United States Government Accountability Office

Report to Congressional Committees

March 2019

CYBERSECURITY WORKFORCE

Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs

GAO

Highlights

Highlights of GAO-19-144, a report to congressional committees

March 2019

CYBERSECURITY WORKFORCE

Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs

Why GAO Did This Study

A key component of mitigating and responding to cyber threats is having a qualified, well-trained cybersecurity workforce. The act requires OPM and federal agencies to take several actions related to cybersecurity workforce planning. These actions include categorizing all IT, cybersecurity, and cyber-related positions using OPM personnel codes for specific work roles, and identifying critical staffing needs.

The act contains a provision for GAO to analyze and monitor agencies' workforce planning. GAO's objectives were to (1) determine the extent to which federal agencies have assigned work roles for positions performing IT, cybersecurity, or cyber-related functions and (2) describe the steps federal agencies took to identify work roles of critical need. GAO administered a questionnaire to 24 agencies, analyzed coding data from personnel systems, and examined preliminary reports on critical needs. GAO selected six of the 24 agencies based on cybersecurity spending levels to determine the accuracy of codes assigned to a random sample of IT positions. GAO also interviewed relevant OPM and agency officials.

What GAO Recommends

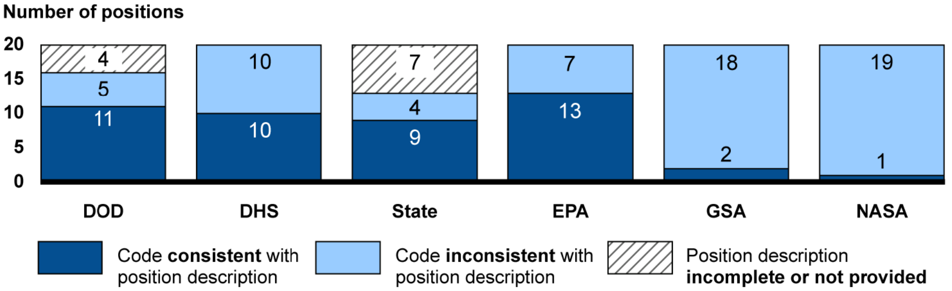
GAO is making 28 recommendations to 22 agencies to review and assign the appropriate codes to their IT, cybersecurity, and cyber-related positions. Of the 22 agencies to which GAO made recommendations, 20 agreed with the recommendations, one partially agreed, and one did not agree with one of two recommendations. GAO continues to believe that all of the recommendations are warranted.

View GAO-19-144. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

What GAO Found

The 24 reviewed federal agencies generally assigned work roles to filled and vacant positions that performed information technology (IT), cybersecurity, or cyber-related functions as required by the *Federal Cybersecurity Workforce Assessment Act of 2015* (the act). However, six of the 24 agencies reported that they had not completed assigning the associated work role codes to their vacant positions, although they were required to do so by April 2018. In addition, most agencies had likely miscategorized the work roles of many positions. Specifically, 22 of the 24 agencies assigned a "non-IT" work role code to 15,779 (about 19 percent) of their IT positions within the 2210 occupational series. Further, the six agencies that GAO selected for additional review had assigned work role codes that were not consistent with the work roles and duties described in corresponding position descriptions for 63 of 120 positions within the 2210 occupational series that GAO examined (see figure).

Consistency of Assigned Work Role Codes with Position Descriptions for Random Sample of IT Positions Within the 2210 Occupational Series at Six Selected Agencies



DOD (Department of Defense), DHS (Department of Homeland Security), State (Department of State), EPA (Environmental Protection Agency), GSA (General Services Administration), NASA (National Aeronautics and Space Administration),

Source: GAO analysis of DOD, DHS, State, NASA, EPA and GSA cybersecurity coding data. | GAO-19-144

Human resource and IT officials from the 24 agencies generally reported that they had not completely or accurately categorized work roles for IT positions within the 2210 occupational series, in part, because they may have assigned the associated codes in error or had not completed validating the accuracy of the assigned codes. By assigning work roles that are inconsistent with the IT, cybersecurity, and cyber-related positions, the agencies are diminishing the reliability of the information they need to improve workforce planning.

The act also required agencies to identify work roles of critical need by April 2019. To aid agencies with identifying their critical needs, the Office of Personnel Management (OPM) developed guidance and required agencies to provide a preliminary report by August 2018. The 24 agencies have begun to identify critical needs and submitted a preliminary report to OPM that identified information systems security manager, IT project manager, and systems security analyst as the top three work roles of critical need. Nevertheless, until agencies accurately categorize their positions, their ability to effectively identify critical staffing needs will be impaired.

Contents

Letter 1

Background 6
Agencies Generally Categorized Positions, but Did Not Ensure the Reliability of Their Efforts 14
OPM and Agencies Had Taken Steps to Identify IT, Cybersecurity, and Cyber-related Work Roles of Critical Need 24
Conclusions 29
Recommendations for Executive Action 30
Agency Comments and Our Evaluation 33

Appendix I Objectives, Scope, and Methodology 42

Appendix II Office of Personnel Management Information Technology, Cybersecurity, and Cyber-related Work Role Codes 47

Appendix III Summary of 24 Chief Financial Officers Act Agencies' Implementation of the Federal Cybersecurity Workforce Assessment Act of 2015, as of Nov. 2018 53

Appendix IV Top 12 Work Roles of Critical Need as Identified by the 24 Chief Financial Officers (CFO) Act Agencies in Their Preliminary Reports of Critical Need 55

Appendix V Comments from the Department of Commerce 56

Appendix VI Comments from the Department of Defense 57

Appendix VII Comments from the Department of Education 59

Appendix VIII	Comments from the Department of Energy	60
Appendix IX	Comments from the Department of Health and Human Services	62
Appendix X	Comments from the Department of Homeland Security	64
Appendix XI	Comments from the Department of the Interior	67
Appendix XII	Comments from the Department of Labor	68
Appendix XIII	Comments from the Department of State	69
Appendix XIV	Comments from the Department of Veterans Affairs	71
Appendix XV	Comments from the Environmental Protection Agency	73
Appendix XVI	Comments from the General Services Administration	75
Appendix XVII	Comments from the Nuclear Regulatory Commission	77
Appendix XVIII	Comments from the Office of Personnel Management	78
Appendix XIX	Comments from the Small Business Administration	79

Appendix XX Comments from the Social Security Administration 80

Appendix XXI Comments from the National Aeronautics and Space Administration 82

Appendix XXII Comments from the United States Agency for International Development 84

Appendix XXIII GAO Contact and Staff Acknowledgments 85

Tables

Table 1: Status of Federal Agencies' Implementation of Six Selected Activities Required by the *Federal Cybersecurity Workforce Assessment Act of 2015*, as of October 2018 14

Table 2: Status of Federal Agencies' Efforts to Assign Work Roles to Positions as Required by the *Federal Cybersecurity Workforce Assessment Act of 2015*, as of October 2018 15

Table 3: The Number and Percentage of 2210 IT Management Positions Assigned Work Role Code "000" by the 24 CFO Act Agencies, According to OPM's Enterprise Human Resources Integration Data, as of May 2018 19

Table 4: Random Sample of Work Role Coded IT Positions within the 2210 Occupational Series Compared with Position Descriptions Duties 22

Table 5: Status of Federal Agencies' Implementation of Selected Activities to Identify Work Roles of Critical Need as Required by the *Federal Cybersecurity Workforce Assessment Act of 2015*, as of November 2018 25

Table 6: Submission Status of Preliminary Reports on Cybersecurity Work Roles of Critical Need by the 24 CFO Act Agencies as of November 2018 28

Table 7: Office of Personnel Management (OPM) Federal Information Technology, Cybersecurity, and Cyber-related Work Role Codes 47

Table 8: Federal Chief Financial Officer (CFO) Act Agencies' Implementation of the *Federal Cybersecurity Workforce Assessment Act of 2015* Requirements, as of November 2018 53
Table 9: Top 12 Preliminary Work Roles of Critical Need Reported by the 24 CFO Act Agencies as of November 2018 55

Figures

Figure 1: National Initiative for Cybersecurity Education Cybersecurity Workforce Framework Categories and Specialty Areas (NIST SP 800-181, August 2017) 8
Figure 2: Specialty Areas and Work Roles Defined in the "Securely Provision" Cybersecurity Workforce Framework Category, August 2017 9

Abbreviations

Agriculture	Department of Agriculture
CFO	Chief Financial Officers
Commerce	Department of Commerce
DHS	Department of Homeland Security
DOD	Department of Defense
Education	Department of Education
Energy	Department of Energy
EPA	Environmental Protection Agency
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
IT	information technology
Interior	Department of the Interior
Justice	Department of Justice
Labor	Department of Labor
NASA	National Aeronautics and Space Administration
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SBA	Small Business Administration
SSA	Social Security Administration
State	Department of State
Transportation	Department of Transportation
Treasury	Department of the Treasury
USAID	U.S. Agency for International Development
VA	Department of Veterans Affairs

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.

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

March 12, 2019

Congressional Committees

The security of federal information systems and data is critical to the nation's safety, prosperity, and well-being. However, federal systems and networks are inherently at risk because of their complexity, technological diversity, and geographic dispersion. Further, threats to federal information technology (IT) infrastructure continue to grow in number and sophistication, posing a risk to the reliable functioning of our government.

A key component of the government's ability to mitigate and respond to cybersecurity 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 IT systems. However, skills gaps in personnel who perform IT, cybersecurity, or other cyber-related functions may impede the federal government from protecting information systems and data that are vital to the nation.

We and other organizations have previously reported that federal agencies face challenges in ensuring that they have an effective cybersecurity workforce.[1] 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.[2]

In 2001, we added strategic human capital management to our high-risk list, and reported that human capital shortfalls are eroding the ability of some agencies to perform their core missions.[3] In addition, in our 2017 update to the high-risk list, we reported that the federal government continued to face challenges in addressing mission critical skills gaps,

[1] The 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) and RAND Corporation, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (2014).

[2] GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

[3] GAO, *High-Risk Series: An Update,* GAO-01-263 (Washington, D.C.: Jan. 1, 2001).

including cybersecurity skills gaps.[4] Further, in September 2018, we reported that effective cybersecurity workforce management was a critical action for addressing cybersecurity challenges facing the nation.[5]

To address the cybersecurity skills gaps within the executive branch of the federal government, the *Federal Cybersecurity Workforce Assessment Act of 2015* (the act) 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.[6] Among other things, the act requires:

- OPM, in coordination with NIST, to develop a cybersecurity coding structure that aligns with the work roles[7] identified in the *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*,[8] for agencies to identify and categorize all federal IT, cybersecurity, and cyber-related positions.
- Federal agencies to complete the assignment of work role codes to their filled and vacant IT, cybersecurity, or cyber-related positions that perform these functions.[9]
- Federal agencies to identify their IT, cybersecurity, or cyber-related work roles of critical need in the workforce and submit a report describing these needs to OPM.

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

[5] GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[6] The *Federal Cybersecurity Workforce Assessment Act of 2015* was enacted as part of the *Consolidated Appropriations Act, 20*16, Pub. L. No. 114-113, Div. N, Title III, sec. 301 (Dec. 18, 2015) 129 Stat. 2242, 2975-77.

[7] Work roles provide a description of the roles and responsibilities of IT, cybersecurity, or cyber-related job functions.

[8] NIST, which heads NICE, issued the *NICE Cybersecurity Workforce Framework* in August 2017, to describe IT, cybersecurity, or cyber-related work roles and positions. The cybersecurity coding structure identifies a unique numeric code for each of the 52 work roles and 33 specialty areas defined in the framework.

[9] Our use of the term “position” refers to positions that are filled by an employee or are vacant. For the purposes of this report, we will refer to encumbered positions as “filled” positions.

The act also includes a provision for us to review the agencies' implementation of these requirements and report on our assessment to Congress. Toward this end, in June 2018, we issued an initial report on agencies' efforts to implement selected activities that the act required them to complete by November 2017.[10] In that report, we made 30 recommendations to 13 agencies to develop and submit their baseline assessment reports and to fully address the required activities in OPM's guidance in their procedures for assigning work role codes to their civilian IT, cybersecurity, or cyber-related positions.

This second report addresses agencies' efforts in implementing selected additional activities required by the act. Specifically, our objectives for this report were to (1) determine the extent to which federal agencies have assigned work role codes to positions performing IT, cybersecurity, or cyber-related functions and (2) describe the steps federal agencies took to identify work roles of critical need. The scope of our review included the 24 major departments and agencies covered by the *Chief Financial Officers (CFO) Act of 1990*.[11]

To address our objectives, we administered a questionnaire to the 24 CFO Act agencies to obtain information on their efforts in assigning work role codes to positions performing IT, cybersecurity, or cyber-related functions, and in identifying work roles of critical need. We reviewed and analyzed the agencies' responses to the questionnaire in comparison to the act's requirements, OPM guidance, and the *NICE Cybersecurity Workforce Framework* (framework). We also obtained, reviewed, and analyzed reports and other documents supporting questionnaire responses to assess whether agencies assigned codes in accordance with OPM's coding guidance.

Further, to analyze the extent to which federal agencies have assigned work role codes to positions performing IT, cybersecurity, or cyber-related

[10] GAO, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions,* GAO-18-466 (Washington, D.C.: June 14, 2018).

[11] The 24 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; 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)).

functions, we obtained workforce data for the 24 agencies from OPM's Enterprise Human Resources Integration system.[12] We reviewed this collection of data to determine its completeness and to determine the number of positions in the 2210 IT management occupational series[13] to which the 24 agencies had assigned the code of "000" as of May 2018.[14] We reviewed positions from the 2210 IT management series because, based on the definition of the series, these positions are most likely to perform IT, cybersecurity, or cyber-related functions.[15]

We then identified a subset of the 24 agencies and performed an additional review of these agencies' work role coding efforts. We selected these agencies based on their total cybersecurity spending for fiscal year 2016, as reported by the Office of Management and Budget (OMB) in its *Federal Information Security Modernization Act* annual report.[16] We sorted the 24 agencies' IT cybersecurity spending from highest to lowest and then divided the agencies into three equal groups of high, medium, and low cybersecurity spending. We then selected the top two agencies from each group. Based on these factors, we selected six agencies: the (1) Department of Defense (DOD), (2) Department of Homeland Security (DHS), (3) Department of State (State), (4) National Aeronautics and

[12] The Enterprise Human Resources Integration Data Warehouse is a centralized collection of federal workforce data that includes the work role codes that agencies assigned to their workforce positions.

[13] According to OPM, an occupational series is a grouping of positions with a similar line of work and qualification requirements. For example, the 2210 IT management occupational series covers positions that manage, supervise, lead, administer, develop, deliver, and support information technology systems and services. This series covers positions for which the paramount requirement is knowledge of IT principles, concepts, and methods; e.g., data storage, software applications, networking. For the purposes of this report, we also refer to the 2210 IT management occupational series as 2210 IT management positions.

[14] The code of "000" designates positions that do not perform IT, cybersecurity, or cyber-related functions.

[15] Office of Personnel Management, *Job Family Standard for Administrative Work in the Information Technology Group, 2200*, (Washington, D.C.: May 2011), and *Interpretive Guidance for the Information Technology Management Series, GS-2210* (Washington, D.C.: June 2001).

[16] Office of Management and Budget (OMB), *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, Fiscal Year 2016 (Washington, D.C.: March 10, 2017). At the start of the engagement, OMB's fiscal year 2016 data was the most current available.

Space Administration (NASA), (5) Environmental Protection Agency (EPA), and (6) General Services Administration (GSA).

We randomly selected a sample of 20 positions from each of the six selected agencies (120 total positions) within the 2210 IT management occupational series. We also selected a second nonstatistical sample of 12 positions for each of the six agencies (72 total positions) from the 2210 IT management occupational series based on pairs of positions that had identical position titles, occupational series, and sub-agencies, but for which the agencies had assigned different work role codes for the positions.[17] For the selected positions, we reviewed the work role coding data from the agencies' human resources systems and compared them to the duties described in the corresponding position descriptions to determine whether agencies had assigned work role codes that were consistent with the duties described in the position descriptions.[18]

To address our second objective, we evaluated OPM's and agencies' actions to identify IT, cybersecurity, or cyber-related work roles of critical need. To do this, we obtained and analyzed OPM's progress report to Congress and its guidance for identifying critical needs by comparing the contents of these documents to the act's requirements. We also reviewed any available documentation from the 24 agencies on their progress in identifying critical needs, such as project plans or preliminary critical needs reports. We supplemented our analysis with interviews of the agencies' human capital and IT officials regarding their progress in assigning work role codes and identifying critical needs. Appendix I provides a full description of our objectives, scope, and methodology.

We conducted this performance audit from February 2018 to March 2019 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

[17] We selected these examples to examine why agencies assigned different codes to similar positions. For example, two positions could have identical position titles, occupational series, and sub-agencies, but one position was assigned a work role code while the other was assigned a code designated for positions that do not perform IT, cybersecurity, or cyber-related functions (i.e., "000").

[18] Agencies used their human resources systems to record work role codes for their positions and to track employee data along with position data.

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.

A resilient, well-trained, and dedicated cybersecurity workforce is essential to protecting federal IT systems. Nevertheless, OMB and our prior reports have pointed out that the federal government and private industry face a persistent shortage of cybersecurity and IT professionals to implement and oversee information security protections to combat cyber threats.

As we noted in our prior report, the RAND Corporation[19] and the Partnership for Public Service have reported on a nationwide shortage of cybersecurity experts in the federal government.[20] According to these reports, the existing shortage of cybersecurity professionals makes securing the nation's networks more challenging and may leave federal IT systems vulnerable to malicious attacks. The persistent shortage of cyber-related workers has given rise to the identification and assessment of the federal cybersecurity workforce across agencies so that efforts to increase the number of those workers can be applied in the most efficient and accurate manner.

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

[20] The 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).

The NICE Framework and OPM Coding Structure Describe Federal Cybersecurity Work Roles

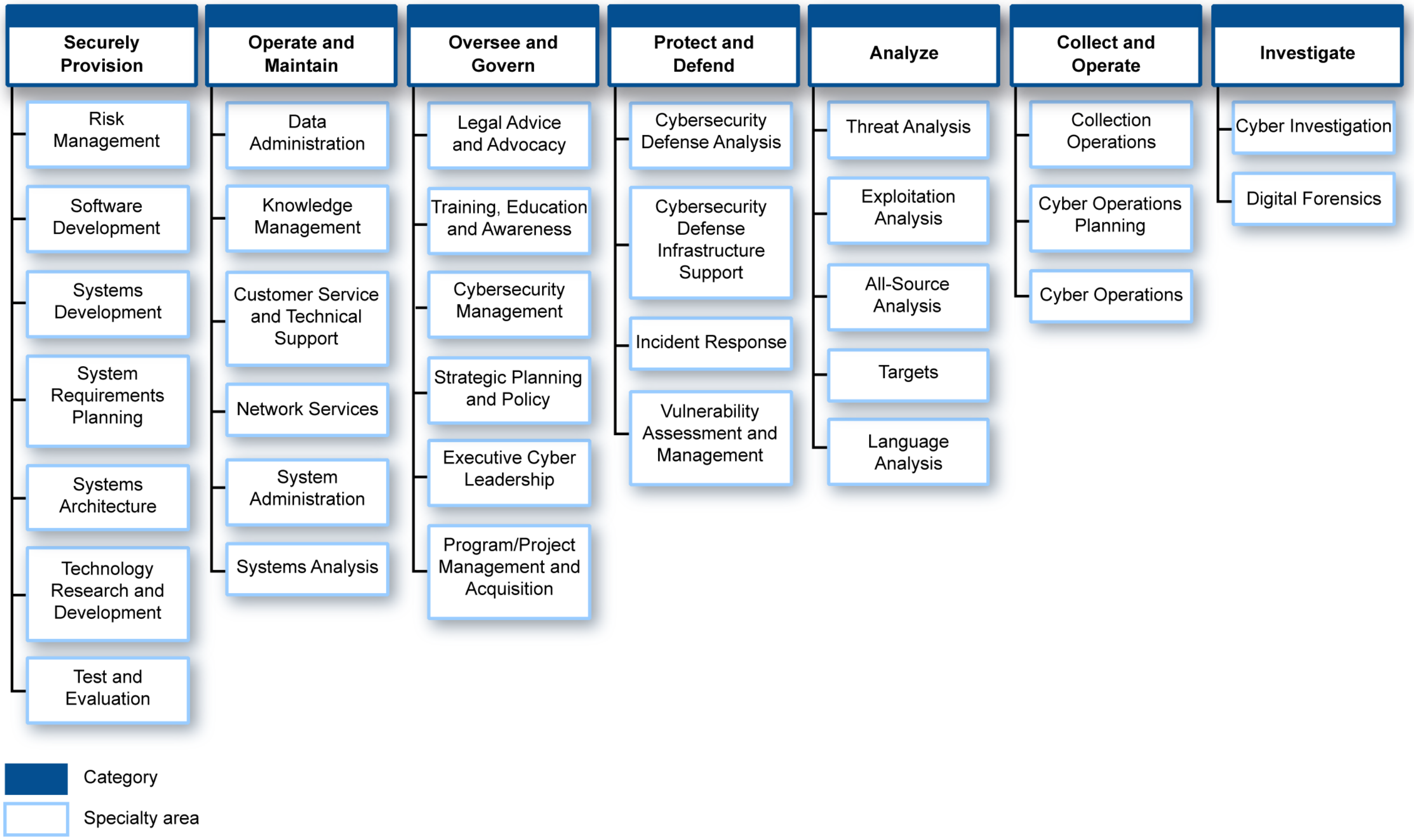
NIST coordinates the National Initiative for Cybersecurity Education (NICE) partnership among government, academia, and the private sector. The initiative's goal is to improve cybersecurity education, awareness, training, and workforce development in an effort to increase the number of skilled cybersecurity professionals.

