the act.

Limitations in Agency Baseline Assessments Raise Concerns About the Reliability of Information about Certifications Held by Agencies' Cybersecurity Employees

Limitations in the 21 agencies' baseline assessments raise concerns about the reliability of the assessments, thus constraining the conclusions that can be drawn from their results about the federal cybersecurity workforce's certifications. The 21 agencies in our review that conducted assessments were not able to collect complete, comprehensive, or consistent information about the certifications held by their cybersecurity workforces for various reasons. As a result, these agencies had limited assurance that the certification information contained in their baseline assessment reports was reliable, thereby diminishing the usefulness of the assessments in determining the certification and training needs of their cybersecurity employees.

Agencies Were Required to Assess Cyber Employees' Certifications before They Had Fully Defined Their Cybersecurity Workforces

As previously noted, OPM's August 2016 memorandum on the requirements of the act stated that, agencies were to report their baseline assessments to Congress by December 2016. However, according to OPM's January 2017 coding guidance, agencies were not required to complete the assignment of the appropriate 3-digit employment codes to each position until April 2018. Consequently, agencies were required to submit their reports on the percentage of personnel performing cybersecurity functions who possessed certifications before the agencies had identified all members of their cybersecurity workforce and assigned the 3-digit cybersecurity employment codes to each position.

Because the agencies had not yet fully defined their cybersecurity workforces using the NICE Framework and the 3-digit coding structure, the 21 agencies in our review that prepared assessments did not use consistent criteria to define the population of personnel with cybersecurity job functions that were included in their baseline assessments. Examples of the criteria that these agencies used to define the target populations for their assessments included:

- cybersecurity employees who had been coded with the 2-digit cybersecurity employment codes during the 2013 Special Cybersecurity Workforce Project;

-
- employees within certain occupational series, such as the 2210 Information Technology Management series;²⁶
 - personnel within certain roles or organizations, such as the Office of Information Security or the Office of the CIO; or
 - personnel who performed cybersecurity duties for a defined percentage of the time.²⁷

As a result of not having fully defined their cybersecurity workforces prior to conducting their baseline assessments, the agencies have limited assurance that their baseline assessments reflected all relevant agency positions or personnel performing cybersecurity functions as defined by the NICE Framework.

Agencies Were Not Always Able to Obtain Certification Information from All Relevant Employees

Several agencies reported that they were not able to obtain information on certifications from all of the employees they surveyed when conducting their baseline assessments. Specifically, 6 of the 21 agencies that prepared assessments reported response rates of between 15 and 42 percent to their surveys or data calls to employees for such information.²⁸ Also, officials from two agencies told us that employees' responses to their information requests were voluntary due to union and legal concerns. As a result, these agencies have limited assurance that their baseline assessment reports conveyed comprehensive information about all agency cybersecurity personnel and the certifications that they held because of the limited response from employees.

²⁶An occupational series is used to identify a specific occupation and generally includes all jobs in that particular kind of work at all grade levels. Many agencies use the occupational series developed by the Office of Personnel Management.

²⁷The percentage of time required for an individual to be counted as a cybersecurity employee varied among agencies and was typically between 20 percent and 30 percent.

²⁸The response rate was not required to be included in the assessment report, but these six agencies chose to include this information. The other 15 agencies in our review that prepared baseline assessments did not report response rates.

NICE Had Not Defined Appropriate Industry-Recognized Certifications

Although the act required agencies to report on the percentage of personnel who held appropriate industry-recognized certifications as identified under NICE, NICE had not defined such a list of certifications as of the agencies' reporting deadline of December 2016. In August 2017, a NICE official told us that the organization did not believe it was appropriate for NICE, which is led by NIST, to identify industry appropriate certifications because doing so may be perceived as endorsing certain private certifications over other certifications. Currently, the NICE website describes an effort under a NICE working group—which includes representatives from government, academia, and the private sector—to map industry-recognized certifications to work roles based on the updated NICE Framework. However, this effort has not yet been completed. According to NICE officials, the mapping of certifications to the NICE Framework is expected to be completed by November 2018.

In the absence of a defined list of industry-recognized certifications, the agencies in our review developed their own approaches for determining the certifications on which they based their assessments. Examples of agencies' approaches included:

- asking that cybersecurity staff provide input on any or all certifications that they held;
- using a list of certifications developed by the DHS National Initiative for Cybersecurity Careers and Studies, which was referenced in OPM's reporting template;²⁹
- using certifications identified in the Department of Defense's (DOD) Information Assurance Workforce Improvement Program,³⁰ or

²⁹DHS, in partnership with several other agencies, launched the National Initiative for Cybersecurity Careers and Studies (NICCS) in February 2013 as an online resource to connect government employees, students, educators, and industry with cybersecurity training providers across the nation. NICCS provides a catalog of cybersecurity-focused training courses that are delivered by accredited colleges and universities, National Security Agency/DHS National Centers of Academic Excellence, federal agencies, and other training providers. NICCS compiled a list of well-known industry cybersecurity certifications online at <https://niccs.us-cert.gov/featured-stories/cybersecurity-certifications>.

- having the agency Office of the CIO or cybersecurity workforce-planning workgroup identify certifications to include in the assessment.

Because the baseline assessments were not based on a defined list of certifications, there is limited assurance that the assessments consistently or accurately conveyed the extent to which federal cybersecurity professionals held industry-recognized certifications that are appropriate for their job functions.

Most Agencies Did Not Require Cybersecurity Personnel to Hold Certifications

In addition, no government-wide requirement exists for cybersecurity personnel to hold certifications, and most of the agencies in our review did not require certifications. Specifically:

- Although OPM guidance states that agencies may use certifications as a selective factor for some positions where specific qualifications are required, no government-wide requirement exists for positions performing cybersecurity related functions to hold certifications.
- Most agencies did not require IT or cybersecurity personnel to hold certifications. Only 6 of the 24 agencies³¹ reported that they had requirements for personnel to hold an industry-recognized certification, while only one agency—DOD—required certifications for all cybersecurity positions.

As a result, the information collected by most agencies about the certifications held by agency cybersecurity personnel may be of limited value for assessing the qualifications and skills of their cybersecurity workforces.

³⁰DOD Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, *DOD 8570.01-M Information Assurance Workforce Improvement Program Incorporating Change 4 11/10/2015*. The Information Assurance Workforce Improvement Program requires individuals that are part of the DOD cybersecurity workforce to obtain the appropriate baseline certification within six months of entry on duty into certain designated cybersecurity positions. The list of approved industry-recognized certifications is maintained online at <http://iase.disa.mil/iawip/Pages/iabaseline.aspx>.

³¹The Departments of Commerce, Defense, Energy, and the Interior; the General Services Administration; and the Small Business Administration.

Most CFO Act Agencies Established Coding Procedures, but Six Agencies' Procedures Only Partially Addressed Activities Required by OPM

Almost all of the CFO Act agencies established procedures to identify all of their civilian positions and assign the appropriate cybersecurity employment codes to the positions as called for by the act. However, 6 agencies' procedures did not fully address 1 or more of 7 activities required by OPM, such as the activities to review all encumbered and vacant positions and annotate reviewed position descriptions with the appropriate employment code. Additionally, DOD did not establish procedures for coding noncivilian cybersecurity positions. By not developing coding procedures that address all of the required activities in their procedures, these agencies may not have reasonable assurance that they will fully realize the benefits of (1) comprehensively identifying the cybersecurity workforce, and (2) applying the employment codes to meet the intended goal of defining the workforce and helping to address critical mission needs.

Most Agencies Established Coding Procedures as Required by the Act

The act required agencies to establish procedures for identifying cybersecurity positions and assigning employment codes to each position. In January 2017, OPM issued a memorandum³² that required agencies to establish their coding procedures by April 2017. The memorandum also required agencies to perform a number of activities to identify and assign codes to cybersecurity positions.³³ Among others, the memorandum stated that agencies were to:

- use the updated cybersecurity coding structure to find the appropriate cybersecurity employment code(s);
- identify encumbered and vacant positions with cybersecurity functions;
- have their CIO staff, managers, and human resources (HR) and classification staff work together to identify cybersecurity positions;
- annotate reviewed position descriptions with the appropriate employment code(s);
- account for the fact that cybersecurity positions will extend beyond the Information Technology Management 2210 (GS-2210) occupational series;
- assign code “000” to positions that do not perform cybersecurity functions; and
- assign up to three employment codes to each position, in the order of the level of criticality.

Most of the agencies in our review had established coding procedures. Specifically, of the 24 CFO Act agencies, 23 had established procedures.

³²Office of Personnel Management, *Memorandum for Heads of Executive Departments and Agencies: Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions* (Washington, D.C.: January 4, 2017).

³³While OPM’s coding guidance required agencies to implement the activities, agencies were not required to address each activity in their coding procedures. Nevertheless, the guidance stated that agencies should use the coding guidance as a resource in establishing agency coding procedures, and officials in OPM’s Employee Services division stated that including instructions for carrying out each of the required activities in agency coding procedures is a good practice.

Fourteen of these 23 agencies established their procedures by April 2017 as OPM required, while the remaining 9 agencies³⁴ established their procedures by March 2018.