In August 2017, NIST revised and published the *NICE Cybersecurity Workforce Framework* (framework).[21] The framework's purpose is to help the federal government better understand the breadth of cybersecurity work by describing IT, cybersecurity, and cyber-related work roles associated with the categories and specialty areas that make up cybersecurity work. The framework organizes IT, cybersecurity, and cyber-related job functions into categories, representing high-level groupings of cybersecurity functions; and into specialty areas, representing areas of concentrated work or functions.

Figure 1 identifies the seven categories and the 33 specialty areas in the NICE framework.

[21] National Institute of Standards and Technology, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, SP 800-181 (Gaithersburg, Md.: August 2017). NICE issued the previous version of the framework, called the *National Cybersecurity Workforce Framework*, in April 2013.

Figure 1: National Initiative for Cybersecurity Education Cybersecurity Workforce Framework Categories and Specialty Areas (NIST SP 800-181, August 2017)

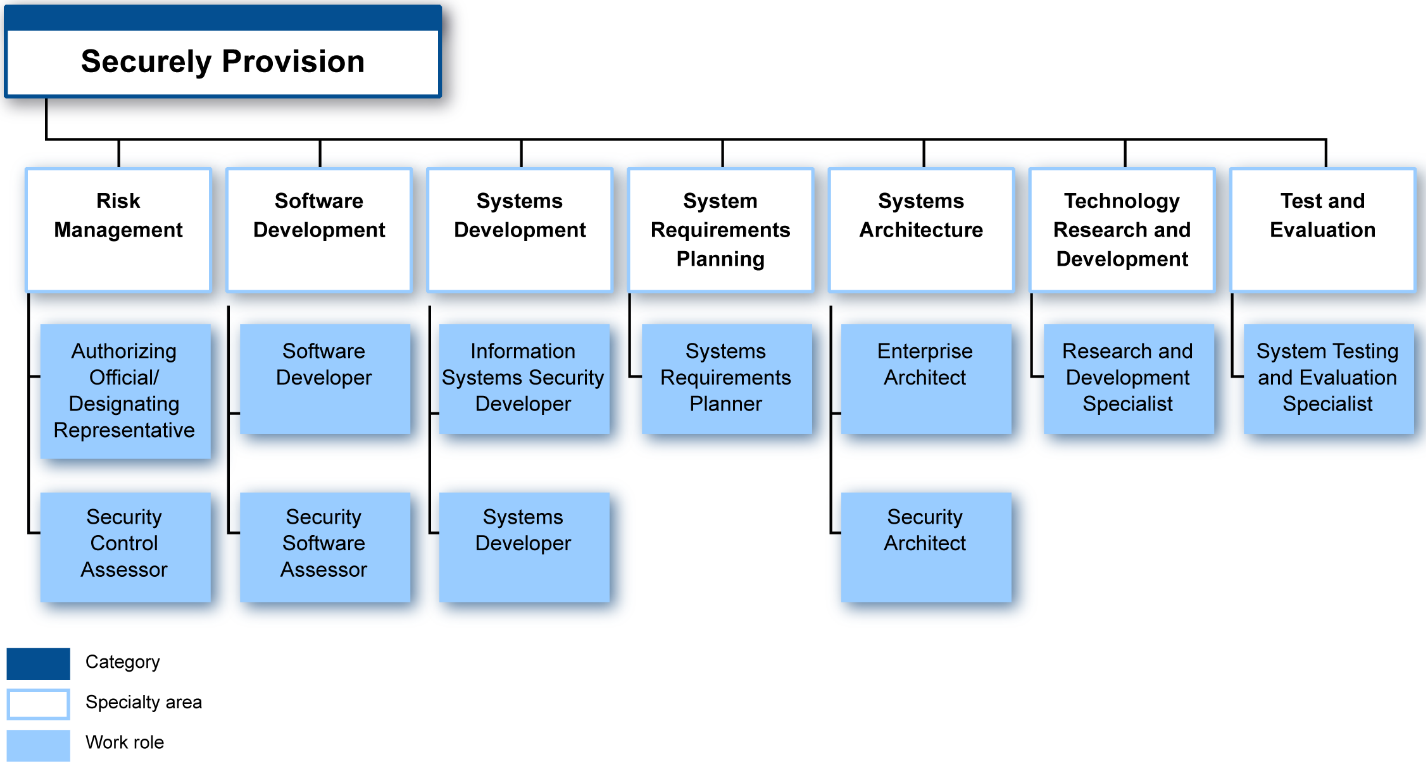


Source: GAO analysis of National Institute of Standards and Technology, *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*, SP-800-181. | GAO-19-144

In addition to categories and specialty areas, the NICE framework introduced the concept of work roles. Work roles provide a more detailed description of the roles and responsibilities of IT, cybersecurity, and cyber-related job functions than do the category and specialty area components of the framework. The framework defines one or more work roles within each specialty area. For example, as depicted in figure 2, the framework defines 11 work roles within the seven specialty areas of the

“Securely Provision” category.[22] In total, the framework defines 52 work roles across the 33 specialty areas.

Figure 2: Specialty Areas and Work Roles Defined in the “Securely Provision” Cybersecurity Workforce Framework Category, August 2017


Securely Provision
Risk Management
Authorizing Official/ Designating Representative
Security Control Assessor
Software Development
Software Developer
Security Software Assessor
Systems Development
Information Systems Security Developer
Systems Developer
System Requirements Planning
Systems Requirements Planner
Systems Architecture
Enterprise Architect
Security Architect
Technology Research and Development
Research and Development Specialist
Test and Evaluation
System Testing and Evaluation Specialist
Category
Specialty area
Work role

Source: GAO analysis of National Institute of Standards and Technology, *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*, SP-800-181. | GAO-19-144

The NICE framework work roles include, among others, the Technical Support Specialist, IT Project Manager, and Software Developer. The framework identifies these IT, cybersecurity, and cyber-related work roles as essential functions. For example, a Technical Support Specialist may have a role in identifying the occurrence of a cybersecurity event, an IT Project Manager may need to manage cybersecurity risk to systems, and

[22] The 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.

a Software Developer may need to implement appropriate cybersecurity safeguards.

In October 2017, OPM updated the federal cybersecurity coding structure to incorporate the work roles identified in the NICE framework.[23] The coding structure assigned a unique 3-digit cybersecurity code to each work role, which supplanted the prior coding structure's 2-digit codes.[24] According to OPM, the coding of federal positions with these specific 3-digit work role codes is intended to enhance agencies' ability to identify critical IT, cybersecurity, and cyber-related workforce needs, recruit and hire employees with needed skills, and provide appropriate training and development opportunities to cybersecurity employees. Appendix II provides a summary of the IT, cybersecurity, and cyber-related work roles and corresponding OPM codes.

Federal Cybersecurity Workforce Assessment Act of 2015 Establishes Workforce Planning Requirements

In 2015, Congress and the President enacted the *Federal Cybersecurity Workforce Assessment Act*, which required OPM, NIST, and other federal agencies to undertake a number of cybersecurity workforce-planning activities. The act required these agencies to complete the activities within specified time frames. We addressed the first six activities in our prior report we issued in June 2018, and addressed the subsequent activities 7 through 10 in this report.[25]

Among the required cybersecurity workforce-planning activities are the following 10 that we selected for our review.

1. OPM, in coordination with NIST, was to develop a cybersecurity coding structure that aligns with the work roles identified in the NICE Cybersecurity Workforce Framework. (Due June 2016)
2. OPM was to establish procedures to implement a cybersecurity coding structure to identify all federal civilian positions that require the performance of IT, cybersecurity, or other cyber-related functions. (Due September 2016)

[23] Office of Personnel Management, *Federal Cybersecurity Coding Structure*, version 2.0, (October 18, 2017).

[24] In October 2012, OPM published the initial cybersecurity employment coding structure that assigned a unique 2-digit cybersecurity employment code to each category and specialty area aligned with the initial version of the *National Cybersecurity Workforce Framework*.

[25] GAO-18-466.

3. OPM was to submit a report to Congress on the progress that agencies made in identifying and assigning codes to their positions that perform IT, cybersecurity, or cyber-related functions. (Due June 2016)
4. Each federal agency was to submit a report to Congress on its baseline assessment and on the extent to which its employees who perform IT, cybersecurity, or cyber-related functions held certifications. (Due December 2016)
5. Each federal agency was to establish procedures to identify all filled and vacant IT, cybersecurity, or cyber-related positions and assign the appropriate code to each position. (Due April 2017 for civilian positions)
6. The Department of Defense (DOD) was to establish procedures to implement the cybersecurity coding structure to identify all federal noncivilian (i.e., military) positions. (Due June 2017)
7. Each agency was to complete the assignment of work role codes to its filled and vacant positions that perform IT, cybersecurity, or cyber-related functions. (Due April 2018 for civilian positions)
8. OPM was to identify critical needs across federal agencies and submit a progress report to Congress on the identification of critical needs. (Due December 2017)
9. OPM was to provide federal agencies with timely guidance for identifying IT, cybersecurity, or cyber-related work roles of critical need, including work roles with acute and emerging skill shortages. (The act did not specify a due date for this requirement).
10. Federal agencies were to identify their IT, cybersecurity, or cyber-related work roles of critical need in the workforce and submit a report describing these needs to OPM. (Due April 2019)

Prior GAO Report Examined Agencies' Implementation of the Initial Activities Required by the Federal Cybersecurity Workforce Assessment Act of 2015

In June 2018, we reported on federal agencies' implementation of the first six of the 10 selected activities required by the *Federal Cybersecurity Workforce Assessment Act*.[26] Specifically, we reported that, in November 2016, OPM, in coordination with NIST, had issued a cybersecurity coding structure that aligned with the NICE framework work roles (activity 1). Also, these two agencies developed procedures for assigning codes to federal civilian IT, cybersecurity, or cyber-related positions in January 2017 (activity 2). We noted that OPM had issued the cybersecurity coding structure and procedures later than the act's deadlines because it was working with NIST to align the structure and procedures with the draft version of the *NICE Cybersecurity Workforce Framework*, which NIST issued later than planned. Regarding activity 3, we noted that OPM had submitted a report to Congress in July 2016 on the agencies' progress in implementing the act's required activities, as well as OPM's efforts to develop a coding structure and government-wide coding procedures.

We also reported that 21 of the 24 agencies had submitted baseline assessment reports identifying the extent to which their IT, cybersecurity, or cyber-related employees held professional certifications (activity 4). However, the three other agencies had not submitted such reports. In addition, four agencies did not include all reportable information in their reports, such as the extent to which personnel without certifications were ready to obtain them, or strategies for mitigating any gaps, as required by the act. We made 10 recommendations to these seven agencies to develop and submit baseline assessment reports, including all reportable information, to the congressional committees. As of February 2019, none of the seven agencies had implemented any of the 10 recommendations relating to the baseline assessment reports.[27]

Further, we reported that 23 of the 24 agencies had established procedures for assigning the appropriate work role codes to civilian positions that perform IT, cybersecurity, or cyber-related functions

[26] GAO-18-466.

[27] One agency, NASA, did not concur with our recommendation because there is no federal or NASA requirement for employees in positions performing IT, cybersecurity, or cyber-related functions to hold and/or maintain a professional certification.

(activities 5 and 6 above), as required by the act. One agency had not established such procedures.[28]

Further, of the 23 agencies that had established procedures, 6 agencies did not address one or more of seven activities required by OPM in their procedures. For example, the agencies' procedures did not include activities to review all filled and vacant positions and annotate reviewed position descriptions with the appropriate work role code. In addition, DOD had not established procedures for identifying and assigning work role codes to noncivilian (i.e., military) positions.

Our June 2018 report included 20 recommendations to eight agencies to establish or update their procedures to fully address the required activities in OPM's guidance. Subsequent to the report, the eight agencies implemented the 20 recommendations related to establishing or improving agencies' coding procedures to address the required OPM activities. Specifically:

- The Department of Energy (Energy) established coding procedures that addressed the seven OPM required activities.
- The Department of Education (Education), Department of Labor (Labor), NASA, National Science Foundation (NSF), Nuclear Regulatory Commission (NRC), and United States Agency for International Development (USAID) revised their procedures to ensure that the procedures addressed OPM's required activities.
- DOD established a consolidated government-wide and internal procedure for identifying and assigning work role codes to noncivilian (i.e., military) positions.

Table 1 summarizes the status of agencies' implementation of the first six selected activities required by the act as of October 2018. We initially reported on the status of these activities in our June 2018 report.[29]

[28] At the time that we issued our June 2018 report (GAO-18-466), the Department of Energy had not established procedures for identifying and assigning codes to its positions performing IT, cybersecurity, or cyber-related functions.

[29] GAO-18-466.

Table 1: Status of Federal Agencies' Implementation of Six Selected Activities Required by the *Federal Cybersecurity Workforce Assessment Act of 2015*, as of October 2018

Required activity	Due date	Actual completion date	Status of activity
1) OPM, in coordination with NIST, is to develop a cybersecurity coding structure that aligns with the work roles identified in the NICE Cybersecurity Workforce Framework.	June 2016	November 2016	Completed, but delayed by five months due to delay in NIST issuance of the NICE framework.
2) OPM is to establish procedures to implement the cybersecurity coding structure to identify all federal civilian positions that require the performance of IT, cybersecurity, or cyber-related functions.	September 2016	January 2017	Completed, but delayed by four months due to delay in NIST issuance of the NICE framework.
3) OPM is to submit a progress report on the implementation of the identification of IT, cybersecurity, or cyber-related positions and assignment of codes to positions.	June 2016	July 2016	Completed, but delayed by one month.
4) Each federal agency is to submit a report of its baseline assessment of the extent to which IT, cybersecurity, or cyber-related employees held certifications.	December 2016	Ongoing	21 of 24 agencies submitted reports, but three agencies had not submitted reports and four agencies had not addressed all of the reportable information as of October 2018.
5) Each federal agency is to establish procedures to identify all filled and vacant IT, cybersecurity, or cyber-related positions and assign the appropriate code to each position.	April 2017	24 of 24 agencies had established procedures as of August 2018	We made 20 recommendations to eight agencies to fully address this activity. The eight agencies implemented all 20 recommendations.
6) DOD is to establish procedures to implement the cybersecurity coding structure to identify all federal military positions	June 2017	June 2018	Completed, but delayed by one year.

Source: GAO analysis of agency procedures for identifying and assigning work role codes to positions from February-October 2018, and GAO-18-466. | GAO-19-144.

Agencies Generally Categorized Positions, but Did Not Ensure the Reliability of Their Efforts

Regarding the selected activity for agencies to complete the assignment of work role codes to filled and vacant positions that perform IT, cybersecurity, or cyber-related functions (activity 7) as set forth in the *Federal Cybersecurity Workforce Assessment Act of 2015*, the 24 agencies had generally assigned work roles code to their positions. However, several agencies had not completed assigning codes to their vacant positions. In addition, most agencies had likely miscategorized the work roles of many positions. For example, in these instances, the agencies had assigned a code designated for positions that do not perform IT, cybersecurity, or cyber-related functions to positions that most likely perform these functions.

As indicated in table 2, federal agencies' efforts to assign work role codes to filled and vacant positions that performed IT, cybersecurity, or cyber-related functions were ongoing as of October 2018.

Table 2: Status of Federal Agencies' Efforts to Assign Work Roles to Positions as Required by the *Federal Cybersecurity Workforce Assessment Act of 2015*, as of October 2018

Required activity	Due date	Actual completion date	Status of activity
7) Federal agencies are to complete the assignment of work role codes to filled and vacant positions that perform IT, cybersecurity, or cyber-related functions.	April 2018	Ongoing	As of October 2018, all 24 agencies had assigned work role codes to filled positions; however, six agencies had not completed assigning codes to their vacant positions. In addition, 22 of 24 agencies had assigned a work role code designated for positions not performing IT, cybersecurity, or cyber-related functions to many positions that most likely performed these functions.

Source: GAO analysis of agency efforts to assign work role codes to workforce positions. | GAO-19-144.

Agencies Had Generally Assigned Work Role Codes to Positions, but Six Had Not Completely Coded Vacant Positions

To assist agencies with meeting their requirements under the *Federal Cybersecurity Workforce Assessment Act of 2015*, OPM issued guidance that directed agencies to identify filled and vacant positions with IT, cybersecurity, or cyber-related functions and assign work role codes to those positions using the Federal Cybersecurity Coding Structure by April 2018.[30] As previously mentioned, this coding structure designates a unique 3-digit code for each work role defined in the NICE framework. According to OPM's guidance, agencies could assign up to three work role codes to each position, and should assign the code of "000" only to positions that did not perform IT, cybersecurity, or cyber-related functions.

The 24 agencies generally had assigned work role codes to their filled workforce positions that performed IT, cybersecurity, or cyber-related functions. Specifically, 22 of the agencies responded to our questionnaire that, as of April 2018, they had completed assigning work role codes to those filled positions.[31] In addition, data from the OPM Enterprise Human

[30] Office 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).

[31] DOD and the Department of Health and Human Services reported they had not completed the identification and coding of positions performing IT, cybersecurity, or cyber-related functions as of April 2018.

Resources Integration system showed that, as of May 2018, the 24 agencies had collectively assigned work role codes or a “000” code to over 99 percent of the filled positions in their entire workforce.

In addition, 18 of the 24 agencies reported they had identified and assigned codes to their vacant IT, cybersecurity, or cyber-related positions by April 2018. However, the remaining six agencies reported that they were not able to identify or assign codes to all of their vacant positions. For example, four agencies—DOD, EPA, GSA, and NASA—responded to our questionnaire that they did not identify and assign codes to vacant IT, cybersecurity, or cyber-related positions.

- DOD reported that, while some components assigned codes to vacant positions, the department did not have an enterprise-wide capability to assign codes to vacant positions and had not modified the systems to enable the use of the 3-digit work role codes for vacant positions due to time and funding constraints.
- EPA reported that it had assigned codes to vacant positions in April 2018, but it did not have a process for assigning codes to newly created vacant positions.
- GSA human resources officials said that they assigned codes to vacant positions that had been authorized and funded. However, they did not code unfunded vacant positions because they did not anticipate filling them. Agency officials noted that they, instead, tracked unfunded vacant positions through staffing plans.
- NASA human resources and Office of the Chief Information Officer officials said the agency did not identify and code vacant positions because they did not track vacant positions.

Further, the remaining two agencies—Energy and Justice— stated that they could not provide data regarding the number of vacant IT, cybersecurity, or cyber-related positions that had been identified and coded. For example, Justice said that information on vacant positions was not available through its human resources system, and that it would need to send a data call to components to obtain information on the number of vacancies with an assigned work role code. However, according to management division officials, the department would need additional time to collect this information.

OPM stated that it plans to issue additional guidance for tracking IT, cybersecurity, and cyber-related vacancies by January 2019.[32] OPM officials said that agencies have focused on the assignment of codes to filled positions and that tracking vacancies is challenging because agencies vary in the way they track vacancies.

By not completing their efforts to identify and code their vacant IT, cybersecurity, and cyber-related positions, the six agencies lack important information about the state of their workforces. As a result, these agencies may be limited in their ability to identify work roles of critical need and improve workforce planning.

Most Agencies Had Likely Miscategorized the Work Roles of Many Positions

The *Federal Cybersecurity Workforce Assessment Act of 2015* required agencies to assign the appropriate work role codes to each position with cybersecurity, cyber-related, and IT functions, as defined in the NICE framework. In addition, OPM guidance required agencies to assign work role codes using the Federal Cybersecurity Coding Structure.[33] As previously mentioned, according to OPM's guidance, agencies could assign up to three work role codes to each position. Agencies were to assign a code of "000" only to positions that did not perform IT, cybersecurity, or cyber-related functions. Further, the *Standards for Internal Control in the Federal Government* states that agencies should obtain relevant data from reliable sources that are complete and consistent.[34]

However, the 24 agencies had likely miscategorized the work roles of many positions. For example, the 24 agencies routinely assigned work role codes to positions that were likely inconsistent with the positions' functions. Specifically, at least 22 of the 24 agencies assigned the code

[32] Office 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).

[33] Office 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), and *Federal Cybersecurity Coding Structure*, Version 2.0 (October 18, 2017).

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

"000", which is designated for positions not performing IT, cybersecurity, or cyber-related functions, to many positions that most likely performed these functions.

For example, OPM's Enterprise Human Resources Integration data from May 2018 showed that 22 of the 24 agencies had assigned the "000" code to between 5 and 86 percent of their positions in the 2210 IT management occupational series.[35] These positions are most likely to perform IT, cybersecurity, or cyber-related functions, as defined by the NICE framework. OPM and agency officials told us that they would expect agencies to assign a NICE work role code to these positions, with a few exceptions, such as in cases where a position's duties did not align with a NICE work role code.

Table 3 identifies the number and percentage of the 2210 IT management positions that were assigned a "000" code by each of the 24 agencies, according to OPM's Enterprise Human Resources Integration data, as of May 2018. Collectively, the agencies assigned a "000" code to about 15,779 positions, or about 19 percent of the agencies' 2210 IT management positions.

[35] The IT management positions we refer to are those in the 2210 IT management occupational series that cover positions that manage, supervise, lead, administer, develop, deliver, and support information technology systems and services.

Table 3: The Number and Percentage of 2210 IT Management Positions Assigned Work Role Code “000” by the 24 CFO Act Agencies, According to OPM’s Enterprise Human Resources Integration Data, as of May 2018

Agency	Number of 2210 positions	Number of 2210 positions to which the agency assigned “000”	Percentage of 2210 positions to which the agency assigned “000”
Department of Agriculture	3,167	415	13
Department of Commerce	3,292	2,219	67
Department of Defense	37,915	1,782	5
Department of Education	238	15	6
Department of Energy	608	100	16
Department of Health and Human Services	3,254	1,168	36
Department of Homeland Security	4,872	1,382	28
Department of Housing and Urban Development	211	21	10
Department of the Interior	1,960	213	11
Department of Justice	3,170	480	15
Department of Labor	720	89	12
Department of State	797	114	14
Department of Transportation	1,790	1,522	85
Department of the Treasury	7,103	1,304	18
Department of Veterans Affairs	6,636	3,008	45
Environmental Protection Agency	579	105	18
General Services Administration	655	565	86
National Aeronautics and Space Administration	452	327	72
National Science Foundation	97	—[a]	N/A
Nuclear Regulatory Commission	159	19	12
Office of Personnel Management	253	13	5
Small Business Administration	196	71	36
Social Security Administration	3,688	847	23
U.S. Agency for International Development	73	—[a]	N/A
Total	**81,885**	**15,779**[b]	**19**[b]

Legend: OPM = Office of Personnel Management

Source: GAO analysis of OPM’s Enterprise Human Resources Integration data as of May 2018. | GAO-19-44.