Officials from the 9 agencies that did not complete their procedures by April 2017 gave several reasons for their late development or completion of the procedures. For example:

- General Services Administration officials said that the procedures were delayed due to their internal review processes.
- DOD officials said that the procedures were delayed because of the size and complexity of the processes required to identify and code the large number of civilian cybersecurity positions across the department, and because of the length and complexity of the department's policy review processes.
- In October 2017, an official in DHS's Office of the Chief Human Capital Officer stated that the department did not plan to develop procedures until the National Finance Center (NFC)³⁵ payroll systems were updated to accept the 3-digit cybersecurity codes. The NFC systems were updated to accept the new codes in December 2017, and DHS issued its procedures in March 2018.

One agency—the Department of Energy—had not established coding procedures:

- An official in the Department of Energy's Office of the Chief Human Capital Officer stated that, because responsibility for IT is not centralized under the department-level CIO organization (but rather, is distributed throughout the component agencies), the official had not determined who had the authority to issue coding procedures for the entire department. By not establishing coding procedures, the Department of Energy faces increased risk that it will not fully identify its cybersecurity workforce or assign the appropriate employment codes to each position, limiting its ability to identify cybersecurity skills gaps or work roles of critical need.

³⁴The Departments of Defense, Education, Homeland Security, Justice, and Transportation; the General Services Administration; the National Science Foundation; the Nuclear Regulatory Commission; and the U.S. Agency for International Development.

³⁵The National Finance Center is one of the primary payroll service centers used by federal agencies to process employee pay.

Agency Procedures Did Not Always Address Required Coding Activities

The agencies that developed coding procedures generally, but did not always, address the seven required activities that we reviewed in their procedures. Specifically, 17 of the 23 agencies that developed procedures addressed all 7 activities in their procedures, while the remaining 6 agencies partially addressed or did not address 1 or more of the 7 activities. Table 4 describes the extent to which agency procedures addressed the activities required by OPM.

Table 4: Extent That Chief Financial Officers Act Agencies with Procedures Have Addressed Activities Required by OPM in Their Procedures (Civilian Positions),^a as of March 2018

Agency	Use the updated cybersecurity coding structure to find the appropriate code(s)	CIO staff, managers, and HR and classification staff work together to identify cyber positions	Review all encumbered and vacant positions with cybersecurity functions	Annotate reviewed position descriptions with the appropriate employment code(s)	Cybersecurity positions will extend beyond the GS-2210 IT occupational series	Assign code "000" to non-cybersecurity positions	Assign up to three employment codes to each position, in order of the level of criticality
Department of Agriculture	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Department of Commerce	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Department of Defense	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Department of Education	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Not addressed	Fully addressed
Department of Health and Human Services	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Department of Homeland Security	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Department of Housing and Urban Development	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Department of the Interior	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Department of Justice	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Department of Labor	Fully addressed	Fully addressed	Fully addressed	Not addressed	Partially addressed	Partially addressed	Not addressed
Department of State	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Department of Transportation	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed

Letter

Agency	Use the updated cybersecurity coding structure to find the appropriate code(s)	CIO staff, managers, and HR and classification staff work together to identify cyber positions	Review all encumbered and vacant positions with cybersecurity functions	Annotate reviewed position descriptions with the appropriate employment code(s)	Cybersecurity positions will extend beyond the GS-2210 IT occupational series	Assign code "000" to non-cybersecurity positions	Assign up to three employment codes to each position, in order of the level of criticality
Department of the Treasury	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Department of Veterans Affairs	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Environmental Protection Agency	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
General Services Administration	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
National Aeronautics and Space Administration	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Not addressed	Fully addressed
National Science Foundation	Fully addressed	Fully addressed	Partially addressed	Not addressed	Not addressed	Not addressed	Not addressed
Nuclear Regulatory Commission ^b	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Not addressed	Fully addressed	Partially addressed
Office of Personnel Management	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Small Business Administration	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
Social Security Administration	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
U.S. Agency for International Development	Fully addressed	Fully addressed	Partially addressed	Partially addressed	Fully addressed	Not addressed	Not addressed
Total addressed	23	23	21	20	20	18	19
Total partially addressed	0	0	2	1	1	1	1
Total not addressed	0	0	0	2	2	4	3

● = Fully addressed ○ = Partially addressed ○ = Not addressed

Source: GAO analysis of the 24 Chief Financial Officers Act agencies' cybersecurity employment coding procedures. | GAO-18-466

^aThe Department of Energy is not included in this table because it had not developed procedures as of March 2018.

^bIn its comments responding to a draft of this report, the Nuclear Regulatory Commission stated that it had updated its cybersecurity coding procedures to include language explaining that cybersecurity positions will extend beyond the GS-2210 occupational series, and that each position can be assigned up to three employment codes in order of criticality. The agency provided us a copy of the updated procedures along with its comments on May 10, 2018. Due to the date that we received the procedures, we did not include an assessment of the procedures in this report.

The six agencies that did not address all activities required by OPM cited a variety of reasons for not including them in their coding procedures. For example:

- An official in the Department of Education’s Office of Human Resources explained that it was not necessary for the coding procedures that were provided to each component to address assigning code “000” to noncybersecurity positions because the Office of Human Resources would assign the “000” code to any position that did not have an assigned code.
- An official from the National Science Foundation’s Division of Human Resources Management stated that not addressing all activities may have been an oversight by the agency.
- Officials in NASA’s Office of Human Capital Management and its Office of the CIO said they felt that it was unnecessary to address assigning code “000” to noncybersecurity positions in the agency’s coding procedures because the agencies’ existing guidance for assigning the old 2-digit codes specified that such positions should be coded with “00.”

By not addressing all of the activities required by OPM in their procedures, these 6 agencies lack assurance that the activities will be performed or performed consistently throughout their organizations.

DOD Did Not Establish Coding Procedures for Noncivilian Cybersecurity Positions

In addition to developing procedures for civilian positions, the act required DOD to establish government-wide procedures for identifying and assigning employment codes to noncivilian (i.e., military) positions with cybersecurity job functions by June 2017. The act also required DOD to establish its internal departmental procedures for military positions by September 30, 2017.

According to officials in the department’s Office of the CIO and Office of the Chief Human Capital Officer, the only military personnel not currently within DOD are in the Coast Guard (which resides within DHS). Therefore, the department planned to fulfill its requirements to establish government-wide procedures and internal departmental procedures for identifying and coding military positions by establishing a single consolidated procedure. The officials added that the consolidated procedure is to include procedures for DHS to implement the coding

structure for uniformed Coast Guard personnel along with the internal DOD procedures.

However, as of February 2018, DOD had not finalized its consolidated coding procedures. An official in the department's Office of the CIO in February 2018 stated that, because the military services use multiple Human Resources systems that all have to be updated to accommodate the cybersecurity employment codes, the office was working with each of the military services on guidance to meet the act's deadlines while the services develop implementation plans for updating their human resources systems. Until DOD establishes both government-wide and DOD-specific procedures for identifying and coding noncivilian cybersecurity positions, increased risk exists that DOD and DHS will not be able to identify and code all positions in their noncivilian cybersecurity workforce, limiting the departments' ability to identify cybersecurity skills gaps or work roles of critical need in their noncivilian cybersecurity workforce.

Conclusions

To implement the objectives of the Federal Cybersecurity Workforce Assessment Act of 2015, OPM and NIST, although delayed, have revised the coding structure and cybersecurity workforce framework, and developed coding procedures to support the identification and assignment of codes to federal cybersecurity positions. In addition, most CFO Act agencies have developed baseline assessments to identify cybersecurity personnel within their agencies that held certifications. Having information on the certifications held by cybersecurity employees can be a useful indicator of the skills and knowledge of an agency's cybersecurity workforce. However, because agencies have not consistently defined the workforce and NICE had not developed a list of appropriate certifications, efforts such as conducting the baseline assessment to determine the percentage of cybersecurity personnel that hold appropriate certifications have yielded inconsistent and potentially unreliable results. By not conducting assessments or including all required information in the assessments, some of these agencies may lack valuable information that could help them identify the certification and training needs of their cybersecurity employees that are charged with protecting federal information and information systems from cyberattacks.

Lastly, while most CFO agencies have developed procedures for assigning cybersecurity codes to positions, several agencies did not

address activities required by OPM. Unless those agencies address all of the activities, they may not have reasonable assurance that they are comprehensively identifying the cybersecurity workforce and applying the correct employment codes. As such, increased risk exists that the federal government will not meet its intended goal to define the cybersecurity workforce and address the critical mission needs for a qualified cybersecurity workforce.