Note: Data are for civilian positions only and do not include military or Foreign Service positions.

[a] There were 10 or fewer positions in this category and the data were not available. According to the National Science Foundation, no 2210 positions were assigned the “000” code.

[b] Totals are not inclusive of two agencies, the National Science Foundation and U.S. Agency for International Development. According to the National Science Foundation, all of the agency’s 2210 positions had at least one work role code assigned.

Agencies identified varying reasons for why they assigned the “000” code to positions that most likely performed IT, cybersecurity, or cyber-related functions. For example,

- Agency human resources and IT officials from 10 agencies said that they may have assigned the “000” code in error (DOD, Education, Energy, Justice, State, Department of Veterans Affairs (VA), NRC, OPM, Small Business Administration (SBA), Social Security Administration (SSA)).[36]
- Agency human resources and IT officials from 13 agencies said they had not completed the process to validate the accuracy of their codes (Department of Agriculture (Agriculture), Education, Department of Health and Human Services (HHS), DHS, Department of Housing and Urban Development (HUD), Justice, Treasury, VA, EPA, GSA, NRC, SBA, SSA).
- Agency human resources and IT officials from seven agencies said that they assigned the “000” code to positions that did not perform cybersecurity duties for a certain percentage of their time (Commerce, Justice, Labor, Transportation, Treasury, GSA, and NASA).
- Agency human resources and IT officials from 12 agencies said that OPM’s guidance was not clear on whether the 2210 IT management positions should be assigned a work role code and not be assigned the “000” code (Agriculture, Energy, DHS, HUD, Interior, Labor, State, VA, EPA, GSA, NASA, and SSA).
- Agency human resources and IT officials from three agencies stated that they assigned the “000” code to IT positions when their positions did not align with any of the work roles described in the NICE framework (Interior, Treasury, and NRC).

However, the work roles and duties described in the agencies’ position descriptions for the 2210 IT management positions that we reviewed aligned with the work roles defined in the NICE framework. For example, in examining the position descriptions that NRC officials said did not align to work roles in the NICE framework, we were able to match duties described in the position descriptions to work role tasks in the framework and identify potential work role codes for those positions. Additionally,

[36] In January 2019, the Department of Energy provided a report demonstrating that it had not assigned the “000” code as a primary code to any of its 2210 IT management positions. In addition, during the course of our review, in November 2018, the Nuclear Regulatory Commission provided a report demonstrating that it had assigned a work role code to 17 of its 2210 IT management positions that had been previously assigned the “000” code.

Treasury officials said that positions in the area of cryptographic key management did not align with the NICE framework; however, these positions would likely align with the Communications Security Manager (i.e., NICE code 723) work role, which covers cryptographic key management.

By assigning work role codes that are inconsistent with the IT, cybersecurity, and cyber-related functions performed by positions, the agencies in our review are diminishing the reliability of the information they will need to identify their workforce roles of critical need.

Agencies Assigned Work Role Codes to Sample Positions That Were Inconsistent with Duties Described In Corresponding Position Descriptions

Similar to the work role data reported in OPM's Enterprise Human Resources Integration system, the six agencies that we selected for additional review had assigned work role codes to positions in their human resources systems that were not consistent with the duties described in their corresponding position descriptions. Of 120 randomly selected 2210 IT management positions that we reviewed at the six agencies, 63 were assigned work role codes that were inconsistent with the duties described in their position descriptions.[37]

For example,

- DHS assigned a Network Operational Specialist code (NICE code 441) to a position with duties associated with a Cyber Instructional Curriculum Developer (NICE code 751).
- State assigned a Cyber Legal Advisor (NICE code 731) code to a position with duties associated with a Program Manager (NICE code 801).

Table 4 summarizes the consistency of work role coding in comparison to corresponding position description text for the random sample of positions for the six selected agencies.

[37] Agencies assigned a "000" code to 51 of the 63 positions and assigned a code for a work role that was not described in the position description for 12 positions.

Table 4: Random Sample of Work Role Coded IT Positions within the 2210 Occupational Series Compared with Position Descriptions Duties

Agency	Number of positions	Number of positions assigned codes consistent with position description text	Number of positions assigned codes inconsistent with position description text	Number of missing position descriptions (not provided by the agencies[a])
DOD	20	11	5	4
DHS	20	10	10	0
State	20	9	4	7
EPA	20	13	7	0
GSA	20	2	18	0
NASA	20	1	19	0
Total	**120**	**46**	**63**	**11**

Source: GAO analysis of Department of Defense (DOD), Department of Homeland Security (DHS), Department of State (State), National Aeronautics and Space Administration (NASA), Environmental Protection Agency (EPA), and General Services Administration (GSA) IT, cybersecurity, and cyber-related coding data. DOD data do not include noncivilian positions (i.e., military). State data do not include Foreign Service positions and are limited to civil service positions. | GAO-19-144.

Note: DHS, NASA, EPA, and GSA provided data as of May 12, 2018, in order to include pay period data from the end of April 2018. DOD provided data as of June 28, 2018. State provided data as of July 26, 2018. Position descriptions document the major duties and responsibilities of a position, but do not detail every possible activity.

[a] Missing position descriptions were position descriptions requested in the randomly selected sample that agencies were not able to provide during the course of our review.

The six agencies had also assigned different work role codes for positions that had identical position titles and similar functions described in corresponding position descriptions for 46 of 72 positions that we reviewed. For example,

- State had two positions associated with a position description that described duties associated with the IT Program Auditor (NICE code 805). Although State assigned the "805" work role code to one position, it assigned the "000" code to the other position.
- DOD had two positions associated with a position description that described duties associated with the Information Systems Security Manager work role (NICE code 722). However, DOD assigned the "000" code to one position and assigned an invalid 2-digit code to the other position.

The six agencies provided multiple reasons for why they had assigned codes that were not consistent with the work roles and duties described in their corresponding position descriptions:

- DOD officials from the Office of the Chief Information Officer cited the large number of positions that perform IT, cybersecurity, or cyber-related functions and the lack of one-to-one mapping of the NICE framework work roles to positions as impediments.

- DHS human resources officials said that position descriptions may not have been consistent with coding because the assignment of the work role codes could be based on specific tasks that are described in separate documents (e.g., job analyses or employee performance plans) outside of the position descriptions.
- Information Resource Management officials at State said that their system did not require all IT positions to have a work role code. However, according to the officials, they had plans to create and release a business rule in September 2018 to reduce data errors and require the 2210 IT management positions series to have a work role code.[38]
- EPA officials in the Office of Environmental Information and the Office of Human Resources stated that the first-line supervisor made the final determination of each position's work role code. Officials stated that first-line supervisors may have assigned different codes for similar positions because they interpreted OPM guidance and work roles differently.
- GSA human resources officials said they assigned "000" to IT positions because they needed clarification and further interpretive guidance from OPM.[39] According to the officials, once GSA received the guidance, the agency planned to conduct a review of IT positions coded "000." In addition, GSA had assigned the code "000" if the position description did not include 25 percent or more of cybersecurity functions.
- According to NASA officials from the Offices of the Chief Human Capital Officer and Chief Information Officer, the agency miscoded a few positions due to an administrative error that has since been corrected. In addition, NASA officials said that they assigned the "000" code to positions that did not perform cybersecurity duties for a certain percentage of time (e.g., 25 percent or more of the time).

[38] As of October 2018, State has published its business rules and a job aide to assist in ensuring the proper assignment of work role codes to IT, cybersecurity, or cyber-related positions in the 2210 occupational series. State has also updated its positon descriptions to include a section for the annotation of work role codes.

[39] OPM issued interpretive guidance in October 2018. Office of Personnel Management, *Interpretive Guidance for Cybersecurity Positions: Attracting, Hiring and Retaining a Federal Cybersecurity Workforce* (October 2018).

Agencies did not provide further evidence that the positions we evaluated as inconsistently coded were accurate. Moreover, in reviewing 87 position descriptions provided by the six agencies—DOD, DHS, State, EPA, GSA, and NASA—in no case did we find the assignment of the “000” work role code to be consistent with the duties described.

By assigning work role codes that are inconsistent with the IT, cybersecurity, and cyber-related functions performed by positions, the agencies in our review are diminishing the reliability of the information they will need to identify their workforce roles of critical need.

OPM and Agencies Had Taken Steps to Identify IT, Cybersecurity, and Cyber-related Work Roles of Critical Need

As of November 2018, OPM and the 24 agencies had taken steps to address the three selected activities that the *Federal Cybersecurity Workforce Assessment Act of 2015* required to identify IT, cybersecurity, and cyber-related work roles of critical need. Specifically, OPM had reported on agencies’ progress in identifying critical needs (activity 8) and had provided agencies with guidance for identifying IT, cybersecurity, and cyber-related work roles of critical need (activity 9). In addition, the 24 agencies had submitted preliminary reports of their identified critical needs to OPM, but their efforts to identify critical needs were ongoing (activity 10).

Table 5 presents the status of the agencies’ efforts to identify work roles of critical need, as of November 2018. Further, appendix III summarizes the status of implementation of each of the 10 selected activities required by the act.

Table 5: Status of Federal Agencies' Implementation of Selected Activities to Identify Work Roles of Critical Need as Required by the *Federal Cybersecurity Workforce Assessment Act of 2015*, as of November 2018

Required activity[a]	Due date	Actual completion date	Status of activity
8) OPM is to identify critical needs across federal agencies and submit a progress report on the identification of critical needs.	December 2017	December 2017	In December 2017, OPM submitted a progress report on agencies' preliminary efforts to identify IT, cybersecurity, and cyber-related critical needs.[c]
9) OPM is to provide federal agencies with timely guidance for identifying IT, cybersecurity, or cyber-related work roles of critical need including work roles with acute and emerging skill shortages.	Timely[b]	June 2018	In April and June 2018, OPM provided agencies with guidance for identifying IT, cybersecurity, and cyber-related work roles of critical need.
10) Federal agencies are to identify IT, cybersecurity, or cyber-related work roles of critical need in the workforce and submit a report describing these needs to OPM.	April 2019; OPM also required agencies to submit a preliminary report by August 31, 2018	Ongoing	As of November 2018, all 24 agencies had submitted preliminary reports to OPM.

Legend: OPM = Office of Personnel Management.

Source: GAO analysis of OPM guidance and agency efforts to identify IT, cybersecurity, or cyber-related work roles of critical need. | GAO-19-144.

[a] We selected these activities for the focus of this report because we previously reported on the status of agencies' actions to implement activities that the act required agencies to implement by November 2017 in GAO-18-466.

[b] The *Federal Cybersecurity Workforce Assessment Act of 2015* did not specify a specific date for this requirement.

[c] OPM submitted a progress report to Congress, but could not identify critical needs across all federal agencies because agencies were still in the process of assigning work role codes and identifying their critical needs.

OPM Reported on Progress of Efforts and Provided Guidance for Agencies to Identify Cybersecurity Work Roles of Critical Need

The *Federal Cybersecurity Workforce Assessment Act of 2015* required OPM, in consultation with DHS, to identify critical needs for the IT, cybersecurity, or cyber-related workforce across federal agencies and submit a progress report to Congress on the identification of IT, cybersecurity, or cyber-related work roles of critical need by December 2017. The act also required OPM to provide timely guidance for identifying IT, cybersecurity, or cyber-related work roles of critical need, and including current acute and emerging skill shortages.

In December 2017, OPM, in consultation with DHS, reported on the progress of federal agencies' identification of IT, cybersecurity, and cyber-related work roles of critical need to Congress. In the report, OPM could not identify critical needs across all federal agencies because agencies were still in the process of assigning work role codes and identifying their critical needs. As such, OPM reported that agencies were working toward accurately completing their coding efforts by April 2018, as a foundation for assessing the workforce and identifying needed cybersecurity skills. OPM stated in the report that it would begin to identify and report IT, cybersecurity, and cyber-related work roles of critical need following the agencies' completion of their assessments and coding of the workforce.

Further, in April 2018, OPM issued a memorandum to federal agencies' chief human capital officers that provided guidance on identifying IT, cybersecurity, and cyber-related work roles.[40] Specifically, this guidance required agencies to report their greatest skill shortages, analyze the root cause of the shortages, and provide action plans with targets and measures for mitigating the critical skill shortages.[41]

In addition, in June 2018, to ensure that agencies were on track to meet the requirements outlined in the act to submit their critical needs by April 2019, OPM required agencies to provide a preliminary report on work roles of critical need and root causes by August 31, 2018.[42] OPM provided agencies with a template to collect critical information such as critical needs and root causes. OPM guidance stated that these data would provide the Congress with a government-wide perspective of critical needs and insight into how to allocate future resources.

Agencies Have Begun to Identify Cybersecurity Work Roles of Critical Need

The act required agencies to identify IT, cybersecurity, or cyber-related work roles of critical need and submit a report to OPM substantiating these critical need designations by April 2019. OPM also required agencies to submit a preliminary report, which included agencies' identified work roles of critical need and the associated root causes, by August 31, 2018.

[40] Office of Personnel Management, *Memorandum for Human Resources Directors: Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need* (Washington, D.C.: April 2, 2018).

[41] The act required OPM to provide guidance for identifying acute and emerging skill shortages. OPM provided guidance that agencies identify the greatest skill shortages in terms of 1) staffing levels and/or proficiency competency levels and 2) current and emerging shortages, and mission criticality or importance for meeting agencies' most significant organizational missions, priorities, and challenges.

[42] Office of Personnel Management, *Memorandum for Human Resources Directors: Preliminary Report on Agency Cybersecurity Work Roles of Critical Need due August 31, 2018* (Washington, D.C.: June 11, 2018).

The 24 agencies have begun to identify critical needs and submitted a preliminary report of critical needs to OPM. Seventeen agencies submitted their report by the August 31, 2018 deadline, and seven submitted their report after the deadline in September 2018.[43] Most agencies' reports included the required critical needs and root causes. Specifically,

- Twenty-four agencies' reports documented work roles of critical need.
- Twenty-two agencies' reports included the root cause of the critical needs identified.

Table 6 shows the status of the 24 agencies' submissions of preliminary reports on cybersecurity work roles of critical need as of November 2018.

[43] The 24 agencies have not submitted a report to OPM substantiating work roles of critical need because they are not required to do so until April 2019.

Table 6: Submission Status of Preliminary Reports on Cybersecurity Work Roles of Critical Need by the 24 CFO Act Agencies as of November 2018

Agency	Submitted report to OPM	Submitted report to OPM by August 2018 deadline	Documents work roles of critical need	Includes root cause of critical need
Department of Agriculture	✓	✓	✓	—
Department of Commerce	✓	✓	✓	✓
Department of Defense	✓	✓	✓	✓
Department of Education	✓	✓	✓	✓
Department of Energy	✓	✓	✓	✓
Department of Health and Human Services	✓	✓	✓	✓
Department of Homeland Security	✓	—	✓	✓
Department of Housing and Urban Development	✓	—	✓	✓
Department of the Interior	✓	—	✓	✓
Department of Justice	✓	—	✓	✓
Department of Labor	✓	✓	✓	✓
Department of State	✓	✓	✓	✓
Department of Transportation	✓	—	✓	✓
Department of the Treasury	✓	✓	✓	✓
Department of 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	✓	✓	✓	✓
U.S. Agency for International Development	✓	✓	✓	✓
Total	**24**	**17**	**24**	**22**

Legend: OPM = Office of Personnel Management. ✓ = agency submitted preliminary report to OPM and met report requirements. — = agency did not meet OPM report requirements. | GAO-19-144.

Source: GAO analysis of the 24 Chief Financial Officers (CFO) Act agencies' preliminary reports on work roles of critical need to OPM as of November 2018.

The preliminary reports of critical needs for the 24 agencies showed that, as of November 2018, IT project managers, information systems security managers, and systems security analysts are among the top identified work roles of critical need at these agencies. Twelve agencies reported each of these work roles as a critical need. Agencies' preliminary reports should provide a basis for agencies to develop strategies to address shortages and skill gaps in their IT, cybersecurity, and cyber-related workforces. For additional information on the top 12 reported work roles of critical need, see appendix IV.

Conclusions

As required by the *Federal Cybersecurity Workforce Assessment Act of 2015*, the 24 agencies had generally categorized their workforce positions that have IT, cybersecurity, or cyber-related functions; however, agencies did not ensure the work role coding was reliable. For example, six of the 24 agencies had not completed assigning codes to their vacant positions. In addition, 22 of the agencies had assigned a code designated for positions not performing IT, cybersecurity, or cyber-related functions to about 19 percent of filled IT management positions.

Further, six selected agencies—DOD, DHS, State, EPA, GSA, and NASA—had assigned work role codes to positions in their human resources systems that were not consistent with the duties described in the corresponding position descriptions. Until agencies accurately categorize their positions, the agencies may not have reliable information to form a basis for effectively examining their cybersecurity workforce, improving workforce planning, and identifying their workforce roles of critical need.

Although OPM met its deadlines for reporting to congressional committees on agencies' progress in identifying critical needs, the progress report did not identify critical needs across all federal agencies because agencies were still in the process of assigning work role codes and identifying their critical needs. In addition, OPM has since provided agencies with guidance that should assist them in their efforts to identify critical needs by April 2019. Further, all of the 24 agencies have submitted preliminary reports identifying work roles of critical need to OPM. These efforts should assist these agencies in moving forward to develop strategies to address shortages and skill gaps in their IT, cybersecurity, and cyber-related workforces.

Recommendations for Executive Action

We are making a total of 28 recommendations to 22 agencies to take steps to complete the appropriate assignment of codes to their positions performing IT, cybersecurity, or cyber-related functions, in accordance with the requirements of the *Federal Cybersecurity Workforce Assessment Act of 2015*. Specifically:

The Secretary of Agriculture should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 1)

The Secretary of Commerce should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 2)

The Secretary of Defense should complete the identification and coding of vacant positions in the department performing IT, cybersecurity, or cyber-related functions. (Recommendation 3)

The Secretary of Defense should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series, assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions. (Recommendation 4)

The Secretary of Education should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 5)

The Secretary of Energy should complete the identification and coding of vacant positions in the department performing IT, cybersecurity, or cyber-related functions. (Recommendation 6)

The Secretary of Energy should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 7)

The Secretary of Health and Human Services should take steps to review the assignment of the “000” code to any positions in the department in the

2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 8)

The Secretary of Homeland Security should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series, assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions. (Recommendation 9)

The Secretary of Housing and Urban Development should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 10)

The Secretary of Interior should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 11)

The Attorney General should complete the identification and coding of vacant positions in the Department of Justice performing IT, cybersecurity, or cyber-related functions in the Department of Justice. (Recommendation 12)

The Attorney General should take steps to review the assignment of the “000” code to any positions in the Department of Justice in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 13)

The Secretary of Labor should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 14)

The Secretary of State should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series, assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions. (Recommendation 15)

The Secretary of Transportation should take steps to review the assignment of the “000” code to any positions in the department in the

2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 16)

The Secretary of Treasury should take steps to review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 17)

The Secretary of Veterans Affairs should take steps review the assignment of the “000” code to any positions in the department in the 2210 IT management occupational series and assign the appropriate NICE work role codes. (Recommendation 18)

The Administrator of the Environmental Protection Agency should complete the identification and coding of vacant positions in the agency performing IT, cybersecurity, or cyber-related functions. (Recommendation 19)

The Administrator of the Environmental Protection Agency should take steps to review the assignment of the “000” code to any positions in the agency in the 2210 IT management occupational series, assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions. (Recommendation 20)

The Administrator of the General Services Administration should complete the identification and coding of vacant positions at GSA performing IT, cybersecurity, or cyber-related functions. (Recommendation 21)

The Administrator of the General Services Administration should take steps to review the assignment of the “000” code to any positions at GSA in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions. (Recommendation 22)

The Administrator of the National Aeronautics and Space Administration should complete the identification and coding of vacant positions at NASA performing IT, cybersecurity, or cyber-related functions. (Recommendation 23)

The Administrator of the National Aeronautics and Space Administration should take steps to review the assignment of the “000” code to any positions at NASA in the 2210 IT management occupational series, assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions. (Recommendation 24)

The Chairman of the Nuclear Regulatory Commission should take steps to review the assignment of the “000” code to any positions at NRC in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 25)

The Director of the Office of Personnel Management should take steps to review the assignment of the “000” code to any positions at OPM in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 26)

The Administrator of the Small Business Administration should take steps to review the assignment of the “000” code to any positions at SBA in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 27)

The Commissioner of the Social Security Administration should take steps to review the assignment of the “000” code to any positions at SSA in the 2210 IT management occupational series and assign the appropriate NICE framework work role codes. (Recommendation 28)

Agency Comments and Our Evaluation

We provided a draft of this report to the 24 CFO Act agencies and OMB for their review and comment. Of the 22 agencies to which we made recommendations, 20 agencies stated that they agreed with the recommendations directed to them; one agency partially agreed with the recommendation; and one agency agreed with one recommendation but did not agree with one recommendation.

In addition, of the two agencies to which we did not make recommendations, one agency acknowledged its review of the report but did not otherwise provide comments; the other agency provided technical comments, which we incorporated into the report as appropriate. We also received technical comments from three of the agencies to which we made recommendations, and incorporated them into the report as appropriate. Further, OMB responded that it had no comments on the report.