Recommendations for Executive Action

We are making a total of 30 recommendations to 13 agencies in our review to develop and submit their baseline assessments and to fully address the required activities in OPM's guidance in their procedures for assigning employment codes to cybersecurity positions. Specifically:

The Secretary of Commerce should evaluate the level of preparedness for cybersecurity personnel not currently holding certifications to take certification exams, identify strategies for mitigating any gaps identified, and report this information to Congress. (Recommendation 1)

The Secretary of Defense should develop, document, and implement government-wide procedures for identifying IT, cybersecurity, and cyber-related noncivilian positions and assigning employment codes to those positions. (Recommendation 2)

The Secretary of Defense should develop, document, and implement internal departmental procedures for identifying IT, cybersecurity, and cyber-related noncivilian positions and assigning employment codes to those positions. (Recommendation 3)

The Secretary of Education should include requirements to assign code "000" to positions that do not perform IT, cybersecurity, and cyber-related functions in departmental procedures. (Recommendation 4)

The Secretary of Energy should evaluate the level of preparedness for cybersecurity personnel not currently holding certifications to take certification exams and report this information to Congress. (Recommendation 5)

The Secretary of Energy should develop, document, and implement departmental procedures for identifying IT, cybersecurity, and cyber-related positions and assigning employment codes to those positions,

taking into account the key elements described in OPM's instructions for agencies' procedures. (Recommendation 6)

The Secretary of Homeland Security should conduct a baseline assessment of the department's cybersecurity workforce that includes (1) the percentage of personnel with IT, cybersecurity, or other cyber-related job functions who hold certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel. (Recommendation 7)

The Secretary of Homeland Security should submit a report of the department's baseline assessment of its existing cybersecurity workforce to the appropriate congressional committees of jurisdiction. (Recommendation 8)

The Secretary of Housing and Urban Development should conduct a baseline assessment of the department's cybersecurity workforce that includes (1) the percentage of personnel with IT, cybersecurity, or other cyber-related job functions who hold certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel. (Recommendation 9)

The Secretary of Housing and Urban Development should submit a report of the department's baseline assessment of its existing cybersecurity workforce to the appropriate congressional committees of jurisdiction. (Recommendation 10)

The Secretary of the Interior should evaluate the level of preparedness for cybersecurity personnel not currently holding certifications to take certification exams and report this information to Congress. (Recommendation 11)

The Secretary of Labor should include requirements to annotate reviewed position descriptions with the appropriate cybersecurity data standard code(s) in departmental procedures. (Recommendation 12)

The Secretary of Labor should ensure that departmental procedures fully account for the fact that IT, cybersecurity, and cyber-related positions will extend beyond the Information Technology Management 2210 occupational series. (Recommendation 13)

The Secretary of Labor should fully clarify requirements to assign code "000" to positions that do not perform IT, cybersecurity, and cyber-related functions in departmental procedures. (Recommendation 14)

The Secretary of Labor should include requirements to assign up to three employment codes per position in order of their criticality in departmental procedures. (Recommendation 15)

The Administrator of the National Aeronautics and Space Administration should evaluate the level of preparedness for cybersecurity personnel not currently holding certifications to take certification exams and report this information to Congress. (Recommendation 16)

The Administrator of the National Aeronautics and Space Administration should include requirements to assign code "000" to positions that do not perform IT, cybersecurity, and cyber-related functions in agency procedures. (Recommendation 17)

The Director of the National Science Foundation should fully clarify requirements to review all encumbered and vacant positions performing IT, cybersecurity, and cyber-related functions in agency procedures. (Recommendation 18)

The Director of the National Science Foundation should include requirements to annotate reviewed position descriptions with the appropriate cybersecurity data standard code(s) in agency procedures. (Recommendation 19)

The Director of the National Science Foundation should ensure that agency procedures account for the fact that IT, cybersecurity, and cyber-related positions will extend beyond the Information Technology Management 2210 occupational series. (Recommendation 20)

The Director of the National Science Foundation should include requirements to assign code "000" to positions that do not perform IT, cybersecurity, and cyber-related functions in agency procedures. (Recommendation 21)

The Director of the National Science Foundation should include requirements to assign up to three employment codes per position in order of their criticality in agency procedures. (Recommendation 22)

The Chairman of the Nuclear Regulatory Commission should ensure that agency procedures account for the fact that IT, cybersecurity, and cyber-related positions will extend beyond the Information Technology Management 2210 occupational series. (Recommendation 23)

The Chairman of the Nuclear Regulatory Commission should fully clarify requirements to assign up to three employment codes per position in order of their criticality in agency procedures. (Recommendation 24)

The Administrator of the Small Business Administration should conduct a baseline assessment of the department's cybersecurity workforce that includes (1) the percentage of personnel with IT, cybersecurity, or other cyber-related job functions who hold certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel. (Recommendation 25)

The Administrator of the Small Business Administration should submit a report of its baseline assessment of its existing cybersecurity workforce to the appropriate congressional committees of jurisdiction. (Recommendation 26)

The Administrator of the U.S. Agency for International Development should fully clarify requirements to review all encumbered and vacant positions performing IT, cybersecurity, and cyber-related functions in agency procedures. (Recommendation 27)

The Administrator of the U.S. Agency for International Development should fully clarify requirements to annotate reviewed position descriptions with the appropriate cybersecurity data standard code(s) in agency procedures. (Recommendation 28)

The Administrator of the U.S. Agency for International Development should include requirements to assign code "000" to positions that do not perform IT, cybersecurity, and cyber-related functions in agency procedures. (Recommendation 29)

The Administrator of the U.S. Agency for International Development should include requirements to assign up to three employment codes per position in order of their criticality in agency procedures. (Recommendation 30)

Agency Comments and Our Evaluation

We provided a draft of this report to the 24 CFO Act agencies for their review and comment. Of the 13 agencies to which we made recommendations, 7 agencies stated that they agreed with all of the recommendations directed to them; 1 agency agreed with one and did not agree with one recommendation; 2 agencies provided comments but did not state whether they agreed or disagreed with the recommendations; 2 agencies stated that they had no comments; and 1 agency—DOD—did not respond to our request for comments on the report.

In addition, of the 11 agencies to which we did not make recommendations, 2 provided comments on the report and 9 responded that they had no comments on the report. We also received technical comments from 2 agencies, which we have incorporated into the report as appropriate.

The following seven agencies agreed with our recommendations:

- In its written comments (reprinted in appendix II), the Department of Commerce agreed with our recommendation. The department stated that it will evaluate the level of preparedness for cybersecurity personnel who do not hold certifications to take certification exams, identify strategies for mitigating any gaps identified, and report this information to Congress.
- In its written comments (reprinted in appendix III), the Department of Education agreed with our recommendation. The department stated that it had updated its coding guidance to require that positions that do not perform substantial work in information technology, cybersecurity, or cyber-related functions be assigned a code of “000.”
- In its written comments (reprinted in appendix IV), the Department of Energy agreed with our recommendations and stated that it has planned, or taken steps to address them. Specifically, with regard to our recommendation concerning cybersecurity certification, the department stated that it plans to conduct a department-wide evaluation of the level of preparedness for its cybersecurity personnel without existing credentials to take certification exams and will report the information to Congress.

In addition, the department stated that it had developed and issued procedures for identifying and coding IT, cybersecurity, and cyber-related positions, as we recommended, and that it had since

completed its coding of applicable positions across the department. The department also provided us its updated coding procedures, along with its written comments.

- In its written comments (reprinted in appendix V), the Department of Homeland Security agreed with our recommendations. Regarding the recommendation to conduct a baseline assessment of its cybersecurity workforce, the department stated that it is taking steps to collect data about certifications relevant to DHS cybersecurity work. The department also stated that it plans to identify the percentage of its cybersecurity workforce that holds certifications, the percentage prepared to take a relevant certification exam, and strategies for mitigating any gaps. The department added that it plans to provide this information to Congress, as we recommended. The department also provided technical comments, which we have incorporated into this report as appropriate.
- In its written comments (reprinted in appendix VI), the Department of the Interior stated that it agreed with our recommendation. The department also indicated that it is exploring options to determine the extent to which its cybersecurity employees who currently do not hold certifications are prepared to take certification exams.
- In its written comments (reprinted in appendix VII), the Small Business Administration agreed with our recommendations. The agency also stated that it had recently completed an assessment of its IT workforce and reported on existing skills gaps, and that it plans to execute its IT workforce plan to address the requirements of the Federal Cybersecurity Workforce Assessment Act of 2015.
- In comments on a draft of this report provided via email on May 15, 2018, a Program Analyst in the National Science Foundation's Office of Integrative Activities stated that the agency concurred with our recommendations.

One agency did not agree with one of the two recommendations directed to it:

- In its written comments (reprinted in appendix VIII), the National Aeronautics and Space Administration did not agree with our first recommendation and agreed with the second. Specifically:
 - NASA did not concur with our recommendation to evaluate the level of preparedness for cybersecurity personnel not currently holding certifications to take certification exams and report this information to Congress. The agency stated that there is no

federal or NASA requirement for employees in cybersecurity positions to hold and/or maintain a certification, and therefore the agency has no plans to assess the readiness of its cybersecurity personnel to take certification exams.

Nonetheless, we continue to believe our recommendation remains valid because the level of preparedness of personnel without certifications to take certification examinations can be a useful indicator of the skills and knowledge of an agency's cybersecurity workforce. In addition, this information could help the agency identify and meet the certification and training needs of its cybersecurity employees who are charged with protecting NASA's information and information systems from cyberattacks. Moreover, the act contains provisions that demonstrate congressional interest in assessing agency use of professional certifications.

- NASA concurred with our recommendation to include in the agency's coding procedures, requirements to assign code "000" to positions that do not perform IT, cybersecurity, and cyber-related functions. The agency stated that it planned to update its procedures to include this requirement, and indicated that supervisors and human resource specialists had been trained to assign cybersecurity codes to all positions, including code "000."

The following two agencies provided comments, but did not state whether they agreed or disagreed with our recommendations:

- In its written comments (reprinted in appendix IX), the Nuclear Regulatory Commission stated that it was in general agreement with the overall content of the draft report. However, the agency asked that we revise the final report to reflect that the Nuclear Regulatory Commission had updated its cybersecurity coding procedures to include language explaining that IT, cybersecurity, and cyber-related positions will extend beyond the GS-2210 occupational series, and to outline the requirement that positions can be assigned up to three different employment codes in order of criticality. The agency provided its updated coding procedures along with its written comments.
- In its written comments (reprinted in appendix X), the U.S. Agency for International Development stated that it had completed various actions related to coding its cybersecurity positions which addressed our four recommendations. For example, among other actions, the agency said it had updated its plan for coding cybersecurity positions to include procedures for assigning codes for multiple functional areas, with the predominant functional area being coded first.

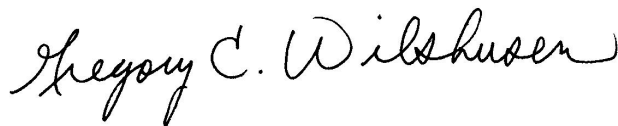
In addition, two agencies to which we made recommendations—the Departments of Housing and Urban Development and Labor—stated via email that they did not have comments on the report. The agencies did not state whether they agreed or disagreed with our recommendations.

Of the agencies to which we did not make recommendations, the Social Security Administration also provided a letter acknowledging its review of the report. The agency's letter is reprinted in appendix XI.

The remaining nine agencies to which we did not make recommendations—the Departments of Agriculture, Health and Human Services, Justice, State, Transportation, and Treasury; the Environmental Protection Agency; the General Services Administration; and the Office of Personnel Management—stated that they did not have any comments on our report.

We are sending copies of this report to interested congressional committees, the Director of the Office of Management and Budget, the secretaries and agency heads of the departments and agencies addressed in this report, and other interested parties. In addition, this report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you have any questions regarding this report, please contact me at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix XII.



Gregory C. Wilshusen
Director, Information Security Issues

List of Committees

The Honorable John McCain
Chairman

The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Ron Johnson
Chairman

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

The Honorable Richard Burr
Chairman

The Honorable Mark Warner
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable John Thune
Chairman

The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Mac Thornberry
Chairman

The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

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

The Honorable Trey Gowdy
Chairman
The Honorable Elijah Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Devin Nunes
Chairman
The Honorable Adam Schiff
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine whether (1) OPM developed a coding structure and procedures for assigning codes to cybersecurity positions and submitted a progress report to Congress, (2) Chief Financial Officers (CFO) Act agencies¹ submitted complete and reliable baseline assessment reports of their cybersecurity workforces, and (3) CFO Act agencies established procedures to identify and assign codes to cybersecurity positions.

The scope of our review included the 24 departments and agencies (hereafter referred to as agencies) covered by the Chief Financial Officers Act of 1990. It also included OPM, DOD, DHS, and NIST in their roles related to the development of a cybersecurity coding structure and related guidance. Our work focused on the agencies' cybersecurity positions and on workforce planning actions that the act required the agencies to complete by November 2017.

To address the first objective, we obtained and compared OPM's federal cybersecurity employment coding structure, issued in November 2016, to the work roles described in the *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, issued in draft form by NIST in November 2016.² We also examined OPM memorandums to identify if and when OPM had issued procedures to agencies for identifying cybersecurity positions and assigning

¹The 24 federal agencies covered by the Chief Financial Officers Act of 1990 are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

²National Institute of Standards and Technology (NIST), *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, Draft NIST Special Publication 800-181 (Gaithersburg, Md.: November 2016).

employment codes.³ Additionally, we reviewed any progress reports submitted by OPM to Congress on the implementation of the act. We compared the issuance date of each of these documents to the deadlines by which OPM was to issue them, as established in the act. Also, we interviewed OPM and NIST officials about their efforts to develop these documents and the reasons for any delays.

To address the second objective, we obtained available baseline assessments from each of the 24 CFO Act agencies and evaluated them against the act's requirements to include information on (1) cybersecurity personnel holding certifications, (2) the level of preparedness of other personnel to take certification exams, and (3) strategies for mitigating any gaps identified. We also obtained agencies' letters transmitting their assessments to the relevant congressional committees and evaluated them against the reporting deadline established in OPM guidance. In addition, we analyzed other relevant agency documentation and interviewed cognizant agency officials about their efforts to identify the appropriate certifications, identify relevant personnel, and collect information on employee certifications. We obtained the officials' views on the reasons for any delays in agencies' submissions of the assessments and the reliability of assessment results.

To address the third objective, we obtained and analyzed available cybersecurity coding procedures established by each of the 24 CFO Act agencies. We reviewed the required coding activities described in OPM's *Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions*. We judgementally selected seven of the activities that we determined to be particularly important for effectively identifying and coding all relevant encumbered and vacant cybersecurity positions. We then evaluated each agency's procedures against these seven required coding activities. We also compared the issuance date of the procedures to the deadline established in OPM's coding guidance for agencies to issue the procedures. In addition, we interviewed agency officials about their efforts to complete the procedures by the required deadline and the reasons for any delays.

³Office of Personnel Management, *Memorandum for Heads of Executive Departments and Agencies: Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions* (Washington, D.C.: January 4, 2017).

Further, the Federal Cybersecurity Workforce Assessment Act of 2015 established a separate requirement and deadline for DOD to develop government-wide procedures for implementing the coding structure for federal noncivilian cyber positions. As such, we reviewed relevant documentation and interviewed cognizant officials from the Department of Defense's Office of the Chief Information Officer and Office of the Under Secretary for Personnel and Readiness about their efforts to establish coding procedures for both civilian and noncivilian positions by the deadlines set forth in the act.

We conducted this performance audit from October 2016 to June 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: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

May 23, 2018

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

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report titled *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions* (GAO-18-466).

On behalf of the Department of Commerce, I have enclosed our comments on the draft report. The Department of Commerce agrees with the recommendation and will evaluate the level of preparedness for cybersecurity personnel who do not hold professional certifications. Additionally, the Department of Commerce will also identify strategies for mitigating gaps and will report the information to Congress.

If you have any questions, please contact MaryAnn Mausser, Commerce GAO/Office of Inspector General Audit Liaison, at (202) 482-8120.

Sincerely,


Wilbur Ross

Enclosure

**Department of Commerce's Comments on
GAO Draft Report titled *Cybersecurity Workforce: Agencies Need to Improve Baseline
Assessments and Procedures for Coding Positions*
(GAO-18-466)**

The Department of Commerce has reviewed the draft report, and we offer the following response for GAO's consideration.

Comments on Recommendations

- **Recommendation 1:** The Secretary of Commerce should evaluate the level of preparedness for cybersecurity personnel not currently holding professional certifications to take certification exams, identify strategies for mitigating any gaps identified, and report this information to Congress. (Recommendation 1).
- **Commerce Response:** The Department of Commerce agrees with the recommendation and will evaluate the level of preparedness for cybersecurity personnel who do not hold professional certifications to take certification exams applicable to positions held. The Department of Commerce will also identify strategies for mitigating gaps and will report the information to Congress by the end of Q4, FY 2018 and will continue to provide updates quarterly in the following fiscal year.

Appendix III: Comments from the Department of Education



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF MANAGEMENT

May 11, 2018

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

I am writing on behalf of the U.S. Department of Education (Department) to respond to the recommendation made in the Government Accountability Office (GAO) draft report, "Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions" (GAO-18-466). The Department appreciates the opportunity to respond to the draft GAO report. Below is our response to GAO's specific recommendation to the Department. We urge GAO to note that the Department has already taken action to address GAO's draft recommendation.

Recommendation 4: The Secretary of Education should include requirements to assign code "000" to positions that do not perform IT, cybersecurity, and cyber-related functions in departmental procedures.

Response: The Department concurs with this recommendation and has already completed actions to address GAO's draft recommendation. The Department developed and implemented on April 18, 2018, guidance that requires positions that do not perform substantial work in information technology, cybersecurity, or cyber-related functions to be assigned code "000." Enclosed is a copy of the guidance. The Department has completed cyber security coding for all current positions.

Thank you for the opportunity to respond to the GAO report. If you or your staff members have any questions regarding our response, please contact James Simmons at (202) 805-5543 or by e-mail at James.K.Simmons@ed.gov.