The following 20 agencies agreed with the recommendations in our report:

- In comments provided via email on February 19, 2019, the Director of Strategic Planning, Policy, E-government and Audits in Agriculture's Office of the Chief Information Officer stated that the department concurred with the recommendation in our report.
- In written comments (reprinted in appendix V), Commerce agreed with our recommendation and stated that it would ensure the proper coding of 2210 IT management occupational series positions with the appropriate NICE framework work role codes.
- In written comments (reprinted in appendix VI), DOD concurred with our two recommendations. With regard to our recommendation that it complete the identification and coding of vacant positions performing IT, cybersecurity, or cyber-related functions, the department stated that its longer-term initiative is to code positions, including vacant positions, in DOD's manpower requirements systems to provide true gap analysis capabilities. Regarding our recommendation that it review the assignment of "000" codes, the department stated that it would continue efforts to remediate erroneously coded positions.
- In written comments (reprinted in appendix VII), Education concurred with our recommendation. The department stated that its Office of Human Resources would continue to review the 2210 IT positions and ensure the assignment of appropriate work role codes.
- In written comments (reprinted in appendix VIII), Energy concurred with our two recommendations. Regarding our recommendation that it complete the identification and coding of vacant IT, cybersecurity, and cyber-related positions, the department stated that it had instituted procedures to review and code vacant positions.

  Regarding our recommendation that it review the assignment of "000" codes, the department said that it had ensured that all 2210 IT management positions were assigned the appropriate work role codes by April 2018. However, our review of the May 2018 data from OPM's Enterprise Human Resources Integration System found that Energy had assigned the "000" code to about 16 percent of its 2210 IT management positions. Further, along with its comments on the draft report, in January 2019, the department provided a report indicating that Energy had not assigned the "000" work role code to its positions in the 2210 IT management occupation series. We plan to take follow-up steps to verify the completeness of the department's actions.

  In addition to the aforementioned comments, Energy provided technical comments, which we have incorporated into this report, as appropriate.

- In written comments (reprint in appendix IX), HHS concurred with our recommendation and outlined steps to identify, review, and make necessary corrections to its 2210 IT management positions that were coded as “000.”
- In written comments (reprinted in appendix X), DHS concurred with our recommendation. The department stated that personnel in its Office of the Chief Human Capital Officer had established processes for periodically reviewing cybersecurity workforce coding data and for collaborating with components to ensure positions with significant responsibilities associated with the NICE framework—including 2210 positions—were properly coded.

  Nevertheless, DHS expressed concern with our finding that it had miscategorized the work roles for some positions. The department stated that its position descriptions are often written in a generalized format, and are static, baseline, point-in-time documents. The department added that, several positions may align with the same position description, yet have specific duties and content captured in other human capital documents such as employee performance plans. Thus, some positions may have the same position description yet require different cybersecurity codes.

  While we agree that position descriptions do not detail every possible activity, according to OPM, the position descriptions should document the major duties and responsibilities of a position.[44] However, we found that DHS did not always assign codes consistent with major duties and responsibilities described in the position descriptions. For example, the department assigned a Network Operational Specialist code to a position with major duties associated with a Cyber Instructional Curriculum Developer. The department did not provide evidence that the positions we evaluated as inconsistently coded were accurately coded. If work role codes are not consistent with position descriptions, DHS may not have reliable information to form a basis for effectively examining its cybersecurity workforce, improving workforce planning, and identifying its workforce roles of critical need.

  The department also provided technical comments, which we have incorporated into this report as appropriate.

[44] Office of Personnel Management, *Introduction to the Position Classification Standards*, (August 2009).

- In comments provided via email on February 14, 2019, an audit liaison officer in HUD’s Office of the Chief Human Capital Officer stated that the department agreed with our recommendation.
- In written comments (reprinted in appendix XI), Interior concurred with our recommendation and stated that it had taken steps to change the designation of the “000” code for the remaining personnel in the 2210 IT management occupational series.
- In comments provided via email on February 4, 2019, an audit liaison specialist in Justice’s Management Division stated that the department concurred with the two recommendations.
- In written comments (reprinted in appendix XII), Labor concurred with our recommendation and stated that it had taken steps to review and code the department’s 2210 IT positions using the NICE framework.
- In written comments (reprinted in appendix XIII), State concurred with our recommendation. The department said that it will conduct a comprehensive review of its 2210 positions and include instructions to change the coding of any such positions that have been assigned a “000” code. In addition, the department stated that it had created a new business rule in its human resources system to ensure that 2210 positions are assigned a primary work role code.
- In comments provided via email on December 20, 2018, an audit relations analyst in Transportation’s Office of the Secretary stated via email that the department concurred with our findings and recommendation.
- In written comments (reprinted in appendix XIV), VA concurred with our recommendation and stated that the department had begun conducting a review of its cyber coding.
- In written comments (reprinted in appendix XV), EPA concurred with our two recommendations to the agency. With regard to our recommendation that it complete the identification and coding of vacant positions performing IT cybersecurity or cyber-related functions, EPA stated that it would update its standard operating procedures to include the requirement to code vacant positions during the position classification process. Nevertheless, while including this requirement in the procedures is an important step, it is imperative that the agency implement the procedures to ensure that its vacant positions are assigned appropriate work role codes.

  With regard to our recommendation that the agency review the assignment of the “000” code to its 2210 IT management occupation series, EPA stated that it would review all such positions and assign the appropriate NICE framework codes to any positions that were erroneously coded with the non-IT work role code.

- In comments provided via email on January 31, 2019, the Director of the Human Capital Policy and Programs Division stated that GSA agreed with our two recommendations. Also, in written comments (reprinted in appendix XVI), GSA stated that, once it completes the ongoing transition to a position-based human resources system, it will explore options to include vacant positions in its new system. In addition, GSA stated that it had completed an initial review of cyber codes and indicated that it would update all coding by March 2019.
- In written comments (reprinted in appendix XVII), NRC agreed with the findings in our draft report and said it had taken actions to address our recommendation by assigning appropriate work role codes to IT management positions previously assigned a “000” code.
- In written comments (reprinted in appendix XVIII), OPM concurred with our recommendation to the agency. OPM stated that its human resources and subject matter experts plan to assess the assignment of “000” codes to personnel in the 2210 IT management occupation series to help ensure accurate coding and appropriate application of the NICE framework work role codes.
- In written comments (reprinted in appendix XIX), SBA concurred with our recommendation. The agency stated that its Office of the Chief Information Officer, Office of Human Resources Solutions, and appropriate program offices would review the assignment of the “000” code to any 2210 IT management occupation series positions and assign the appropriate NICE framework role codes. The agency also provided technical comments, which we have incorporated into this report as appropriate.
- In written comments (reprinted in appendix XX), SSA agreed with our recommendation and stated that it had taken steps to complete the assignment of codes to the remaining 2210 IT management positions.

In addition, one agency partially agreed with the recommendations in our report. In comments provided via email on February 15, 2019, the Acting Director for Treasury’s Office of Human Capital Strategic Management stated that the department partially concurred with our recommendation that it review the assignment of “000” codes. According to the Acting Director, the Deputy Assistant Secretary for Human Resources and Chief Human Capital Officer had issued guidance to all Treasury Bureaus to validate the coding of 2210 IT management positions.

However, Treasury did not agree with our finding that positions in the area of cryptographic key management could be aligned to the NICE framework work role code for the Communications Security Manager. The official stated that the cryptographic key management functions did not completely align with any of the NICE framework work roles.

We acknowledge that there may be positions that do not completely align with work roles described in the NICE framework. However, according to OPM, the framework currently covers a broad array of functions that describe the majority of IT, cybersecurity, and cyber-related work. As noted in our report, OPM officials told us that they would expect agencies to assign a NICE work role code to 2210 IT management positions, with a few exceptions, such as in cases where a position's duties did not align with a NICE work role code. As such, we maintain that Treasury likely miscategorized over 1,300 IT management positions by assigning a "000" code to them, designating those positions as not performing IT, cybersecurity, or cyber-related work and, thus, should review these positions and assign the appropriate work role codes.

Further, one agency did not agree with one of the two recommendations directed to it. Specifically, in written comments (reproduced in appendix XXI) NASA stated that it concurred with our recommendation to review the assignment of "000" codes to 2210 IT management positions. In this regard, the agency stated that it would complete a review of the assignment of "000" codes to 2210 IT management positions and assign the appropriate NICE framework work role codes.

NASA did not concur with our other recommendation to complete the identification and coding of vacant positions performing IT, cybersecurity, or cyber-related functions. The agency stated that it had met the intention of the recommendation with existing NASA processes that assign a code at the time a vacancy is identified. However, the agency's workforce planning process is decentralized and the agency previously noted that it did not track vacancies.

We maintain that the Federal Cybersecurity Workforce Assessment Act requires agencies to identify and code vacant positions and that NASA could compile necessary information from components to identify and code vacant IT, cybersecurity, and cyber-related positions. These efforts would provide important information about vacant IT, cybersecurity, and cyber-related positions across the agency to enhance NASA's workforce planning. Thus, we continue to believe that our recommendation is warranted.

In addition, of the two agencies to which we did not make recommendations, one agency—USAID—provided a letter (reprinted in appendix XXII) acknowledging its review of the report and the other agency—NSF—provided technical comments, which we have incorporated into the report as appropriate.

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 XXIII.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

List of Committees

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

The Honorable Roger Wicker
Chairman
The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Ron Johnson
Chairman
The Honorable Gary Peters
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 Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Bennie Thompson
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Elijah Cummings
Chairman
The Honorable Jim Jordan
Ranking Member
Committee on Oversight and Reform
House of Representatives

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

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine the extent to which federal agencies have assigned work role codes to positions performing information technology (IT), cybersecurity, or cyber-related functions, and (2) describe the steps federal agencies took to identify work roles of critical need. The scope of our review included the 24 major departments and agencies covered by the *Chief Financial Officers (CFO) Act of 1990*.[1]

To address our objectives, we reviewed the provisions of the *Federal Cybersecurity Workforce Assessment Act of 2015*[2] and assessed the workforce planning actions taken by the Office of Personnel Management (OPM) and the other 23 CFO Act agencies against the selected four activities required by the act.[3]

To evaluate the four selected activities of the act and objectives 1 and 2, we reviewed the *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*[4] and OPM's cybersecurity coding structure and guidance.[5] The guidance provided information on how agencies should identify and assign work role codes to IT, cybersecurity, and cyber-related positions. We also designed and administered a questionnaire to each of the 24 agencies regarding their efforts to identify

[1] The 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)).

[2] The *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. 301 (Dec. 18, 2015) 129 Stat. 2242, 2975-77.

[3] In June 2018, we issued an initial report on agencies' efforts to implement selected activities that the act required them to complete by November 2017. GAO, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions,* GAO-18-466 (Washington, D.C.: June 14, 2018).

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

[5] Office 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), and *Federal Cybersecurity Coding Structure Version 2.0* (October 18, 2017).

and assign work role codes to IT, cybersecurity, or cyber-related positions, and identify work roles of critical need. In developing the questionnaire, we took steps to ensure the accuracy and reliability of responses. We pre-tested the questionnaire with OPM and the Department of Homeland Security (DHS) officials to ensure that the questions were clear, comprehensive, and unbiased, and to minimize the burden the questionnaire placed on respondents. We also asked the chief information officer and the chief human capital officer of each agency to certify that they reviewed and validated the responses to the questionnaires.

We administered the questionnaire between June and October 2018. We received completed questionnaires from each of the 24 agencies, for a response rate of 100 percent. We examined the questionnaire results and performed computer analyses to identify missing data, inconsistencies, and other indications of error, and addressed such issues as necessary, including through follow-up communications with the 24 agencies. We reviewed and analyzed the agencies' responses to the questionnaire in comparison to the act's requirements and OPM's and NICE's guidance. We also obtained, reviewed, and analyzed supporting documentation of questionnaire responses, such as reports of cybersecurity employment code data, to assess whether agencies assigned work role codes in accordance with the activities in OPM's coding guidance, by April 2018.[6]

Further, to analyze how federal agencies assigned work role codes to positions performing IT, cybersecurity, or cyber-related functions, we obtained IT, cybersecurity, or cyber-related workforce coding data for the 24 agencies from OPM's Enterprise Human Resources Integration system. To assess the reliability of coding data from OPM's system, we reviewed these data to determine its completeness, and asked officials responsible for entering and reviewing the work role coding data a series of questions about the accuracy and reliability of the data. In addition, we examined the Enterprise Human Resources Integration IT, cybersecurity, or cyber-related coding data to determine the number of positions the 24 agencies had assigned the "000" code to positions in the 2210 IT

[6] Agencies were asked to provide responses as of May 12, 2018, which was the end of the pay period that included April 30, 2018.

management occupational series as of May 2018.[7] We reviewed positions from the 2210 IT management occupational series because those positions are likely to perform IT, cybersecurity, or cyber-related functions. In the report, we note some challenges with the reliability of these data and are careful to present our data in line with these limitations.

We then identified a subset of the 24 agencies and performed an additional review of these agencies' work role coding efforts. We selected these agencies based on their total cybersecurity spending for fiscal year 2016, as reported by the Office of Management and Budget (OMB) in its *Federal Information Security Modernization Act* annual report.[8] We sorted the 24 agencies' IT cybersecurity spending from highest to lowest and then divided them into three equal groups of high, medium, and low. We then selected the top two agencies from each group. Based on these factors, we selected six agencies: the (1) Department of Defense (DOD), (2) DHS, (3) Department of State (State), (4) National Aeronautics and Space Administration (NASA), (5) Environmental Protection Agency (EPA), and (6) General Services Administration (GSA).We performed an additional review of the agencies' work role coding efforts. We did this by evaluating the six selected agencies' coding processes against their established procedures and OPM requirements. We also obtained and reviewed coding data that included the assigned work role codes for civilian employees from each agency's human resources system.[9]

[7] Office of Personnel Management, *Job Family Standard for Administrative Work in the Information Technology Group, 2200*, (Washington, D.C.: May 2011), and *Interpretive Guidance for the Information Technology Management Series, GS-2210* (Washington, D.C.: June 2001).

[8] Office of Management and Budget (OMB), *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, Fiscal Year 2016 (Washington, D.C.: March 10, 2017). At the start of the engagement, OMB's fiscal year 2016 data was the most current available.

[9] We reviewed data from the Department of Defense's Defense Civilian Personnel Data System (DCPDS), the Department of Homeland Security's National Finance Center (NFC), the Department of State's Global Employment Management System (GEMS), the National Aeronautics and Space Administration's Federal Personnel and Payroll System (FPPS), the Environmental Protection Agency Federal Personnel and Payroll System (FPPS), and the General Services Administration's (GSA) Comprehensive Human Resources Integrated System (CHRIS). We did not review noncivilian positions, and excluded Foreign Service positions because Department of State officials said they considered them sensitive.

To assess the reliability of coding data from the selected six agencies' systems, we reviewed related documentation such as the agencies' coding procedures, processing guides, personnel bulletins, and system screen shots. We also conducted electronic testing for missing data, duplicate data, or obvious errors. In addition, we asked officials responsible for entering and reviewing the work role coding data a series of questions about the accuracy and reliability of the data. For any anomalies in the data, we followed up with the six selected agencies' offices of the chief information officer and chief human capital officer to either understand or correct those anomalies. Further, we assessed the reliability of data in terms of the extent to which codes were completely assigned and reasonably accurate. In the report, we note some challenges with the reliability of these data and are careful to present our data in line with these limitations.

We randomly selected a sample of 20 positions from each of the six selected agencies (120 total positions) within the 2210 IT management occupational series. We reviewed positions from the IT management 2210 series because those positions are likely to perform IT, cybersecurity, or cyber-related functions. For the selected positions, we requested position descriptions and reviewed whether the position work role codes in the coding data were consistent with the corresponding position description text. We also selected a second nonstatistical sample of 12 positions for each of the six agencies (72 total positions) from the 2210 IT management occupational series based on pairs of positions that had identical position titles, occupational series, and sub-agencies, but for which the agencies had assigned different work role codes for the positions.[10] An analyst reviewed the work role coding data and compared them to the duties described by the position descriptions to determine whether they were consistent with the position duties. A second analyst verified whether or not the position's work role code was consistent with the position description. A third analyst adjudicated cases in which the first and second analysts' evaluations did not match.

Lastly, to evaluate agencies' actions to address the last three activities of the act related to the identification of cybersecurity work roles of critical

[10] We selected these examples to examine why agencies assigned different codes to similar positions. For example, two positions could have identical position titles, occupational series, and sub-agencies, but one position was assigned a work role code while the other was assigned a code designated for positions that do not perform IT, cybersecurity, or cyber-related functions (i.e., "000").

need, we obtained, reviewed, and analyzed OPM's guidance for identifying critical needs and its progress report to Congress by comparing it to the act's requirements.[11] We reviewed agencies' responses to our questionnaire regarding whether they had developed methodologies or project plans for identifying critical needs. We also reviewed any available documentation on the 24 agencies' progress in identifying critical needs, such as project plans, timelines, and preliminary reports. In addition, OPM required agencies to submit a preliminary report on work roles of critical need by August 31, 2018.[12] We obtained copies of the preliminary reports from the 24 agencies. We evaluated agencies' efforts to meet the deadline, as well as for meeting OPM's requirements for documenting work roles of critical need and determining root causes of those needs.

To supplement our analysis, we interviewed agency officials from human resources and chief information officer offices at the 24 agencies regarding their progress in coding and identifying cybersecurity work roles of critical need.

We conducted this performance audit from February 2018 to March 2019 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.

[11] Office of Personnel Management, *Memorandum for Human Resources Directors: Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need* (Washington, D.C.: April 2, 2018).

[12] Office of Personnel Management, *Memorandum for Human Resources Directors: Preliminary Report on Agency Cybersecurity Work Roles of Critical Need due August 31, 2018* (Washington, D.C.: June 11, 2018).

Appendix II: Office of Personnel Management Information Technology, Cybersecurity, and Cyber-related Work Role Codes

Table 7: Office of Personnel Management (OPM) Federal Information Technology, Cybersecurity, and Cyber-related Work Role Codes

Specialty Area	Work Role	OPM Code	Work Role Description
Securely Provision Category			
Risk Management	Authorizing Official/Designating Representative	611	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation (CNSSI 4009).
	Security Control Assessor	612	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
Software Development	Software Developer	621	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
	Secure Software Assessor	622	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
Systems Architecture	Enterprise Architect	651	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
	Security Architect	652	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
Technology R&D	Research & Development Specialist	661	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
Systems Requirements Planning	Systems Requirements Planner	641	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
Test and Evaluation	System Testing and Evaluation Specialist	671	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

Specialty Area	Work Role	OPM Code	Work Role Description
Systems Development	Information Systems Security Developer	631	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
	Systems Developer	632	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.
Operate and Maintain Category			
Data Administration	Database Administrator	421	Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.
	Data Analyst	422	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.
Knowledge Management	Knowledge Manager	431	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
Customer Service and Technical Support	Technical Support Specialist	411	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).
Network Services	Network Operations Specialist	441	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
Systems Administration	System Administrator	451	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
Systems Analysis	Systems Security Analyst	461	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Oversee and Govern Category			
Legal Advice and Advocacy	Cyber Legal Advisor	731	Provides legal advice and recommendations on relevant topics related to cyber law.
	Privacy Officer/Privacy Compliance Manager	732	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.

Specialty Area	Work Role	OPM Code	Work Role Description
Training, Education, and Awareness	Cyber Instructional Curriculum Developer	711	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
	Cyber Instructor	712	Develops and conducts training or education of personnel within cyber domain.
Cybersecurity Management	Information Systems Security Manager	722	Responsible for the cybersecurity of a program, organization, system, or enclave.
	Communications Security (COMSEC) Manager	723	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).
Strategic Planning and Policy	Cyber Workforce Developer and Manager	751	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training, and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
	Cyber Policy and Strategy Planner	752	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
Executive Cyber Leadership	Executive Cyber Leadership	901	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
Program/Project Management and Acquisition	Program Manager	801	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.
	IT Project Manager	802	Directly manages information technology projects.
	Product Support Manager	803	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
	IT Investment/Portfolio Manager	804	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.
	IT Program Auditor	805	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.
Protect and Defend Category			
Cyber Defense Analysis	Cyber Defense Analyst	511	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
Cyber Defense Infrastructure Support	Cyber Defense Infrastructure Support Specialist	521	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.

Specialty Area	Work Role	OPM Code	Work Role Description
Incident Response	Cyber Defense Incident Responder	531	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Vulnerability Assessment and Management	Vulnerability Assessment Analyst	541	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Analyze			
Threat Analysis	Threat/Warning Analyst	141	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
Exploitation Analysis	Exploitation Analyst	121	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
All-Source Analysis	All-Source Analyst	111	Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.
	Mission Assessment Specialist	112	Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.
Targets	Target Developer	131	Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.
	Target Network Analyst	132	Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.

Specialty Area	Work Role	OPM Code	Work Role Description
Language Analysis	Multi-Disciplined Language Analyst	151	Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.
Collect and Operate Category			
Collection Operations	All Source-Collection Manager	311	Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.
	All Source-Collection Requirements Manager	312	Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.
Cyber Operational Planning	Cyber Intel Planner	331	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.
	Cyber Ops Planner	332	Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.
	Partner Integration Planner	333	Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

Specialty Area	Work Role	OPM Code	Work Role Description
Cyber Operations	Cyber Operator	321	Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.
Investigate Category			
Cyber Investigation	Cyber Crime Investigator	221	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
Digital Forensics	Law Enforcement/Counterintelligence Forensics Analyst	211	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
	Cyber Defense Forensics Analyst	212	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.
Not Applicable			
Not Applicable	Not Applicable	000	Does NOT involve work functions in information technology (IT), cybersecurity, or cyber-related areas.

Source: GAO analysis of OPM's IT, cybersecurity, and cyber-related work role codes. | GAO-19-144.