Regards,

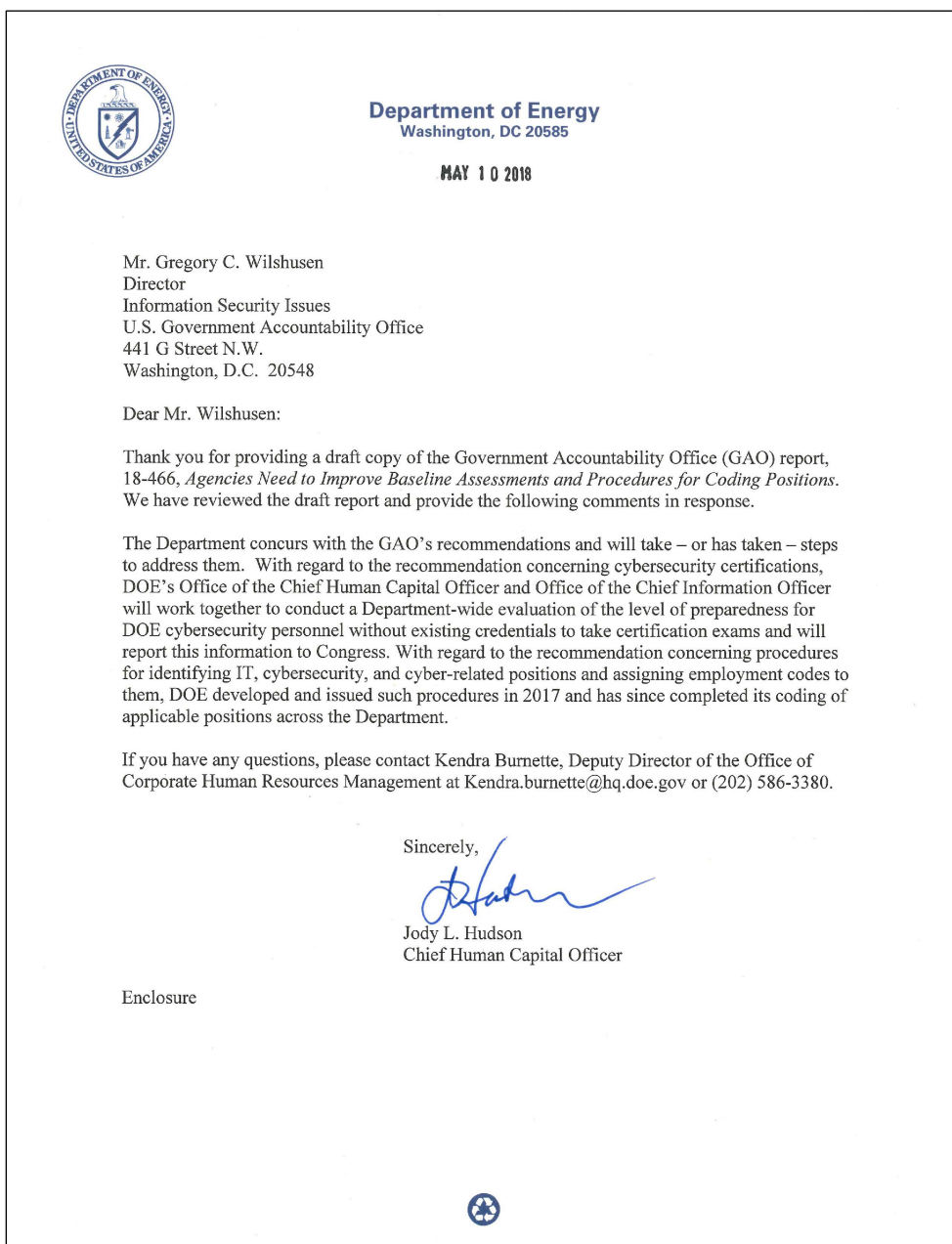
A handwritten signature in cursive script that reads "A. Bianca Green".

A. Bianca Green
Chief Human Capital Officer
Office of Management

400 MARYLAND AVE., S.W., WASHINGTON, D.C. 20202-4500
www.ed.gov

The Department of Education's mission is to promote student achievement and preparation of global competitiveness by fostering educational excellence and ensuring equal access.

Appendix IV: Comments from the Department of Energy



Response to Report Recommendations

Recommendation 5: *The Secretary of Energy should evaluate the level of preparedness for cybersecurity personnel not currently holding professional certification to take certification exams and report this information to Congress.*

Management Response: Concur

DOE's Office of the Chief Information Officer (OCIO) and Office of the Chief Human Capital Officer (OCHCO) will work together to evaluate the level of preparedness for DOE cybersecurity personnel without existing credentials to take certification exams. Using the National Initiative for Cybersecurity Education (NICE) certification mapping, which is expected to be completed by November 2018, DOE's OCHCO and OCIO will develop criteria for identifying personnel who are prepared to take certification exams and will perform a Department-wide evaluation. Once this gap has been closed, DOE will report its findings to Congress. The estimated completion date for this action is June 30, 2019, contingent upon the actual issuance date of the NICE certification mapping.

Recommendation 6: *The Secretary of Energy should develop, document, and implement departmental procedures for identifying IT, cybersecurity, and cyber-related positions and assigning employment codes to those positions, taking into account the key elements described in OPM's instructions for agencies' procedures.*

Management Response: Concur

This recommendation is closed. DOE's OCHCO issued Department-wide procedures for identifying IT, cybersecurity, and cyber-related positions and assigning employment codes to those positions on August 22, 2017. Since the issuance of that guidance, the OCHCO has engaged in a collaborative effort with IT professionals throughout the agency to conduct a Department-wide evaluation of all employee position descriptions, taking into account key elements as described by OPM and in accordance with The Federal Cybersecurity Workforce Assessment Act. As of April 29, 2018, DOE has completed this effort. Employment codes have been assigned to applicable positions, annotated on employee position descriptions, and uploaded into the system of record.

Appendix V: Comments from the Department of Homeland Security

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



May 14, 2018

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

RE: Management's Response to Draft Report GAO-18-466, "CYBERSECURITY WORKFORCE: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions"

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 recognition of actions DHS has taken to identify its cybersecurity positions and assign employment codes to each position. DHS remains committed to strengthening processes for examining its cybersecurity workforce, while identifying and addressing critical gaps.

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 set of 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.

It is also important to highlight the draft report's heavy focus on professional certifications, in alignment with the analysis and reporting requirements outlined by Congress in the Federal Cybersecurity Workforce Assessment Act of 2015. While DHS Components have identified a broad range of professional certifications relevant to DHS cybersecurity work, DHS has not established Department-wide certification requirements, and does not believe doing so is the appropriate course of action. Ongoing DHS analyses, led by industrial/organizational psychologists, continue to confirm that certain certifications can be an indicator of a candidate or employee's qualifications, but they are not the best or sole determinant of a candidate or employee's ability to perform critical cybersecurity work. When recruiting and selecting

candidates, DHS is required to comply with a series of other laws, which mandate that decisions be based on validated, job-related criteria; professional certifications have yet to be established as such criteria. DHS is committed to pursuing a variety of methods for verifying candidate and employee qualifications, including certifications, and will continue to update Congress on its findings.

The draft report contained 30 recommendations to 13 agencies, two that were for DHS and with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously submitted 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 in the future.

Sincerely,



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

Attachment

**Attachment: Management Response to Recommendations
Contained in GAO-18-466**

GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Conduct a baseline assessment of the Department's cybersecurity workforce that includes (1) the percentage of personnel with [information technology] IT, cybersecurity, or other cyber-related job functions who hold professional certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel. (Recommendation 7)

Response: Concur. The DHS Office of the Chief Human Capital Officer (OCHCO) continues to collect data about professional certifications relevant to DHS cybersecurity work. In FY 2018, OCHCO worked with Components to source data about priority certifications, the number of employees that hold them, and the readiness of other employees to take certification exams. On April 30, 2018, DHS finalized three-digit coding of its federal cybersecurity positions, confirming a new baseline population of cybersecurity positions. During the remainder of FY 2018 and into early FY 2019, OCHCO plans to conduct a series of analyses with Components to review the population of three-digit coded positions, and finalize the percentage who hold certifications as well as the percentage prepared to take a relevant certification exam. In addition, OCHCO will identify and document strategies for mitigating any identified gaps. Estimated Completion Date (ECD): January 31, 2019.

Recommendation 2: Submit a report of the Department's baseline assessment of its existing cybersecurity workforce to the appropriate congressional committees of jurisdiction. (Recommendation 8)

Response: Concur. Upon final leadership review, OCHCO will send Congress a 2017 Comprehensive Cybersecurity Workforce Update report, which provides additional baseline information on the Department's cybersecurity workforce. In addition, OCHCO plans to leverage analysis during the remainder of FY 2018 and into early FY 2019 to produce an additional report for Congress, addressing the requirements of the baseline assessment. ECD: January 31, 2019.

Appendix VI: Comments from the Department of the Interior



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

MAY 08 2018

Mr. David Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Powner:

Thank you for providing the Department of the Interior (Department) the opportunity to review and comment on the draft Government Accountability Office (GAO) report entitled, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions* (GAO-18-466). We appreciate GAO's review of the federal Cybersecurity Workforce.

The Department concurs with the recommendation stating, the Secretary of the Interior should evaluate the level of preparedness for cybersecurity personnel not currently holding professional certifications to take certification exams and report this information to Congress.

Also, the Department suggests that the third bullet on Page 24 be rewritten as follows, to accurately describe the current level of preparedness within the Department.

According to the Department officials, currently neither the U.S. Office of Personnel Management nor the Department requires certifications for these cybersecurity positions. However, the Department's Office of Human Resources and the Office of the Chief Information Officer are exploring options to determine the level of preparedness across its IT workforce. To that effect, the Department is updating its Learning Management System which will assist in tracking on-going requirements and identify baseline preparedness moving forward.

Please incorporate our comments when finalizing the report. If you have any questions or need additional information, please contact Sylvia Burns, Chief Information Officer at Sylvia_Burns@ios.doi.gov.

Sincerely,

Scott J. Cameron
Principal Deputy Assistant Secretary
for Policy, Management and Budget
Exercising the Authority of the
Assistant Secretary for Policy,
Management and Budget

Appendix VII: Comments from the Small Business Administration

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416



May 10, 2018

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

Dear Mr. Wilshusen:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled "Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions" (GAO-18-466).

The draft report measures agency progress in implementing requirements identified in the Federal Cybersecurity Workforce Assessment Act of 2015. SBA agrees with the recommendations made in the report and has made significant progress in the workforce assessment area. Specifically, SBA recently completed an assessment of the SBA's IT workforce and reported on existing skills gaps. SBA plans to execute against the IT workforce plan to include addressing requirements within the Federal Cybersecurity Workforce Assessment Act of 2015. SBA looks forward to working with GAO to address the recommendations made in this report.

Thank you for the opportunity to comment on this report.