Appendix III: Summary of 24 Chief Financial Officers Act Agencies’ Implementation of the Federal Cybersecurity Workforce Assessment Act of 2015, as of Nov. 2018

Table 8: Federal Chief Financial Officer (CFO) Act Agencies’ Implementation of the *Federal Cybersecurity Workforce Assessment Act of 2015* Requirements, as of November 2018

Required activity	Due date	Actual completion date	Status of activity
1) OPM, in coordination with NIST, is to develop a cybersecurity coding structure that aligns with the work roles identified in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.	June 2016	November 2016	Completed, but delayed by 5 months due to delay in NIST issuance of the NICE framework.
2) OPM is to establish procedures to implement the cybersecurity coding structure to identify all federal civilian positions that require the performance of information technology (IT), cybersecurity, or cyber-related functions.	September 2016	January 2017	Completed, but delayed by 4 months due to delay in NIST issuance of the NICE framework.
3) OPM is to submit a progress report on the implementation of the identification of IT, cybersecurity, or cyber-related positions and assignment of codes to positions.	June 2016	July 2016	Completed, but delayed by 1 month.
4) Each federal agency is to submit a report of its baseline assessment of the extent to which IT, cybersecurity, or cyber-related employees held certifications.	December 2016	Ongoing	21 of 24 agencies submitted reports, but three agencies had not submitted reports and four agencies had not addressed all of the reportable information as of October 2018.
5) Each federal agency is to establish procedures to identify all filled and vacant IT, cybersecurity, or cyber-related positions and assign the appropriate code to each position.	April 2017	24 of 24 agencies had established procedures as of August 2018	We made 20 recommendations to eight agencies to fully address this activity. The eight agencies implemented all 20 recommendations.
6) DOD is to establish procedures to implement the cybersecurity coding structure to identify all federal military positions	June 2017	June 2018	Completed, but delayed by 1 year.

Required activity	Due date	Actual completion date	Status of activity
7) Federal agencies are to complete the assignment of work role codes to filled and vacant positions that perform IT, cybersecurity, or cyber-related functions.	April 2018	Ongoing	As of October 2018, all 24 agencies had assigned work role codes to filled positions; however, six agencies had not completed assigning codes to their vacant positions. In addition, 22 of 24 agencies had assigned a work role code designated for positions not performing IT, cybersecurity, or cyber-related functions to many positions that most likely performed these functions.
8) OPM is to identify critical needs across federal agencies and submit a progress report on the identification of critical needs.	December 2017	December 2017	In December 2017, OPM submitted a progress report on agencies' preliminary efforts to identify IT, cybersecurity, and cyber-related critical needs.[b]
9) OPM is to provide federal agencies with timely guidance for identifying IT, cybersecurity, cyber-related work roles of critical need including work roles with acute and emerging skill shortages.	Timely[a]	June 2018	In April and June 2018, OPM provided agencies with guidance for identifying IT, cybersecurity, and cyber-related work roles of critical need.
10) Federal agencies are to identify IT, cybersecurity, or cyber-related work roles of critical need in the workforce and submit a report describing these needs to OPM.	April 2019; OPM also required agencies to submit a preliminary report by August 31, 2018	Ongoing	As of November 2018, all 24 agencies had submitted preliminary reports to OPM.

Legend: DOD = Department of Defense, NIST = National Institute of Standards and Technology, OPM = Office of Personnel Management

Source: GAO analysis of 24 Chief Financial Officers Act agencies' documentation, the Federal Cybersecurity Workforce Assessment Act of 2015, and GAO-18-466. | GAO-19-144.

[a] The Federal Cybersecurity Workforce Assessment Act did not specify a specific date for this requirement.

[b] OPM submitted a progress report to Congress, but could not identify critical needs across all federal agencies because agencies had yet to identify critical needs.

Appendix IV: Top 12 Work Roles of Critical Need as Identified by the 24 Chief Financial Officers (CFO) Act Agencies in Their Preliminary Reports of Critical Need

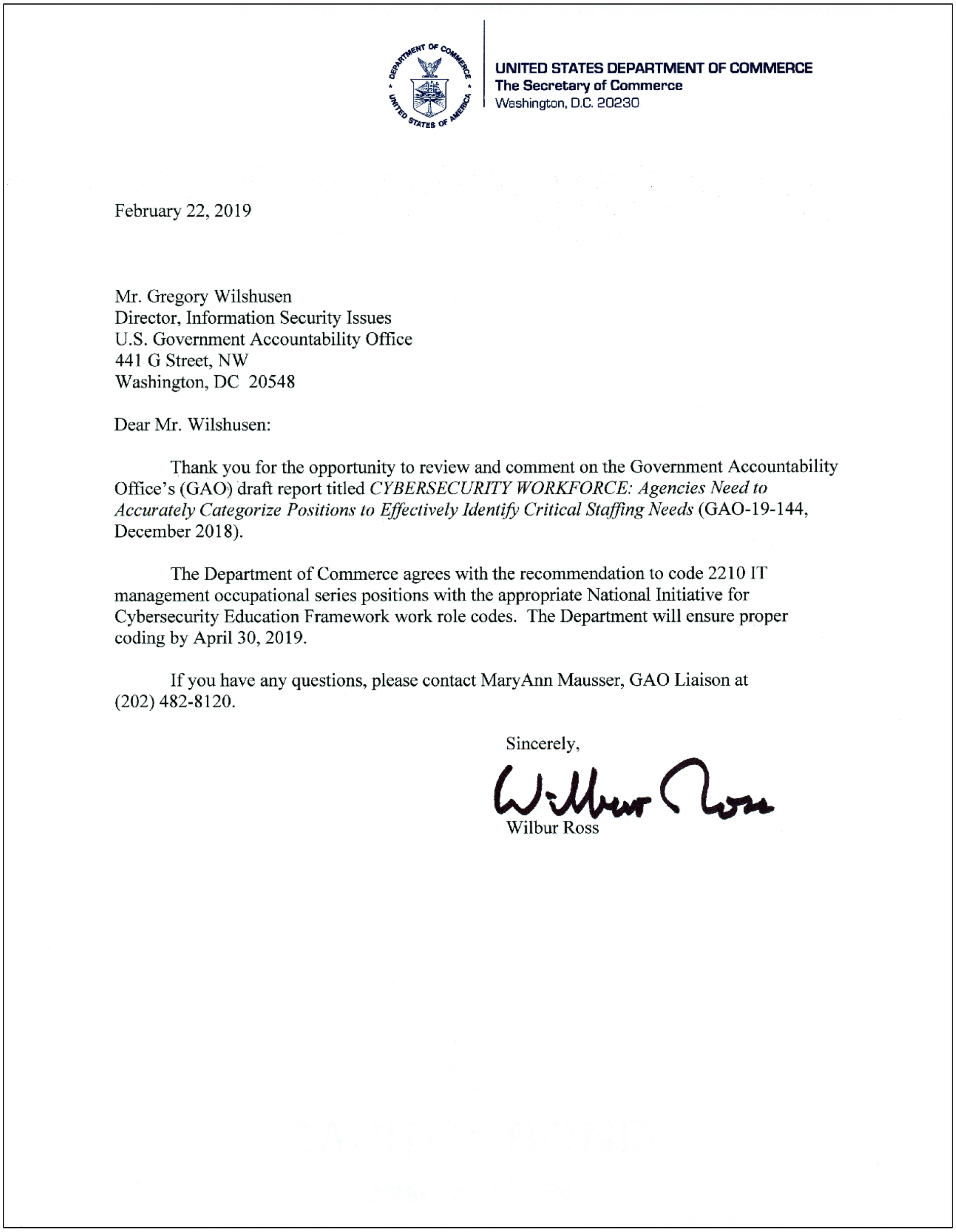
Table 9: Top 12 Preliminary Work Roles of Critical Need Reported by the 24 CFO Act Agencies as of November 2018

	NICE work role	OPM cybersecurity code	Description
1	Information Systems Security Manager (tied for first)	722	Is responsible for the cybersecurity of a program, organization, system, or enclave.
1	IT Project Manager (tied for first)	802	Manages information technology projects directly.
1	Systems Security Analyst (tied for first)	461	Is responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
4	Cyber Defense Analyst	511	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
5	Program Manager (tied for fifth)	801	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.
5	Technical Support Specialist (tied for fifth)	411	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components.
7	Network Operations Specialist (tied for seventh)	441	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
7	Software Developer (tied for seventh)	621	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
7	System Administrator (tied for seventh)	451	Is responsible for setting up and maintaining a system or specific components of a system.
10	Enterprise Architect (tied for tenth)	651	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
10	Security Control Assessor (tied for tenth)	612	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls.
10	Vulnerability Assessment Analyst (tied for tenth)	541	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy.

Source: GAO analysis of the 24 Chief Financial Officers Act agencies' preliminary reports on work roles of critical need as of November 2018. | GAO-19-144.

Note: Agencies did not identify and report on the same number of work roles of critical need.

Appendix V: Comments from the Department of Commerce



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

February 22, 2019

Mr. Gregory 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 Accurately Categorize Positions to Effectively Identify Critical Staffing Needs* (GAO-19-144, December 2018).

The Department of Commerce agrees with the recommendation to code 2210 IT management occupational series positions with the appropriate National Initiative for Cybersecurity Education Framework work role codes. The Department will ensure proper coding by April 30, 2019.

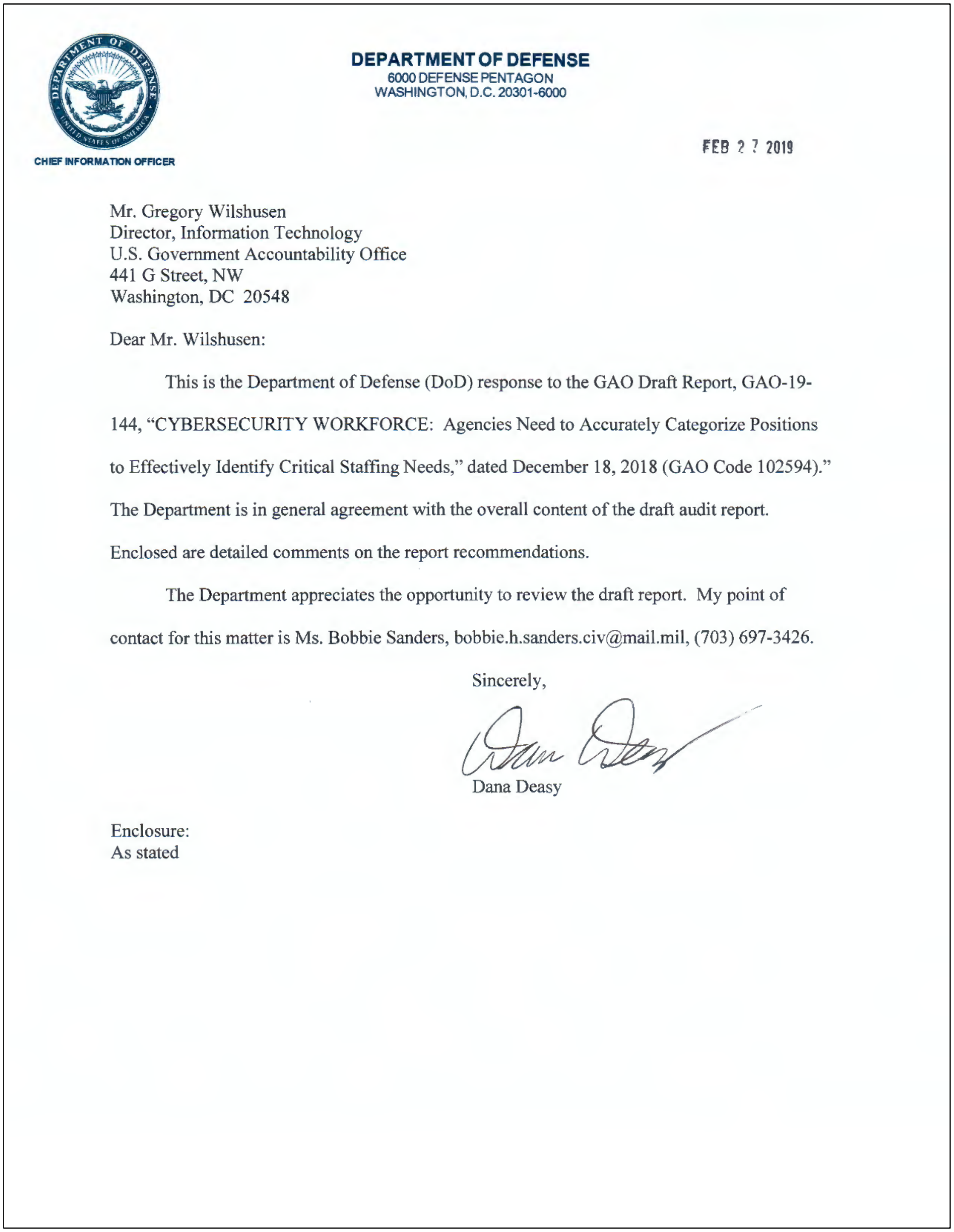
If you have any questions, please contact MaryAnn Mausser, GAO Liaison at (202) 482-8120.

Sincerely,

Wilbur Ross

Wilbur Ross

Appendix VI: Comments from the Department of Defense



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

FEB 27 2019

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

Dear Mr. Wilshusen:

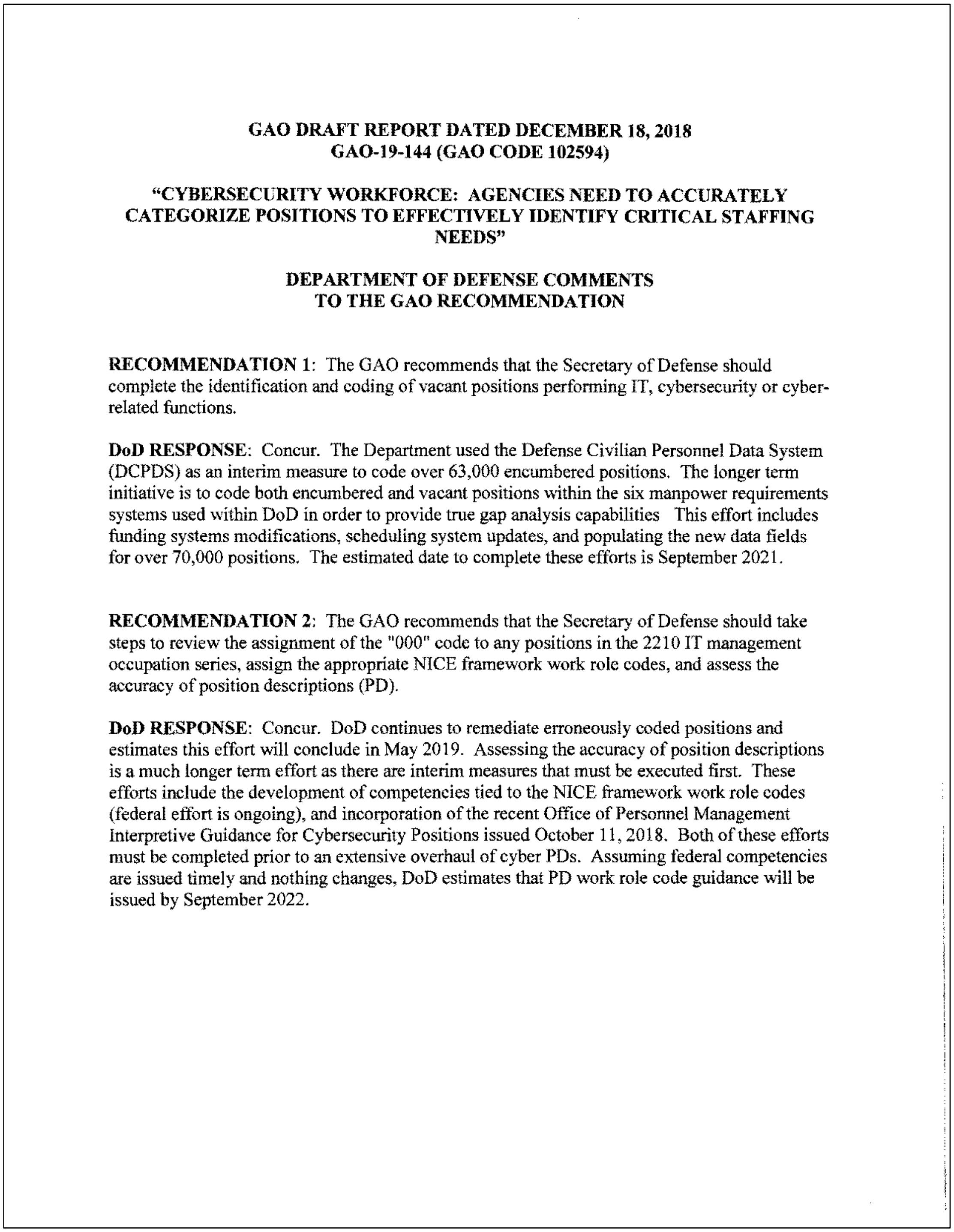
This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-19-144, "CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs," dated December 18, 2018 (GAO Code 102594)." The Department is in general agreement with the overall content of the draft audit report. Enclosed are detailed comments on the report recommendations.

The Department appreciates the opportunity to review the draft report. My point of contact for this matter is Ms. Bobbie Sanders, bobbie.h.sanders.civ@mail.mil, (703) 697-3426.

Sincerely,

Dana Deasy

Enclosure:
As stated



GAO DRAFT REPORT DATED DECEMBER 18, 2018
GAO-19-144 (GAO CODE 102594)

"CYBERSECURITY WORKFORCE: AGENCIES NEED TO ACCURATELY CATEGORIZE POSITIONS TO EFFECTIVELY IDENTIFY CRITICAL STAFFING NEEDS"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

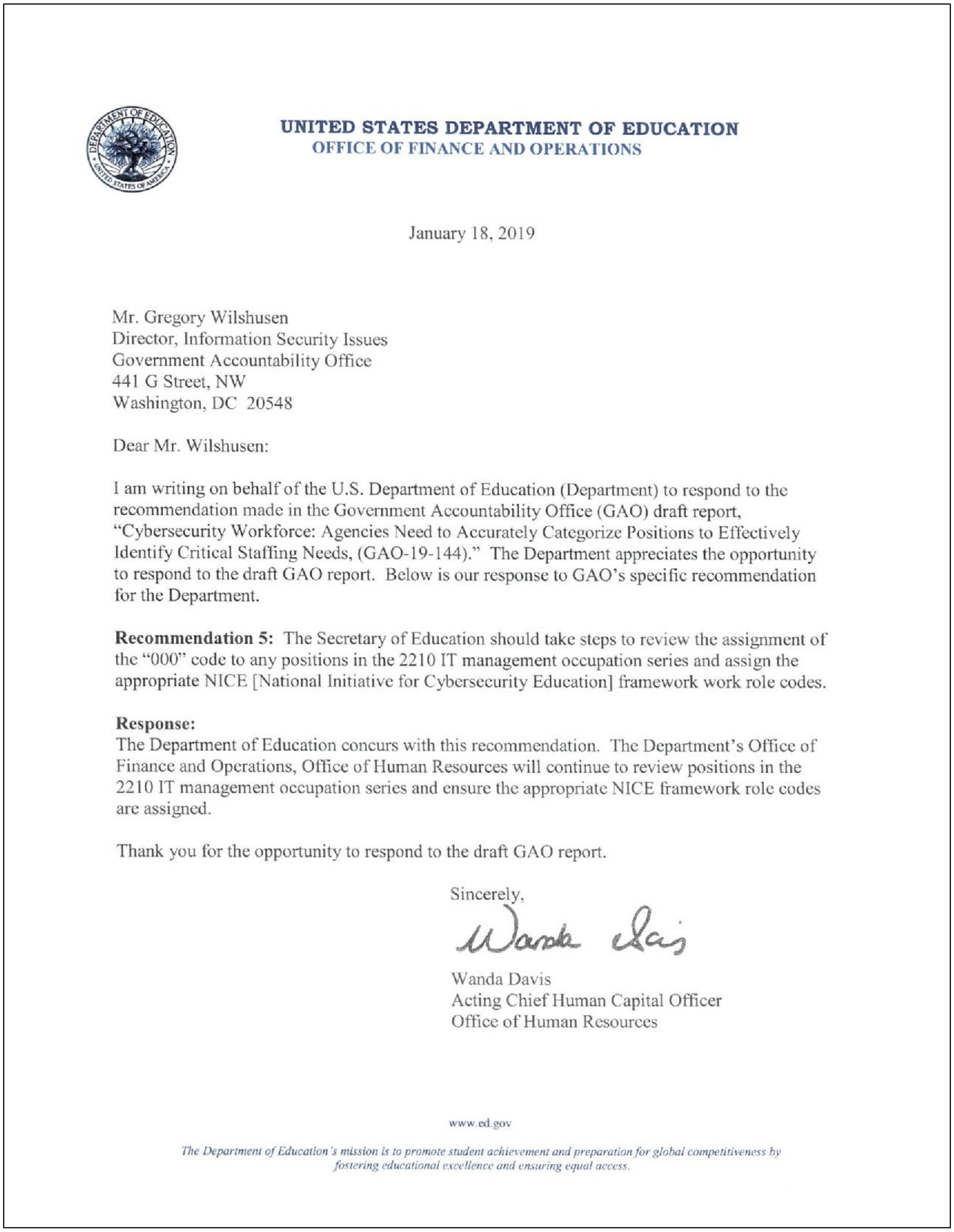
RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should complete the identification and coding of vacant positions performing IT, cybersecurity or cyber-related functions.

DoD RESPONSE: Concur. The Department used the Defense Civilian Personnel Data System (DCPDS) as an interim measure to code over 63,000 encumbered positions. The longer term initiative is to code both encumbered and vacant positions within the six manpower requirements systems used within DoD in order to provide true gap analysis capabilities This effort includes funding systems modifications, scheduling system updates, and populating the new data fields for over 70,000 positions. The estimated date to complete these efforts is September 2021.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series, assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions (PD).

DoD RESPONSE: Concur. DoD continues to remediate erroneously coded positions and estimates this effort will conclude in May 2019. Assessing the accuracy of position descriptions is a much longer term effort as there are interim measures that must be executed first. These efforts include the development of competencies tied to the NICE framework work role codes (federal effort is ongoing), and incorporation of the recent Office of Personnel Management Interpretive Guidance for Cybersecurity Positions issued October 11, 2018. Both of these efforts must be completed prior to an extensive overhaul of cyber PDs. Assuming federal competencies are issued timely and nothing changes, DoD estimates that PD work role code guidance will be issued by September 2022.

Appendix VII: Comments from the Department of Education



UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF FINANCE AND OPERATIONS

January 18, 2019

Mr. Gregory 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 Accurately Categorize Positions to Effectively Identify Critical Staffing Needs, (GAO-19-144)." The Department appreciates the opportunity to respond to the draft GAO report. Below is our response to GAO's specific recommendation for the Department.

Recommendation 5: The Secretary of Education should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series and assign the appropriate NICE [National Initiative for Cybersecurity Education] framework work role codes.

Response:
The Department of Education concurs with this recommendation. The Department's Office of Finance and Operations, Office of Human Resources will continue to review positions in the 2210 IT management occupation series and ensure the appropriate NICE framework role codes are assigned.

Thank you for the opportunity to respond to the draft GAO report.

Sincerely,

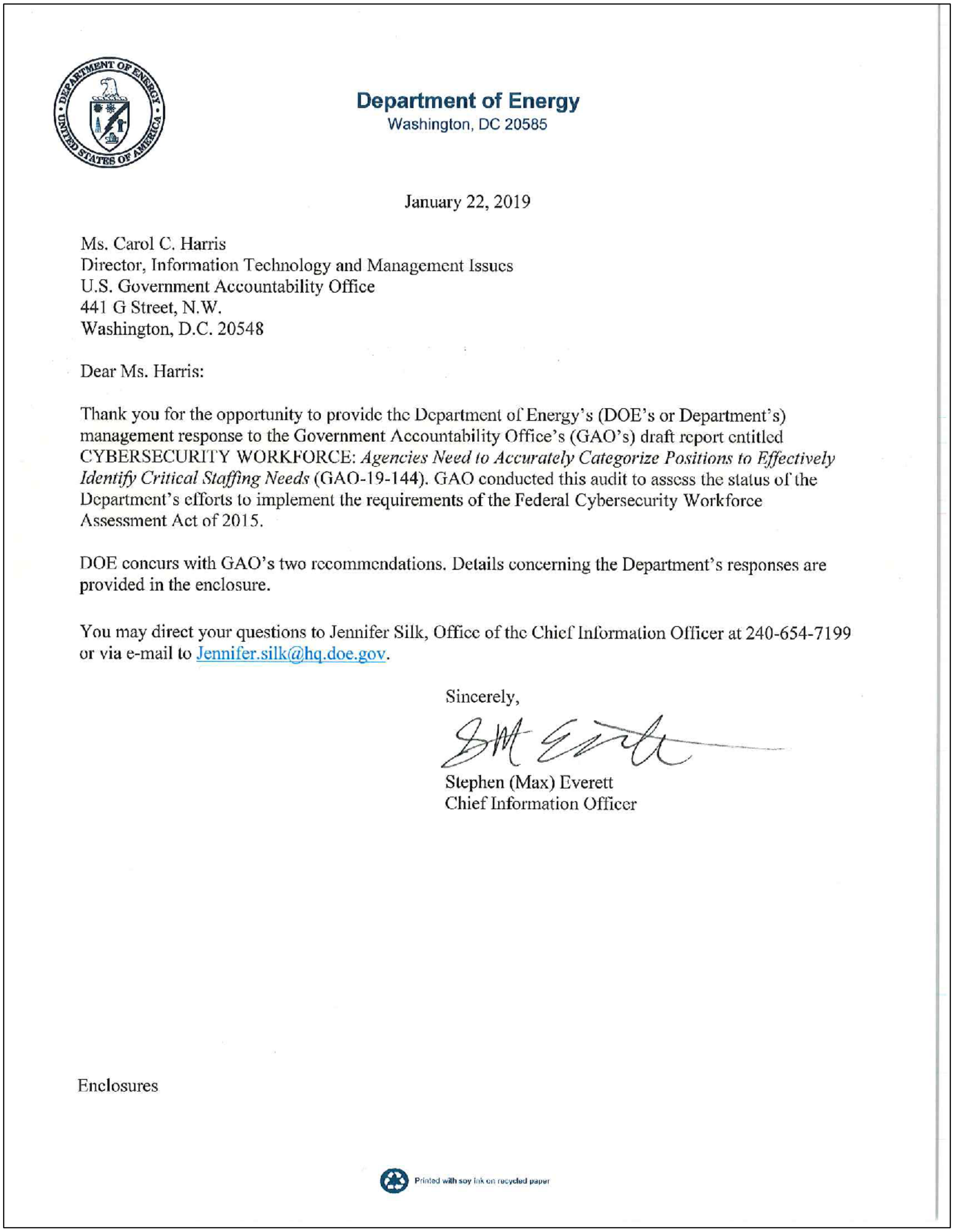
Wanda Davis

Wanda Davis
Acting Chief Human Capital Officer
Office of Human Resources

www.ed.gov

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

Appendix VIII: Comments from the Department of Energy



Department of Energy
Washington, DC 20585

January 22, 2019

Ms. Carol C. Harris
Director, Information Technology and Management Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Harris:

Thank you for the opportunity to provide the Department of Energy's (DOE's or Department's) management response to the Government Accountability Office's (GAO's) draft report entitled CYBERSECURITY WORKFORCE: *Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs* (GAO-19-144). GAO conducted this audit to assess the status of the Department's efforts to implement the requirements of the Federal Cybersecurity Workforce Assessment Act of 2015.

DOE concurs with GAO's two recommendations. Details concerning the Department's responses are provided in the enclosure.

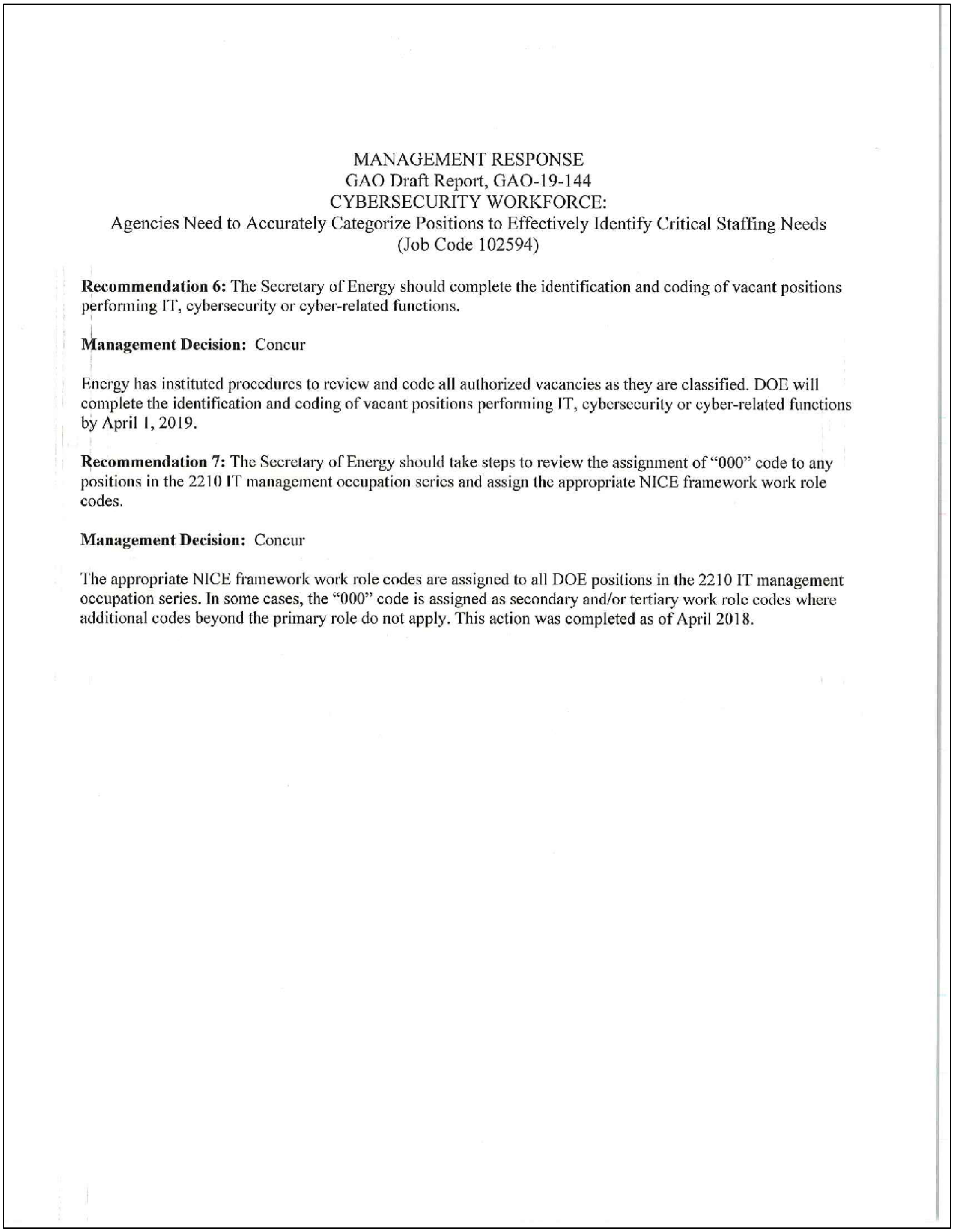
You may direct your questions to Jennifer Silk, Office of the Chief Information Officer at 240-654-7199 or via e-mail to Jennifer.silk@hq.doe.gov.

Sincerely,

Stephen (Max) Everett
Chief Information Officer

Enclosures

Printed with soy ink on recycled paper



MANAGEMENT RESPONSE
GAO Draft Report, GAO-19-144
CYBERSECURITY WORKFORCE:
Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs
(Job Code 102594)

Recommendation 6: The Secretary of Energy should complete the identification and coding of vacant positions performing IT, cybersecurity or cyber-related functions.

Management Decision: Concur

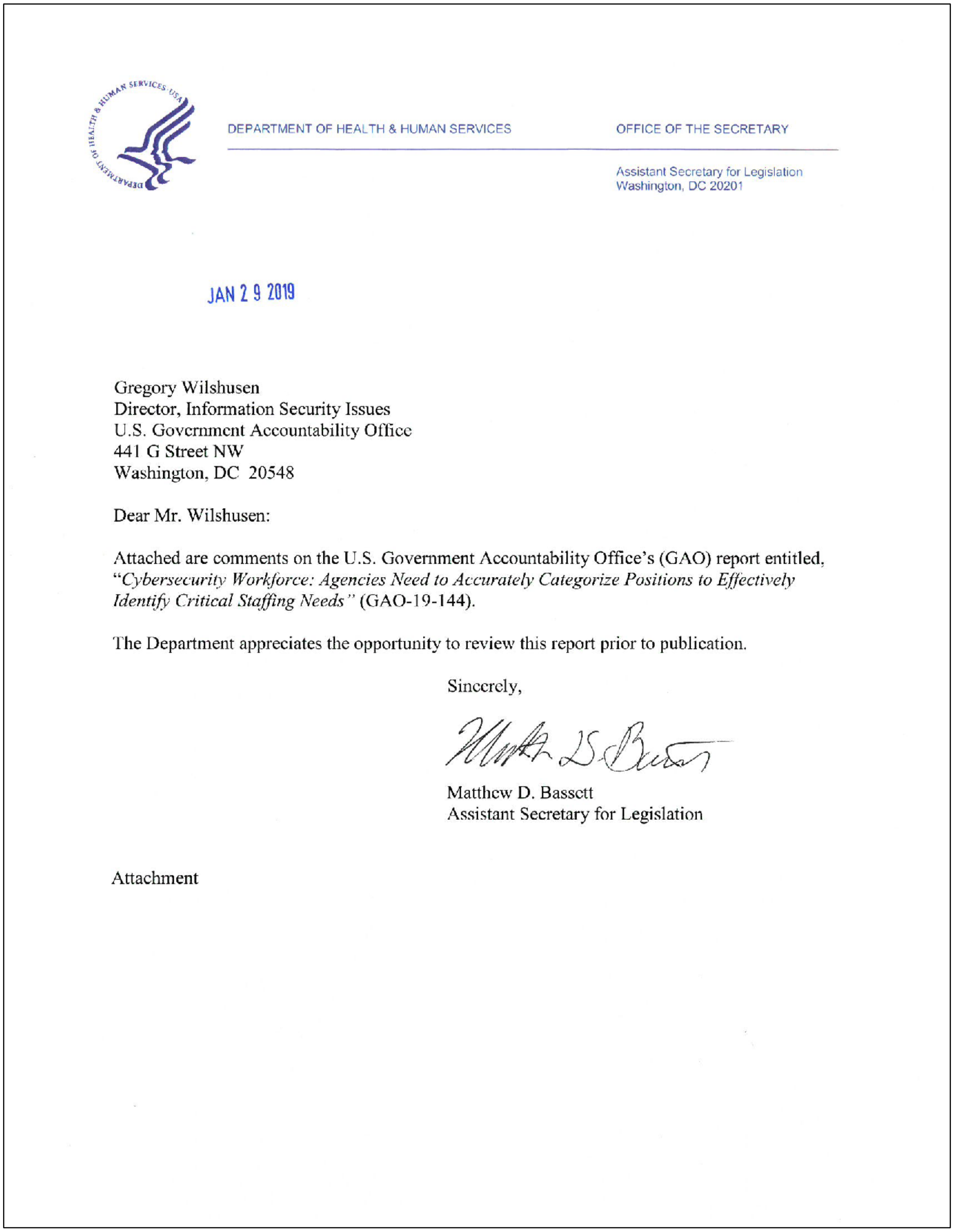
Energy has instituted procedures to review and code all authorized vacancies as they are classified. DOE will complete the identification and coding of vacant positions performing IT, cybersecurity or cyber-related functions by April 1, 2019.

Recommendation 7: The Secretary of Energy should take steps to review the assignment of "000" code to any positions in the 2210 IT management occupation series and assign the appropriate NICE framework work role codes.

Management Decision: Concur

The appropriate NICE framework work role codes are assigned to all DOE positions in the 2210 IT management occupation series. In some cases, the "000" code is assigned as secondary and/or tertiary work role codes where additional codes beyond the primary role do not apply. This action was completed as of April 2018.

Appendix IX: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

JAN 2 9 2019

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

Dear Mr. Wilshusen:

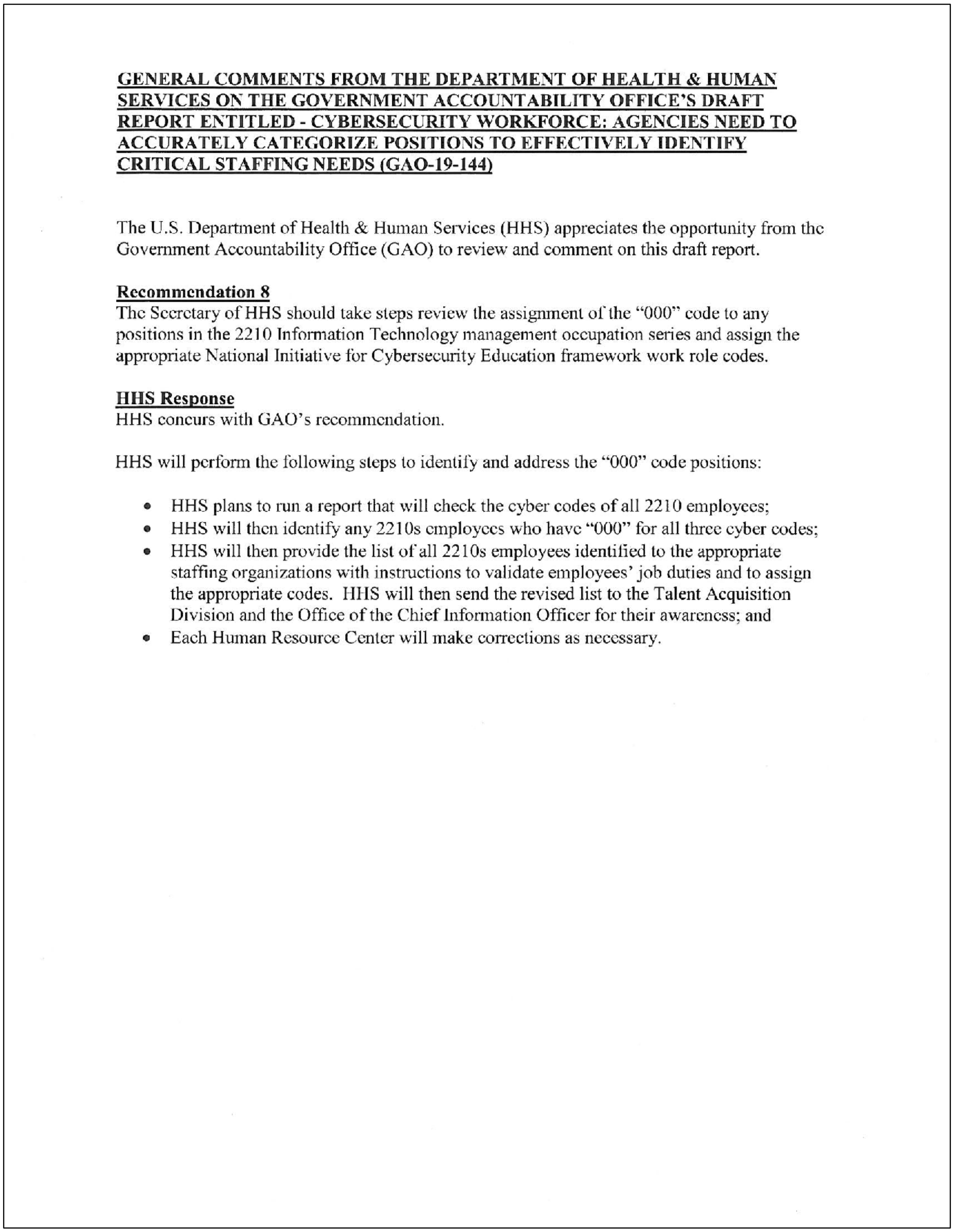
Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*" (GAO-19-144).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Matthew D. Bassett
Assistant Secretary for Legislation

Attachment



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - CYBERSECURITY WORKFORCE: AGENCIES NEED TO ACCURATELY CATEGORIZE POSITIONS TO EFFECTIVELY IDENTIFY CRITICAL STAFFING NEEDS (GAO-19-144)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

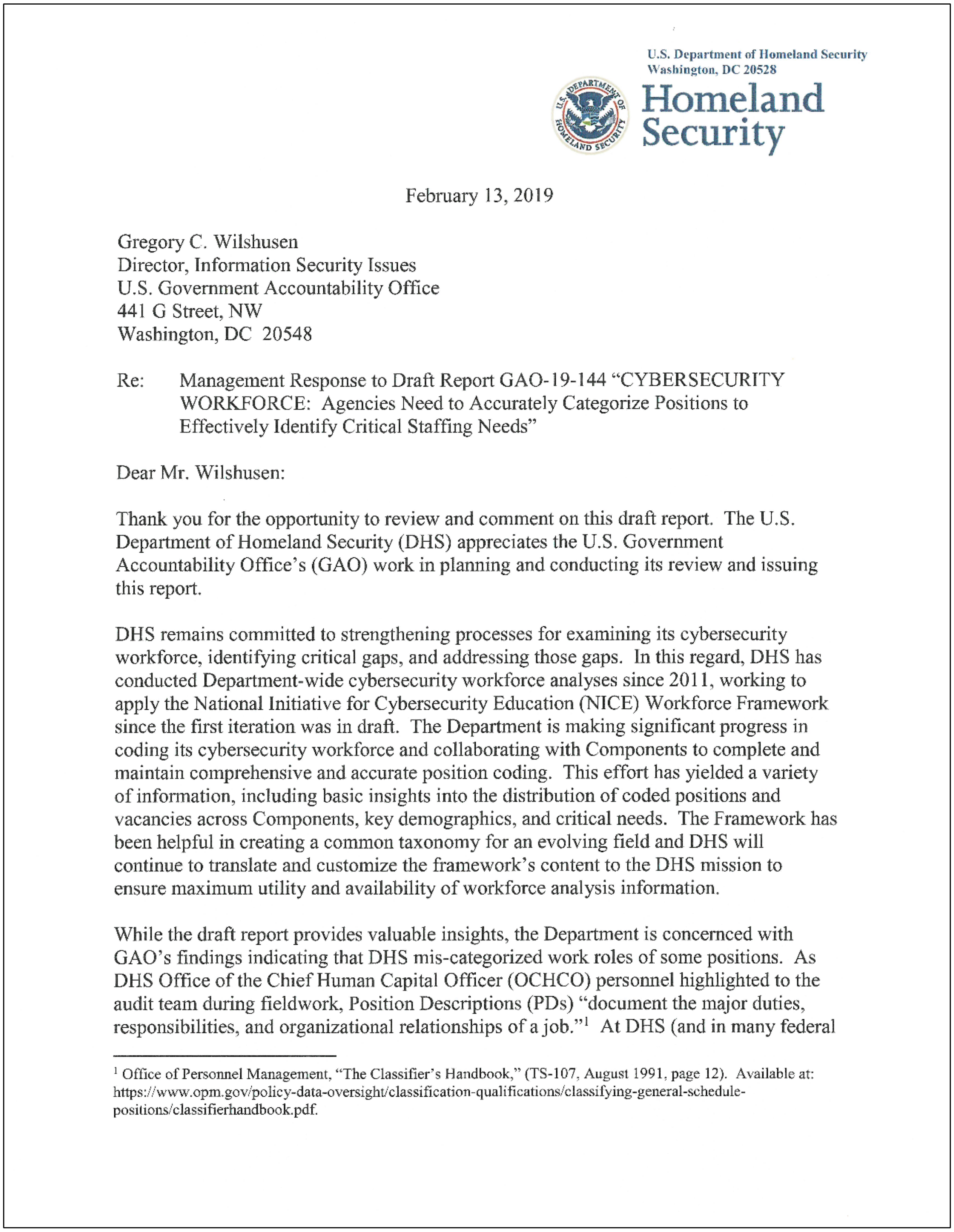
Recommendation 8
The Secretary of HHS should take steps review the assignment of the "000" code to any positions in the 2210 Information Technology management occupation series and assign the appropriate National Initiative for Cybersecurity Education framework work role codes.