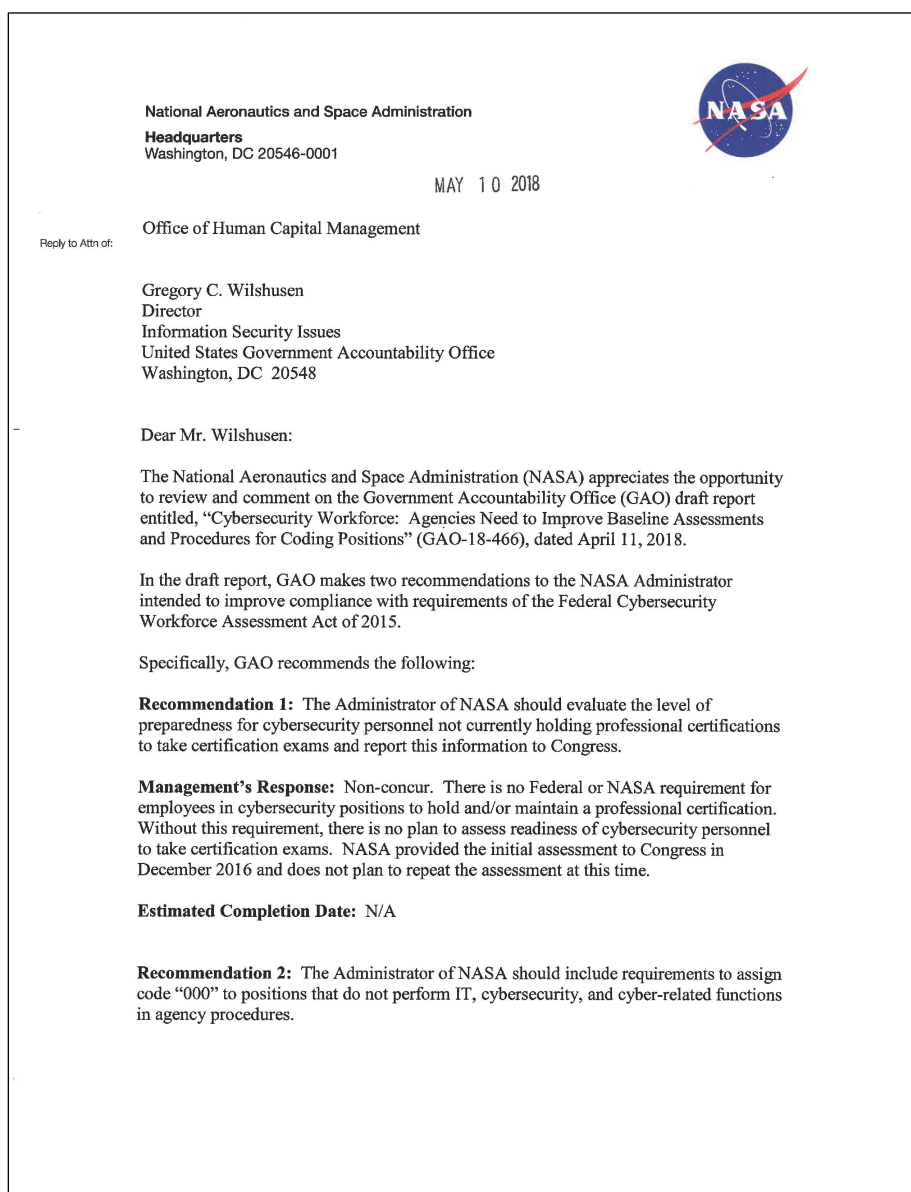
Sincerely,

MARIA
ROAT

Digitally signed by
MARIA ROAT
Date: 2018.05.10
14:46:31 -0400

Maria Roat
Chief Information Officer

Appendix VIII: Comments from National Aeronautics and Space Administration

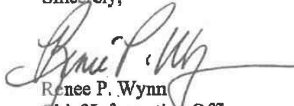


Management's Response: Concur. NASA will update current Agency procedures to document the change from the two-digit code of "00" to the new three-digit code of "000" for positions that do not perform cybersecurity or cybersecurity-related functions. The three-digit framework is available, and positions are being coded properly in our Electronic Position Description System (ePDS) and Federal Personnel Payroll System (FPPS) systems. Guidance is provided in the help buttons in ePDS, and supervisors and Human Resource Specialists have been trained on assigning cybersecurity codes or "000" to all positions. We will issue a new Personnel Bulletin documenting the above by May 18, 2018.

Estimated Completion Date: May 18, 2018

Once again, thank you for the opportunity to comment on the subject draft report. If you have any questions or require additional information, please contact Heather Noiwan on (202) 358-2379.

Sincerely,


Renee P. Wynn
Chief Information Officer


Robert Gibbs
Assistant Administrator for Human Capital Management

Appendix IX: Comments from the Nuclear Regulatory Commission



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

May 10, 2018

Gregory C. Wilshusen, Director
Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20226

Dear Director Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) Draft Audit Report: *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions (GAO-18-466)*, which was provided to the U.S. Nuclear Regulatory Commission (NRC) on April 11, 2018. The NRC staff is in general agreement with the overall content of the draft audit report. However, the NRC staff requests that the evaluation of two factors for the NRC and their associated recommendations be updated in the final report to reflect our current condition. The draft report cited two of the seven factors, in reference to the Cybersecurity Coding Procedures, as incomplete for the NRC. The same two factors were cited as incomplete during the GAO exit conference on October 31, 2017. During this exit conference, we discussed the *Engagement 101198: Statement of Facts and the Preliminary Findings*, which assessed our progress toward completion of Cybersecurity Coding Procedures.

The first factor requires that procedures include language explaining that Information Technology (IT), Cybersecurity, and cyber-related positions will extend beyond the GG-2210 IT occupational series. The second factor requires that the procedures outline the requirement that positions can be assigned up to three different codes and that these codes will be assigned in order of criticality. While these two factors are not required by the Office of Personnel Management, GAO felt strongly that they should be added. Therefore, the NRC Cybersecurity Coding Procedures were revised to incorporate the missing factors in November 2017 (see enclosed with revisions highlighted).

If you have any questions regarding the NRC's response, please contact John R. Jolicoeur by phone at (301) 415-1642 or by email at john.jolicoeur@nrc.gov.

Sincerely,

A handwritten signature in black ink that reads "Victor M. McCrea".

Victor M. McCrea
Executive Director for Operations

Enclosure:
NRC Cybersecurity Coding Procedures

Appendix X: Comments from the United States Agency for International Development



MAY 22 2018

Gregory C. Wilshusen
Director
Information-Security Issues
U.S. Government Accountability Office (GAO)
441 G Street, N.W.
Washington, D.C. 20548

Re: CYBERSECURITY WORKFORCE: Agencies Need to Improve Baseline
Assessments and Procedures for Coding Positions (GAO-18-466)

Dear Mr. Wilshusen:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the GAO draft report entitled, "*CYBERSECURITY WORKFORCE: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions*" (GAO-18-466). USAID is providing this letter and enclosed comments for incorporation as an appendix to the GAO's final report.

USAID is dedicated to maintaining its Government-leading cyber posture. Through the cooperative efforts of our Offices of Human Capital and Talent-Management (HCTM) and Chief Information Officer (CIO), USAID has completed all coding tasks recommended by the GAO. For reference, we have updated and enclosed our plan for coding cybersecurity positions, established to complete the original baseline.

Thank you for the opportunity to respond to the GAO's draft report, and for the courtesies extended by your staff while conducting this engagement.

Sincerely,

A handwritten signature in blue ink, appearing to read "Angélique M. Crumbly".

Angélique M. Crumbly
Acting Assistant Administrator
Bureau for Management

Enclosures: a/s

COMMENTS FROM
THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID)
ON THE DRAFT REPORT PRODUCED
BY THE
U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO) ENTITLED,
“CYBERSECURITY WORKFORCE: Agencies Need to Improve Baseline
Assessments and Procedures for Coding Positions” (GAO-18-466)

This report has four recommendations for USAID, as shown on page 38 of the draft report:

Recommendation 27: The Administrator of USAID should fully clarify requirements to review all encumbered and vacant positions performing information-technology (IT) and cyber-related functions in agency procedures.

- USAID has taken action to close out the recommendation. In March 2018, the Agency updated our plan for coding cybersecurity positions, to include the procedures for reviewing all encumbered and vacant ones. USAID has completed this review, performed by the Office of the Chief Information Office (M/CIO) in the Bureau for Management and the Office of Human Capital and Talent-Management (HCTM).

Recommendation 28: The Administrator of USAID should fully clarify requirements to annotate reviewed position descriptions with the appropriate cybersecurity data standard code(s) in agency procedures.

- USAID has taken action to close out the recommendation. The Agency has reviewed all occupied/vacant positions; identified IT, cybersecurity, and cyber-related positions; and assigned the three-digit codes accordingly. The positions include the following occupational series:

IT (2210), Computer Engineering (0854), Contracting Series (1102), Computer Science (1550), and Miscellaneous Administration and Program (0301).

Further, as is standard practice, M/CIO must provide the three-digit cybersecurity code in Section 24 (Remarks) of the Position Description (OF-8) for all positions that have IT; cybersecurity, and cyber-related functions. The USAID HCTM Human-Capital Service Center/Classification will update Section 24 (Remarks) of the OF-8 on all positions currently in existence.

Recommendation 29: The Administrator of USAID should include requirements to assign code “000” to positions that do not perform IT, cybersecurity, and cyber-related functions in agency procedures.