HHS Response
HHS concurs with GAO's recommendation.

HHS will perform the following steps to identify and address the "000" code positions:

- HHS plans to run a report that will check the cyber codes of all 2210 employees;
- HHS will then identify any 2210s employees who have "000" for all three cyber codes;
- HHS will then provide the list of all 2210s employees identified to the appropriate staffing organizations with instructions to validate employees' job duties and to assign the appropriate codes. HHS will then send the revised list to the Talent Acquisition Division and the Office of the Chief Information Officer for their awareness; and
- Each Human Resource Center will make corrections as necessary.

Appendix X: Comments from the Department of Homeland Security



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

Homeland
Security

February 13, 2019

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

Re: Management Response to Draft Report GAO-19-144 "CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs"

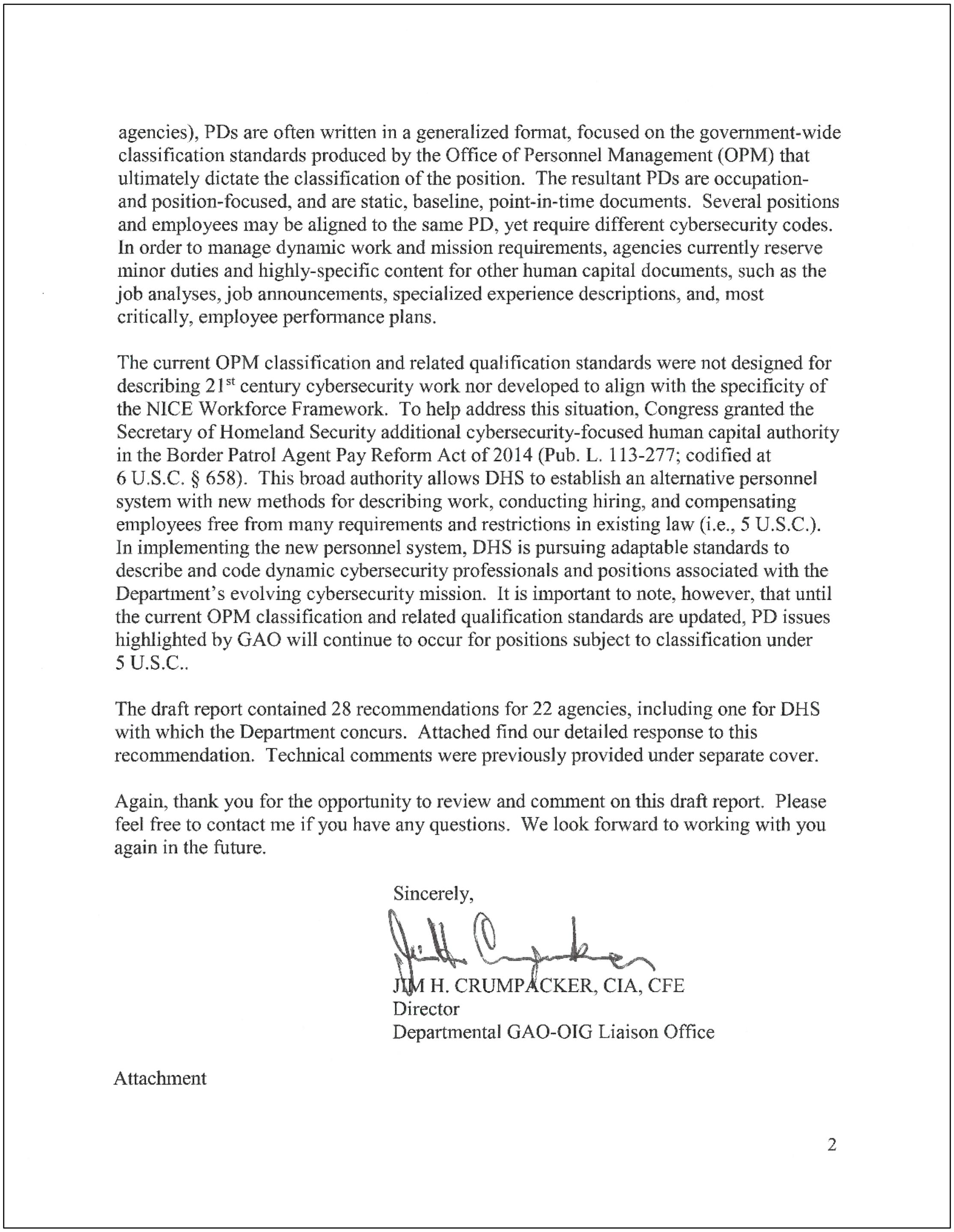
Dear Mr. Wilshusen:

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.

DHS remains committed to strengthening processes for examining its cybersecurity workforce, identifying critical gaps, and addressing those gaps. In this regard, DHS has conducted Department-wide cybersecurity workforce analyses since 2011, working to apply the National Initiative for Cybersecurity Education (NICE) Workforce Framework since the first iteration was in draft. The Department is making significant progress in coding its cybersecurity workforce and collaborating with Components to complete and maintain comprehensive and accurate position coding. This effort has yielded a variety of information, including basic insights into the distribution of coded positions and vacancies across Components, key demographics, and critical needs. The Framework has been helpful in creating a common taxonomy for an evolving field and DHS will continue to translate and customize the framework's content to the DHS mission to ensure maximum utility and availability of workforce analysis information.

While the draft report provides valuable insights, the Department is concernced with GAO's findings indicating that DHS mis-categorized work roles of some positions. As DHS Office of the Chief Human Capital Officer (OCHCO) personnel highlighted to the audit team during fieldwork, Position Descriptions (PDs) "document the major duties, responsibilities, and organizational relationships of a job."[1] At DHS (and in many federal

[1] Office of Personnel Management, "The Classifier's Handbook," (TS-107, August 1991, page 12). Available at: https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/classifierhandbook.pdf.



agencies), PDs are often written in a generalized format, focused on the government-wide classification standards produced by the Office of Personnel Management (OPM) that ultimately dictate the classification of the position. The resultant PDs are occupation- and position-focused, and are static, baseline, point-in-time documents. Several positions and employees may be aligned to the same PD, yet require different cybersecurity codes. In order to manage dynamic work and mission requirements, agencies currently reserve minor duties and highly-specific content for other human capital documents, such as the job analyses, job announcements, specialized experience descriptions, and, most critically, employee performance plans.

The current OPM classification and related qualification standards were not designed for describing 21st century cybersecurity work nor developed to align with the specificity of the NICE Workforce Framework. To help address this situation, Congress granted the Secretary of Homeland Security additional cybersecurity-focused human capital authority in the Border Patrol Agent Pay Reform Act of 2014 (Pub. L. 113-277; codified at 6 U.S.C. § 658). This broad authority allows DHS to establish an alternative personnel system with new methods for describing work, conducting hiring, and compensating employees free from many requirements and restrictions in existing law (i.e., 5 U.S.C.). In implementing the new personnel system, DHS is pursuing adaptable standards to describe and code dynamic cybersecurity professionals and positions associated with the Department's evolving cybersecurity mission. It is important to note, however, that until the current OPM classification and related qualification standards are updated, PD issues highlighted by GAO will continue to occur for positions subject to classification under 5 U.S.C..

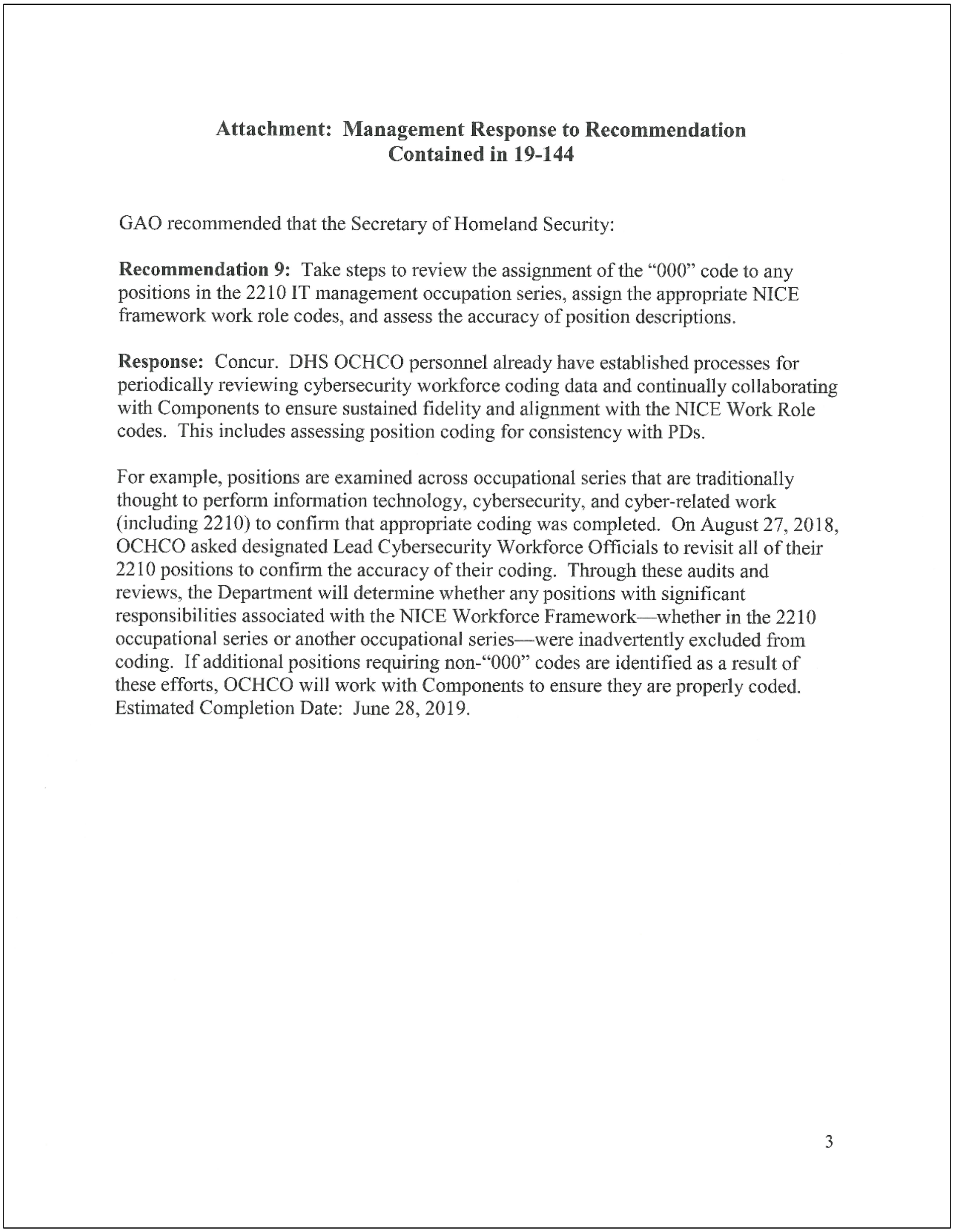
The draft report contained 28 recommendations for 22 agencies, including one for DHS with which the Department concurs. Attached find our detailed response to this recommendation. Technical comments were previously provided under separate cover.

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

Sincerely,

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

Attachment



Attachment: Management Response to Recommendation Contained in 19-144

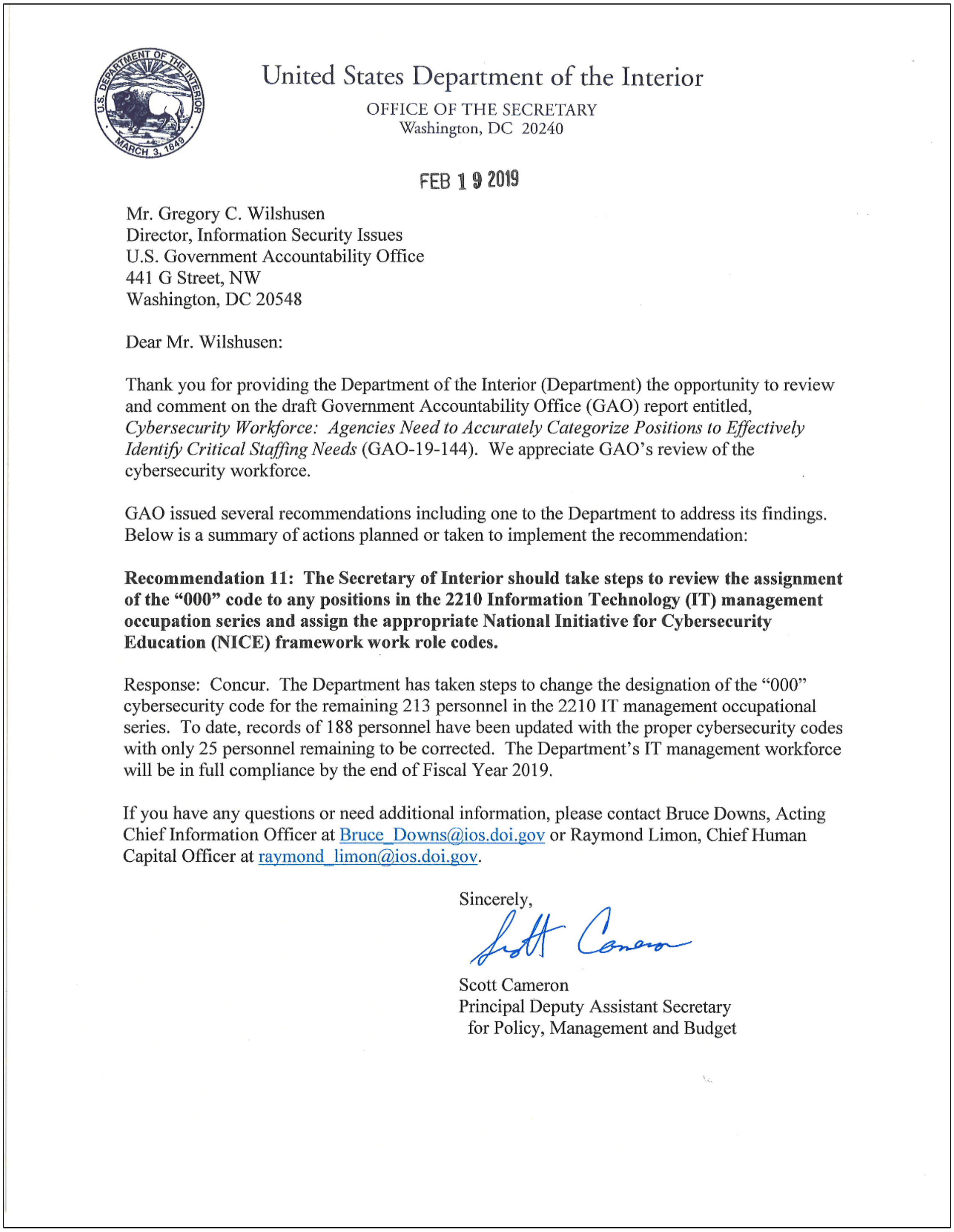
GAO recommended that the Secretary of Homeland Security:

Recommendation 9: Take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series, assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions.

Response: Concur. DHS OCHCO personnel already have established processes for periodically reviewing cybersecurity workforce coding data and continually collaborating with Components to ensure sustained fidelity and alignment with the NICE Work Role codes. This includes assessing position coding for consistency with PDs.

For example, positions are examined across occupational series that are traditionally thought to perform information technology, cybersecurity, and cyber-related work (including 2210) to confirm that appropriate coding was completed. On August 27, 2018, OCHCO asked designated Lead Cybersecurity Workforce Officials to revisit all of their 2210 positions to confirm the accuracy of their coding. Through these audits and reviews, the Department will determine whether any positions with significant responsibilities associated with the NICE Workforce Framework—whether in the 2210 occupational series or another occupational series—were inadvertently excluded from coding. If additional positions requiring non-"000" codes are identified as a result of these efforts, OCHCO will work with Components to ensure they are properly coded. Estimated Completion Date: June 28, 2019.

Appendix XI: Comments from the Department of the Interior



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

FEB 19 2019

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 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 Accurately Categorize Positions to Effectively Identify Critical Staffing Needs* (GAO-19-144). We appreciate GAO's review of the cybersecurity workforce.

GAO issued several recommendations including one to the Department to address its findings. Below is a summary of actions planned or taken to implement the recommendation:

Recommendation 11: The Secretary of Interior should take steps to review the assignment of the "000" code to any positions in the 2210 Information Technology (IT) management occupation series and assign the appropriate National Initiative for Cybersecurity Education (NICE) framework work role codes.

Response: Concur. The Department has taken steps to change the designation of the "000" cybersecurity code for the remaining 213 personnel in the 2210 IT management occupational series. To date, records of 188 personnel have been updated with the proper cybersecurity codes with only 25 personnel remaining to be corrected. The Department's IT management workforce will be in full compliance by the end of Fiscal Year 2019.

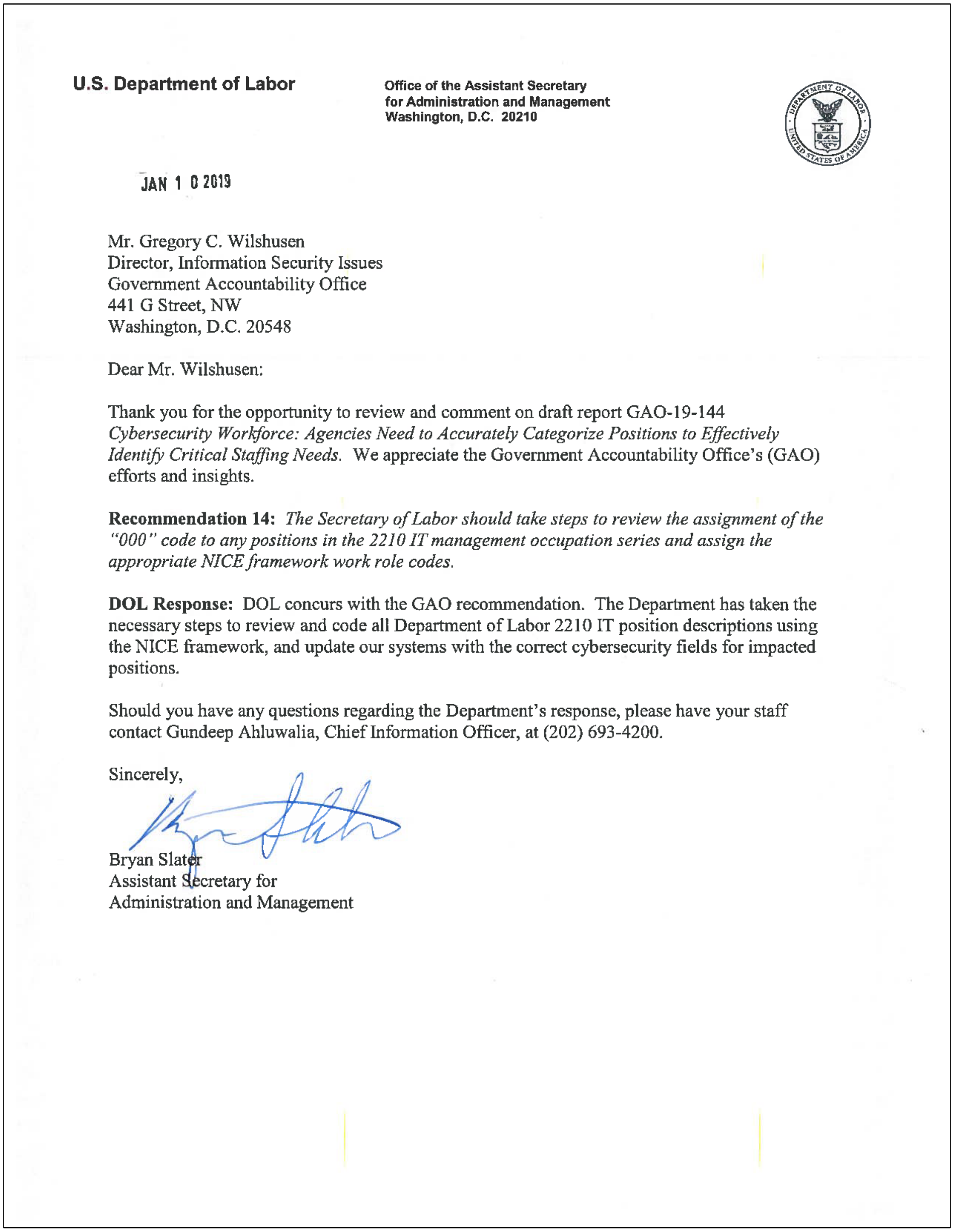
If you have any questions or need additional information, please contact Bruce Downs, Acting Chief Information Officer at Bruce_Downs@ios.doi.gov or Raymond Limon, Chief Human Capital Officer at raymond_limon@ios.doi.gov.

Sincerely,

Scott Cameron

Scott Cameron
Principal Deputy Assistant Secretary
for Policy, Management and Budget

Appendix XII: Comments from the Department of Labor



U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

JAN 1 0 2019

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

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on draft report GAO-19-144 *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs.* We appreciate the Government Accountability Office's (GAO) efforts and insights.