- USAID has taken action to close out the recommendation, and Table 4 on page 32 of the draft report does not accurately reflect the Agency’s progress in this area. On December 1, 2017, USAID assigned code 000 to all non-cyber positions in both HR Connect, a USAID corporate human-resource system, and the National Finance Center (NFC) system, USAID’s corporate payroll/personnel system. The GAO should mark this category in the table as “Fully Addressed.”

Recommendation 30: The Administrator of USAID should include requirements to assign up to three employment codes per position in order of their criticality in agency procedures.

- USAID has taken action to close out the recommendation. In March 2018, USAID updated its plan for coding cybersecurity positions to include procedures on functional coding. When a position aligns with more than one functional area, the Agency codes the predominant functional area first, and will add any others where and when necessary. In April 2018, USAID completed all coding for both encumbered and vacant cybersecurity positions.

Appendix XI: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

May 10, 2018

Mr. Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review the draft report, "CYBERSECURITY WORKFORCE: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions" (GAO-18-466). We are pleased that GAO concluded that, in December 2016, we reported to Congress the required elements in our baseline assessment, as required by the *Federal Cybersecurity Workforce Assessment Act of 2015*. Additionally, in April 2017, as required by guidance released in January 2017 by the Office of Personnel Management, we established and issued coding procedures to identify and assign codes to cybersecurity positions. We have no further comment.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

A handwritten signature in blue ink that reads "Stephanie Hall".

Stephanie Hall
Acting Deputy Chief of Staff

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

Appendix XII: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individual named above, Nick Marinos (director), Tammi Kalugdan (assistant director), William Cook (analyst in charge), Chris Businsky, Virginia Chanley, Wayne Emilien, Lisa Maine, David Plocher, Priscilla Smith, Dwayne Staten, Daniel Wexler, and Merry Woo made significant contributions to this report.

Appendix XIII: Accessible Data

Agency Comment Letter

Text of Appendix III: Comments from the Department of Commerce

Page 1

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report titled *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions* (GAO-18-466).

On behalf of the Department of Commerce, I have enclosed our comments on the draft report. The Department of Commerce agrees with the recommendation and will evaluate the level of preparedness for cybersecurity personnel who do not hold professional certifications. Additionally, the Department of Commerce will also identify strategies for mitigating gaps and will report the information to Congress.

If you have any questions, please contact MaryAnn Mausser, Commerce GAO/Office of Inspector General Audit Liaison, at (202) 482-8120.

Sincerely,

Wilbur Ross

Enclosure

Page 2

**Department of Commerce's Comments on GAO Draft Report titled
Cybersecurity Workforce: Agencies Need to Improve Baseline
Assessments and Procedures for Coding Positions
(GAO-18-466)**

The Department of Commerce has reviewed the draft report, and we offer the following response for GAO's consideration.

Comments on Recommendations

Recommendation 1: The Secretary of Commerce should evaluate the level of preparedness for cybersecurity personnel not currently holding professional certifications to take certification exams, identify strategies for mitigating any gaps identified, and report this information to Congress. (Recommendation 1).

Commerce Response: The Department of Commerce agrees with the recommendation and will evaluate the level of preparedness for cybersecurity personnel who do not hold professional certifications to take certification exams applicable to positions held. The Department of Commerce will also identify strategies for mitigating gaps and will report the information to Congress by the end of Q4, FY 2018 and will continue to provide updates quarterly in the following fiscal year.

**Text of Appendix IV: Comments from the Department of
Energy**

Page 1

Dear Mr. Wilshusen:

Thank you for providing a draft copy of the Government Accountability Office (GAO) report, 18-466, Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions. We have reviewed the draft report and provide the following comments in response.

The Department concurs with the GAO's recommendations and will take - or has taken - steps to address them. With regard to the recommendation concerning cybersecurity certifications, DOE's Office of the Chief Human Capital Officer and Office of the Chief Information Officer will work

together to conduct a Department-wide evaluation of the level of preparedness for DOE cybersecurity personnel without existing credentials to take certification exams and will report this information to Congress. With regard to the recommendation concerning procedures for identifying IT, cybersecurity, and cyber-related positions and assigning employment codes to them, DOE developed and issued such procedures in 2017 and has since completed its coding of applicable positions across the Department.

If you have any questions, please contact Kendra Burnette, Deputy Director of the Office of Corporate Human Resources Management at Kendra.burnette@hq.doe.gov or (202) 586-3380.

Sincerely,

Jody L. Hudson
Chief Human Capital Officer

Enclosure

Page 2

Response to Report Recommendations

Recommendation 5: The Secretary of Energy should evaluate the level of preparedness for cybersecurity personnel not currently holding professional certification to take certification exams and report this information to Congress.

Management Response: Concur

DOE's Office of the Chief Information Officer (OCIO) and Office of the Chief Human Capital Officer (OCHCO) will work together to evaluate the level of preparedness for DOE cybersecurity personnel without existing credentials to take certification exams. Using the National Initiative for Cybersecurity Education (NICE) certification mapping, which is expected to be completed by November 2018, DOE's OCHCO and OCIO will develop criteria for identifying personnel who are prepared to take certification exams and will perform a Department-wide evaluation. Once this gap has been closed, DOE will report its findings to Congress. The estimated completion date for this action is June 30, 2019, contingent upon the actual issuance date of the NICE certification mapping.

Recommendation 6: The Secretary of Energy should develop, document, and implement departmental procedures for identifying IT, cybersecurity, and cyber-related positions and assigning employment codes to those positions, taking into account the key elements described in OPM's instructions for agencies' procedures.

Management Response: Concur

This recommendation is closed. DOE's OCHCO issued Department-wide procedures for identifying IT, cybersecurity, and cyber-related positions and assigning employment codes to those positions on August 22, 2017. Since the issuance of that guidance, the OCHCO has engaged in a collaborative effort with IT professionals throughout the agency to conduct a Department-wide evaluation of all employee position descriptions, taking into account key elements as described by OPM and in accordance with The Federal Cybersecurity Workforce Assessment Act. As of April 29, 2018, DOE has completed this effort. Employment codes have been assigned to applicable positions, annotated on employee position descriptions, and uploaded into the system of record.

Text of Appendix V: Comments from the Department of Homeland Security

Page 1

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 recognition of actions DHS has taken to identify its cybersecurity positions and assign employment codes to each position. DHS remains committed to strengthening processes for examining its cybersecurity workforce, while identifying and addressing critical gaps.

OHS 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 set of 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.

It is also important to highlight the draft report's heavy focus on professional certifications, in alignment with the analysis and reporting requirements outlined by Congress in the Federal Cybersecurity Workforce Assessment Act of 2015. While DHS Components have identified a broad range of professional certifications relevant to OHS cybersecurity work, DHS has not established Department-wide certification requirements, and does not believe doing so is the appropriate course of action. Ongoing DHS analyses, led by industrial/organizational psychologists, continue to confirm that certain certifications can be an indicator of a candidate or employee's qualifications, but they are not the best or sole determinant of a candidate or employee's ability to perform critical cybersecurity work. When recruiting and selecting candidates, OHS is required to comply with a series of other laws, which mandate that decisions be based on validated, job-related criteria; professional certifications have yet to be established as such criteria. OHS is committed to pursuing a variety of methods for verifying candidate and employee qualifications, including certifications, and will continue to update Congress on its findings.

Page 2

The draft report contained 30 recommendations to 13 agencies, two that were for OHS and with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously submitted 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 in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

Page 3

**Attachment: Management Response to Recommendations
Contained in GA0-18-466**

GAO recommended that the Secretary of Homeland Security:

Recommendation 1:

Conduct a baseline assessment of the Department's cybersecurity workforce that includes (1) the percentage of personnel with [information technology] IT, cybersecurity, or other cyber-related job functions who hold professional certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel. (Recommendation 7)

Response:

Concur. The DHS Office of the Chief Human Capital Officer (OCHCO) continues to collect data about professional certifications relevant to DHS cybersecurity work. In FY 2018, OCHCO worked with Components to source data about priority certifications, the number of employees that hold them, and the readiness of other employees to take certification exams. On April 30, 2018, DHS finalized three-digit coding of its federal cybersecurity positions, confirming a new baseline population of cybersecurity positions. During the remainder of FY 2018 and into early FY 2019, OCHCO plans to conduct a series of analyses with Components to review the population of three-digit coded positions, and finalize the percentage who hold certifications as well as the percentage prepared to take a relevant certification exam. In addition, OCHCO will identify and document strategies for mitigating any identified gaps. Estimated Completion Date (ECD): January 31, 2019.

Recommendation 2:

Submit a report of the Department's baseline assessment of its existing cybersecurity workforce to the appropriate congressional committees of jurisdiction. (Recommendation 8)

Response:

Concur. Upon final leadership review, OCHCO will send Congress a 2017 Comprehensive Cybersecurity Workforce Update report, which provides additional baseline information on the Department's cybersecurity workforce. In addition, OCHCO plans to leverage analysis during the remainder of FY 2018 and into early FY 2019 to produce an additional report for Congress, addressing the requirements of the baseline assessment. ECD: January 31, 2019.

Text of Appendix VI: Comments from the Department of the Interior

Page 1

Dear Mr. Powner:

Thank you for providing the Department of the Interior (Department) the opportunity to review and comment on the draft Government Accountability Office (GAO) report entitled, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions* (GAO-18-466). We appreciate GAO's review of the federal Cybersecurity Workforce.

The Department concurs with the recommendation stating, the Secretary of the Interior should evaluate the level of preparedness for cybersecurity personnel not currently holding professional certifications to take certification exams and report this information to Congress.

Also, the Department suggests that the third bullet on Page 24 be rewritten as follows, to accurately describe the current level of preparedness within the Department.

According to the Department officials, currently neither the U.S. Office of Personnel Management nor the Department requires certifications for these cybersecurity positions. However, the Department's Office of Human Resources and the Office of the Chief Information Officer are exploring options to determine the level of preparedness across its IT workforce. To that effect, the Department is updating its Learning Management System which will assist in tracking on-going requirements and identify baseline preparedness moving forward.

Please incorporate our comments when finalizing the report. If you have any questions or need additional information, please contact Sylvia Burns, Chief Information Officer at Sylvia_Burns@ios.doi.gov.

Sincerely,

Scott J. Cameron
Principal Deputy Assistant Secretary for Policy,
Management and Budget Exercising the Authority
of the Assistant Secretary for Policy, Management
and Budget

Text of Appendix VII: Comments from the Small Business Administration

Page 1

Dear Mr. Wilshusen:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled “Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions” (GAO-18-466).

The draft report measures agency progress in implementing requirements identified in the Federal Cybersecurity Workforce Assessment Act of 2015. SBA agrees with the recommendations made in the report and has made significant progress in the workforce assessment area. Specifically, SBA recently completed an assessment of the SBA’s IT workforce and reported on existing skills gaps. SBA plans to execute against the IT workforce plan to include addressing requirements within the Federal Cybersecurity Workforce Assessment Act of 2015. SBA looks forward to working with GAO to address the recommendations made in this report.

Thank you for the opportunity to comment on this report.

Sincerely

Maria Roat
Chief Information Officer

Text of Appendix VIII: Comments from National Aeronautics and Space Administration

Page 1

Dear Mr. Wilshusen:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, “Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions” (GAO-18-466), dated April 11, 2018.

In the draft report, GAO makes two recommendations to the NASA Administrator intended to improve compliance with requirements of the Federal Cybersecurity Workforce Assessment Act of 2015.

Specifically, GAO recommends the following:

Recommendation 1:

The Administrator of NASA should evaluate the level of preparedness for cybersecurity personnel not currently holding professional certifications to take certification exams and report this information to Congress.

Management’s Response:

Non-concur. There is no Federal or NASA requirement for employees in cybersecurity positions to hold and/or maintain a professional certification. Without this requirement, there is no plan to assess readiness of cybersecurity personnel to take certification exams. NASA provided the initial assessment to Congress in December 2016 and does not plan to repeat the assessment at this time.

Estimated Completion Date:

NIA

Recommendation 2:

The Administrator of NASA should include requirements to assign code “000” to positions that do not perform IT, cybersecurity, and cyber-related functions in agency procedures.

Page 2

Management's Response:

Concur. NASA will update current Agency procedures to document the change from the two-digit code of "00" to the new three-digit code of "000" for positions that do not perform cybersecurity or cybersecurity-related functions. The three-digit framework is available, and positions are being coded properly in our Electronic Position Description System (ePDS) and Federal Personnel Payroll System (FPPS) systems. Guidance is provided in the help buttons in ePDS, and supervisors and Human Resource Specialists have been trained on assigning cybersecurity codes or "000" to all positions. We will issue a new Personnel Bulletin documenting the above by May 18, 2018.

Estimated Completion Date:

May 18, 2018

Once again, thank you for the opportunity to comment on the subject draft report. If you have any questions or require additional information, please contact Heather Noiwan on (202) 358-2379.

Sincerely,

Renee P. Wynn
Chief Information Officer
Administrator for Human Capital Management

**Text of Appendix IX: Comments from the Nuclear
Regulatory Commission**

Page 1

Dear Director Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) Draft Audit Report: Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions (GAO-18-466), which was provided to the

U.S. Nuclear Regulatory Commission (NRG) on April 11, 2018. The NRC staff is in general agreement with the overall content of the draft audit report. However, the NRC staff requests that the evaluation of two factors for the NRG and their associated recommendations be updated in the final report to reflect our current condition. The draft report cited two of the seven factors, in reference to the Cybersecurity Coding Procedures, as incomplete for the NRC. The same two factors were cited as incomplete during the GAO exit conference on October 31, 2017. During this exit conference, we discussed the Engagement 101198: Statement of Facts and the Preliminary Findings, which assessed our progress toward completion of Cybersecurity Coding Procedures.

The first factor requires that procedures include language explaining that Information Technology (IT), Cybersecurity, and cyber-related positions will extend beyond the GG*-2210 IT occupational series. The second factor requires that the procedures outline the requirement that positions can be assigned up to three different codes and that these codes will be assigned in order of criticality. While these two factors are not required by the Office of Personnel Management, GAO felt strongly that they should be added. Therefore, the NRG Cybersecurity Coding Procedures were revised to incorporate the missing factors in November 2017 (see enclosed with revisions highlighted).

If you have any questions regarding the NRC's response, please contact John R. Jolicoeur by phone at (301) 415-1642 or by email at john.jolicoeur@nrc.gov.

Victor M. McCree
Executive Director for Operations

Enclosure:
NRG Cybersecurity Coding Procedures

Text of Appendix X: Comments from the United States
Agency for International Development

Page 1

Dear Mr. Wilshusen:

I am pleased to provide the fonnal response of the U.S. Agency for International Development(USAID) to the GAO draft report entitled,

“CYBERSECURITY WORKFORCE: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions” (GAO-18-466). USAID is providing this letter and enclosed comments for incorporation as an appendix to the GAO’s final report.

USAID is dedicated to maintaining its Government-leading cyber posture. Through the cooperative efforts of our Offices of Human Capital and Talent-Management (HCTM) and Chief Information Officer (CIO), USAID has completed all coding tasks recommended by the GAO. For reference, we have updated and enclosed our plan for coding cybersecurity positions, established to complete the original baseline.

Thank you for the opportunity to respond to the GAO’s draft report, and for the courtesies extended by your staff while conducting this engagement.

Sincerely,

Angelique M. Crumbly
Acting Assistant Administrator
Bureau Assistant Administrator
Bureau for Management

Enclosures: a/s

Page 2

COMMENTS FROM THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID) ON THE DRAFT REPORT PRODUCED BY THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) ENTITLED, “CYBERSECURITY WORKFORCE: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions” (GAO-18-466)

This report has four recommendations for USAID, as shown on page 38 of the draft report:

Recommendation 27:

The Administrator of USAID should fully clarify requirements to review all encumbered and vacant positions performing information-technology (IT) and cyber-related functions in agency procedures.

- USAID has taken action to close out the recommendation. In March 2018, the Agency updated our plan for coding cybersecurity positions, to include the procedures for reviewing all encumbered and vacant ones. USAID has completed this review, performed by the Office of the Chief Information Office (M/CIO) in the Bureau for Management and the Office of Human Capital and Talent-Management (HCTM).

Recommendation 28:

The Administrator of USAID should fully clarify requirements to annotate reviewed position descriptions with the appropriate cybersecurity data standard code(s) in agency procedures.

- USAID has taken action to close out the recommendation. The Agency has reviewed all occupied/vacant positions; identified IT, cybersecurity, and cyber-related positions; and assigned the three-digit codes accordingly. The positions include the following occupational series:

IT (2210), Computer Engineering (0854), Contracting Series (1102), Computer Science (1550), and Miscellaneous Administration and Program (0301).

Further, as is standard practice, M/CIO must provide the three-digit cybersecurity code in Section 24 (Remarks) of the Position Description (OF-8) for all positions that have IT; cybersecurity, and cyber-related functions. The USAID HCTM Human-Capital Service Center/Classification will update Section 24 (Remarks) of the OF-8 on all positions currently in existence.

Page 3

Recommendation 29:

The Administrator of USAID should include requirements to assign code “000” to positions that do not perform IT, cybersecurity, and cyber-related functions in agency procedures.

- USAID has taken action to close out the recommendation, and Table 4 on page 32 of the draft report does not accurately reflect the Agency’s progress in this area. On December 1, 2017, USAID assigned code 000 to all non-cyber positions in both HR Connect, a USAID corporate human-resource system, and the National Finance

Center (NFC) system, USAID's corporate payroll/personnel system. The GAO should mark this category in the table as "Fully Addressed."

Recommendation 30:

The Administrator of USAID should include requirements to assign up to three employment codes per position in order of their criticality in agency procedures.

- USAID has taken action to close out the recommendation. In March 2018, USAID updated its plan for coding cybersecurity positions to include procedures on functional coding. When a position aligns with more than one functional area, the Agency codes the predominant functional area first, and will add any others where and when necessary. In April 2018, USAID completed all coding for both encumbered and vacant cybersecurity positions.

Text of Appendix XI: Comments from the Social Security Administration

Page 1

Dear Mr. Wilshusen:

Thank you for the opportunity to review the draft report, "CYBERSECURITY WORKFORCE: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions" (GAO-18-466). We are pleased that GAO concluded that, in December 2016, we reported to Congress the required elements in our baseline assessment, as required by the Federal Cybersecurity Workforce Assessment Act of 2015. Additionally, in April 2017, as required by guidance released in January 2017 by the Office of Personnel Management, we established and issued coding procedures to identify and assign codes to cybersecurity positions. We have no further comment.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall
Acting Deputy Chief of Staff

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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