Recommendation 14: *The Secretary of Labor should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series and assign the appropriate NICE framework work role codes.*

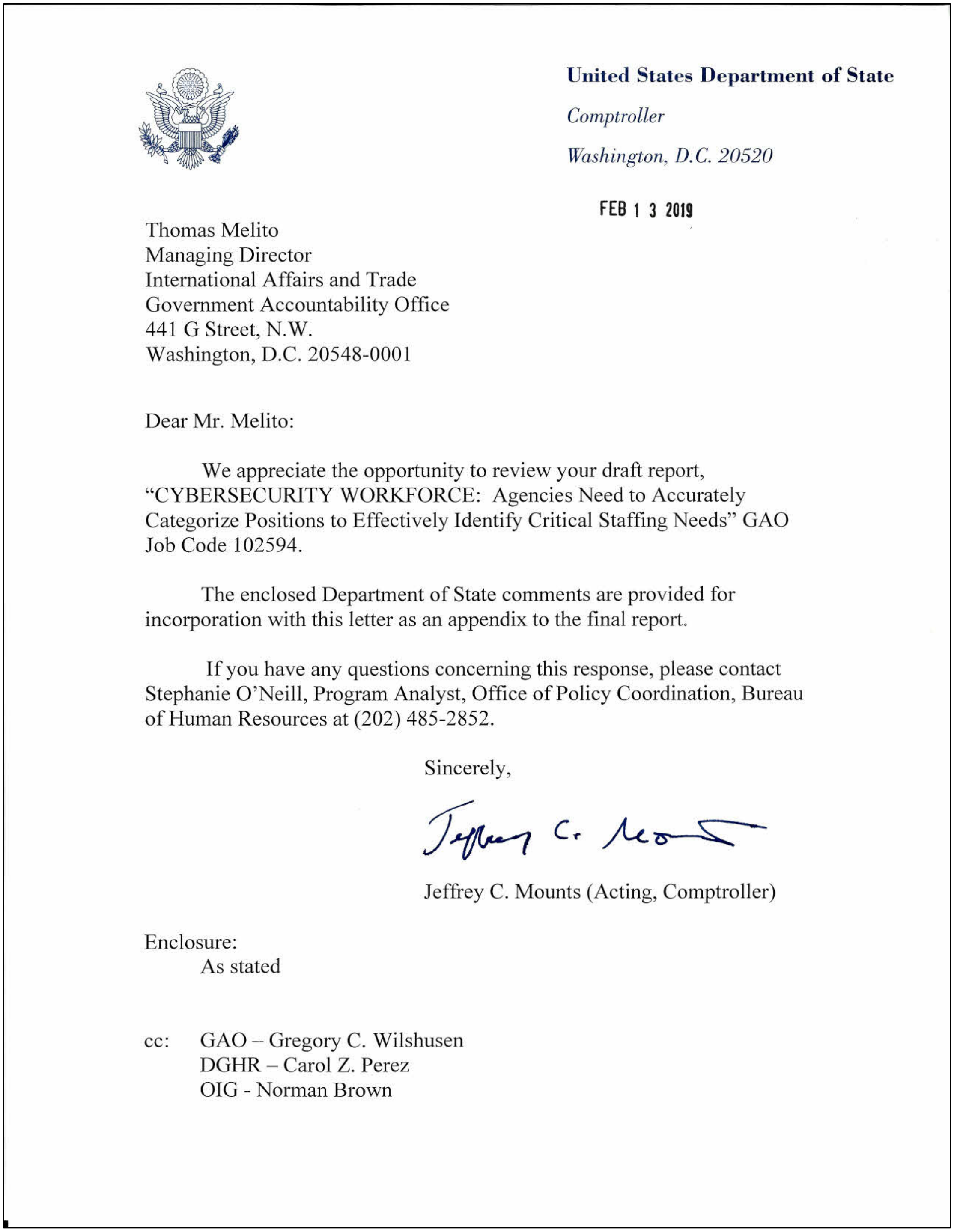
DOL Response: DOL concurs with the GAO recommendation. The Department has taken the necessary steps to review and code all Department of Labor 2210 IT position descriptions using the NICE framework, and update our systems with the correct cybersecurity fields for impacted positions.

Should you have any questions regarding the Department's response, please have your staff contact Gundeep Ahluwalia, Chief Information Officer, at (202) 693-4200.

Sincerely,

Bryan Slater
Assistant Secretary for
Administration and Management

Appendix XIII: Comments from the Department of State



United States Department of State

Comptroller

Washington, D.C. 20520

FEB 1 3 2019

Thomas Melito
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Melito:

We appreciate the opportunity to review your draft report, "CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs" GAO Job Code 102594.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Stephanie O'Neill, Program Analyst, Office of Policy Coordination, Bureau of Human Resources at (202) 485-2852.

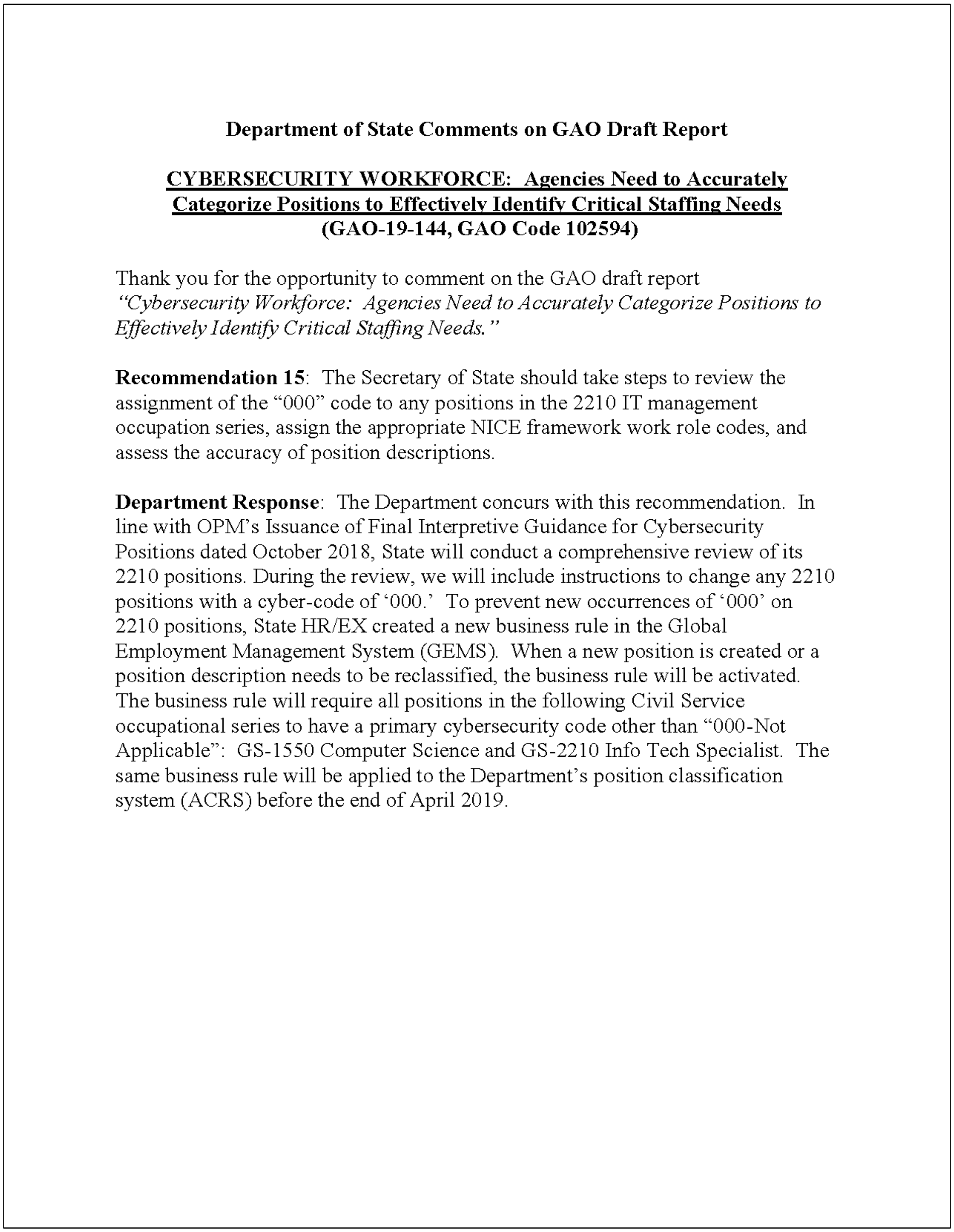
Sincerely,

Jeffrey C. Mounts

Jeffrey C. Mounts (Acting, Comptroller)

Enclosure:
As stated

cc: GAO – Gregory C. Wilshusen
DGHR – Carol Z. Perez
OIG - Norman Brown



Department of State Comments on GAO Draft Report

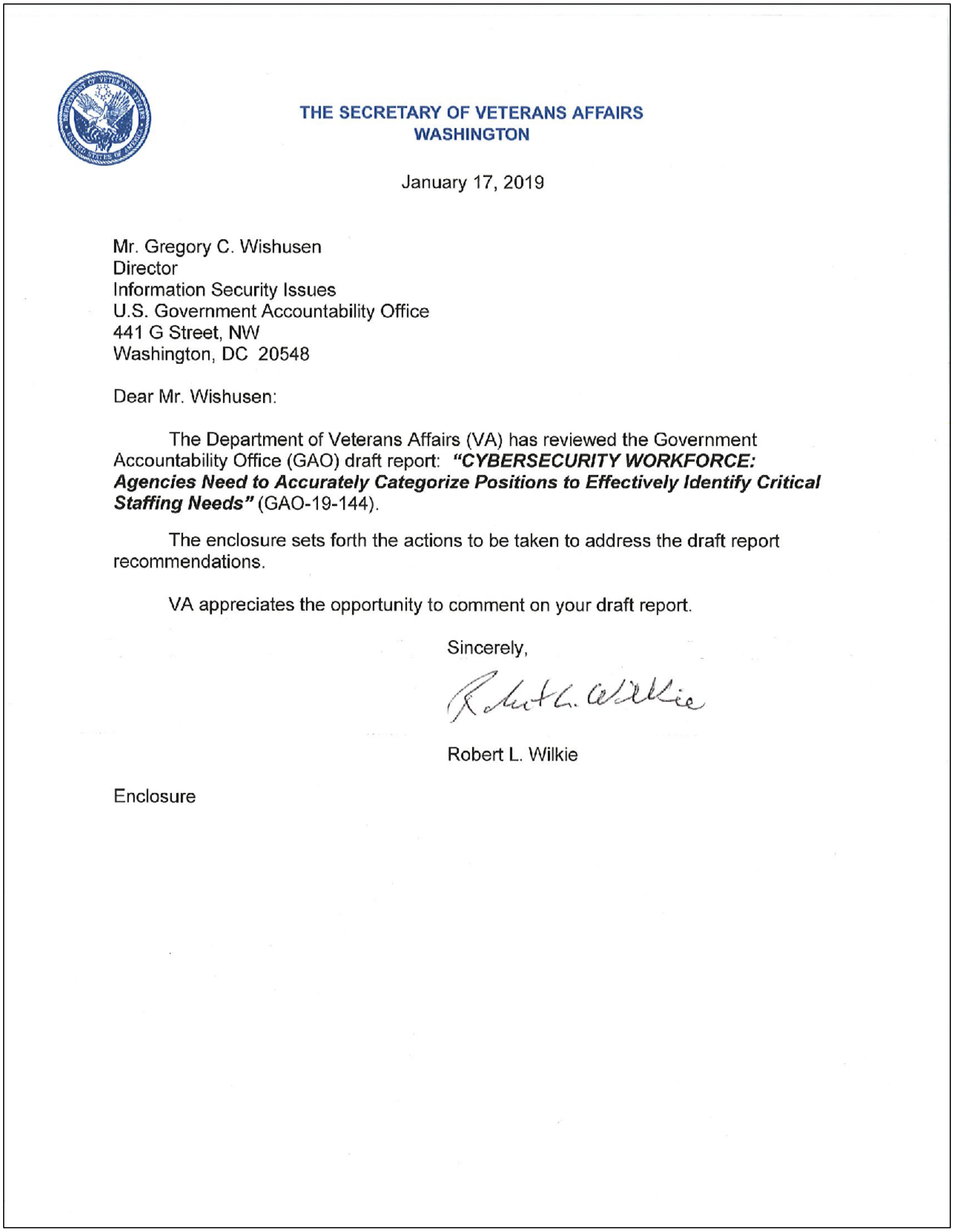
CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs
(GAO-19-144, GAO Code 102594)

Thank you for the opportunity to comment on the GAO draft report *"Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs."*

Recommendation 15: The Secretary of State should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series, assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions.

Department Response: The Department concurs with this recommendation. In line with OPM's Issuance of Final Interpretive Guidance for Cybersecurity Positions dated October 2018, State will conduct a comprehensive review of its 2210 positions. During the review, we will include instructions to change any 2210 positions with a cyber-code of '000.' To prevent new occurrences of '000' on 2210 positions, State HR/EX created a new business rule in the Global Employment Management System (GEMS). When a new position is created or a position description needs to be reclassified, the business rule will be activated. The business rule will require all positions in the following Civil Service occupational series to have a primary cybersecurity code other than "000-Not Applicable": GS-1550 Computer Science and GS-2210 Info Tech Specialist. The same business rule will be applied to the Department's position classification system (ACRS) before the end of April 2019.

Appendix XIV: Comments from the Department of Veterans Affairs



THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

January 17, 2019

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

Dear Mr. Wishusen:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***"CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs"*** (GAO-19-144).

The enclosure sets forth the actions to be taken to address the draft report recommendations.

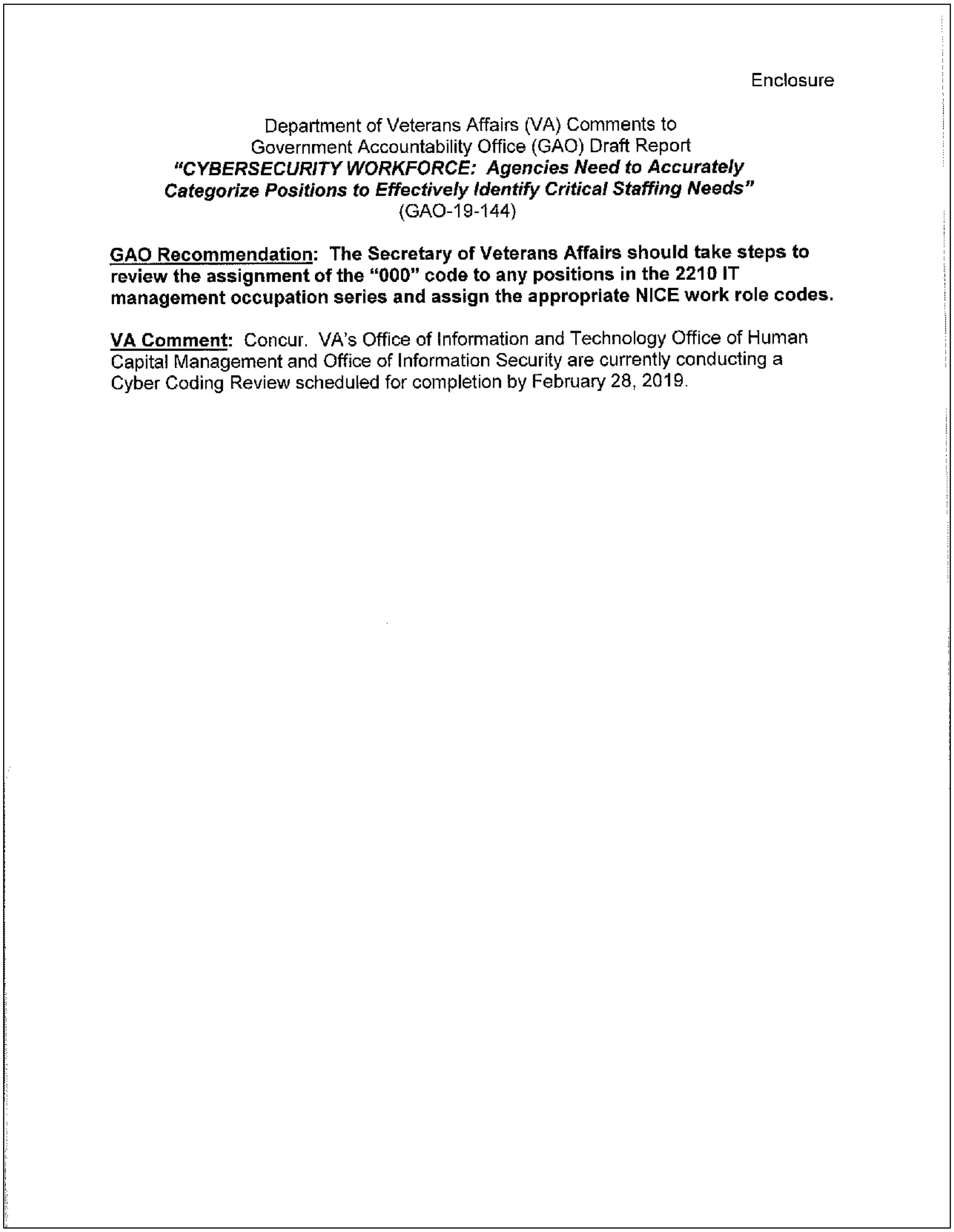
VA appreciates the opportunity to comment on your draft report.

Sincerely,

Robert L. Wilkie

Robert L. Wilkie

Enclosure



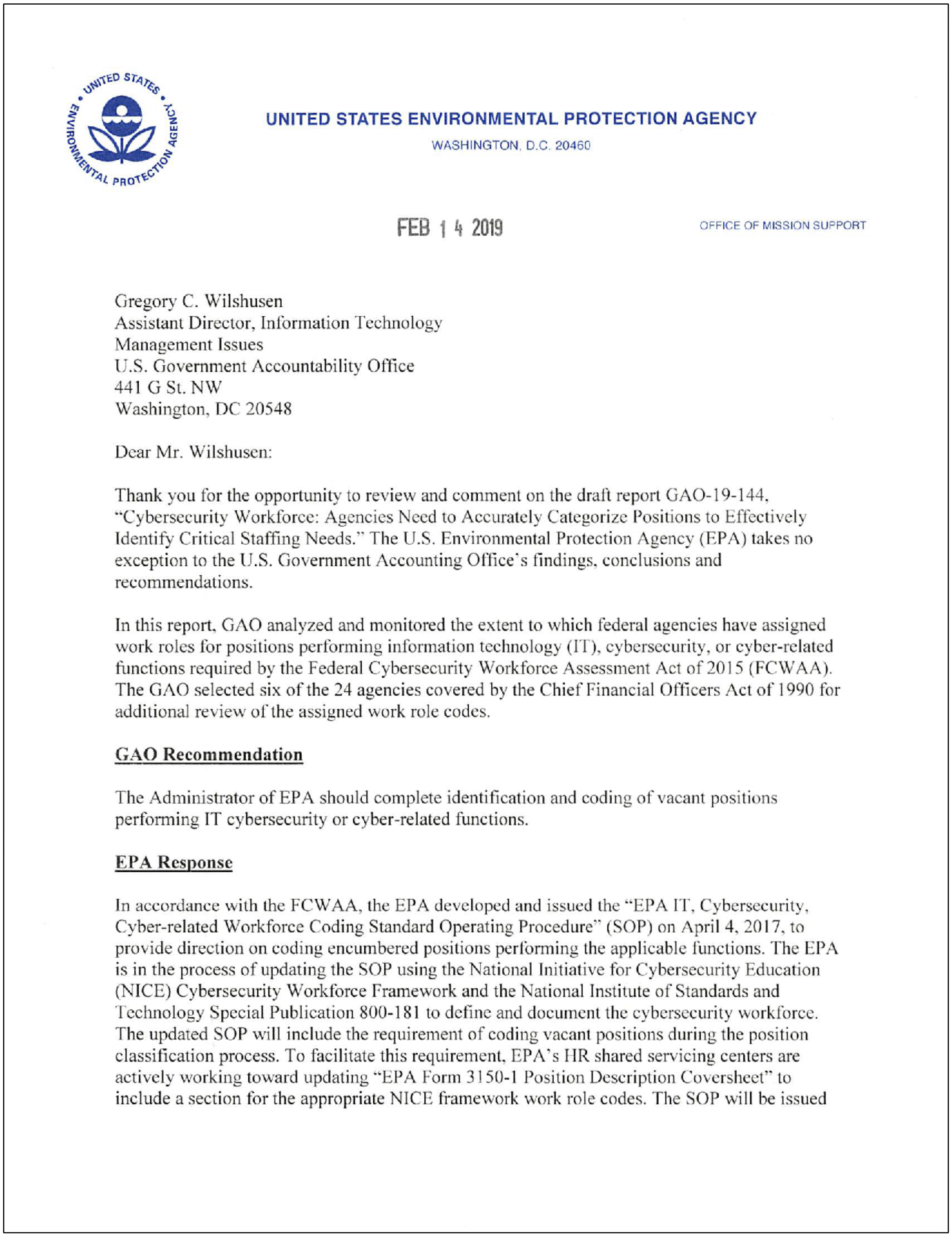
Enclosure

Department of Veterans Affairs (VA) Comments to
Government Accountability Office (GAO) Draft Report
"CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs"
(GAO-19-144)

GAO Recommendation: The Secretary of Veterans Affairs should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series and assign the appropriate NICE work role codes.

VA Comment: Concur. VA's Office of Information and Technology Office of Human Capital Management and Office of Information Security are currently conducting a Cyber Coding Review scheduled for completion by February 28, 2019.

Appendix XV: Comments from the Environmental Protection Agency



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

FEB 14 2019

OFFICE OF MISSION SUPPORT

Gregory C. Wilshusen
Assistant Director, Information Technology
Management Issues
U.S. Government Accountability Office
441 G St. NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the draft report GAO-19-144, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs." The U.S. Environmental Protection Agency (EPA) takes no exception to the U.S. Government Accounting Office's findings, conclusions and recommendations.

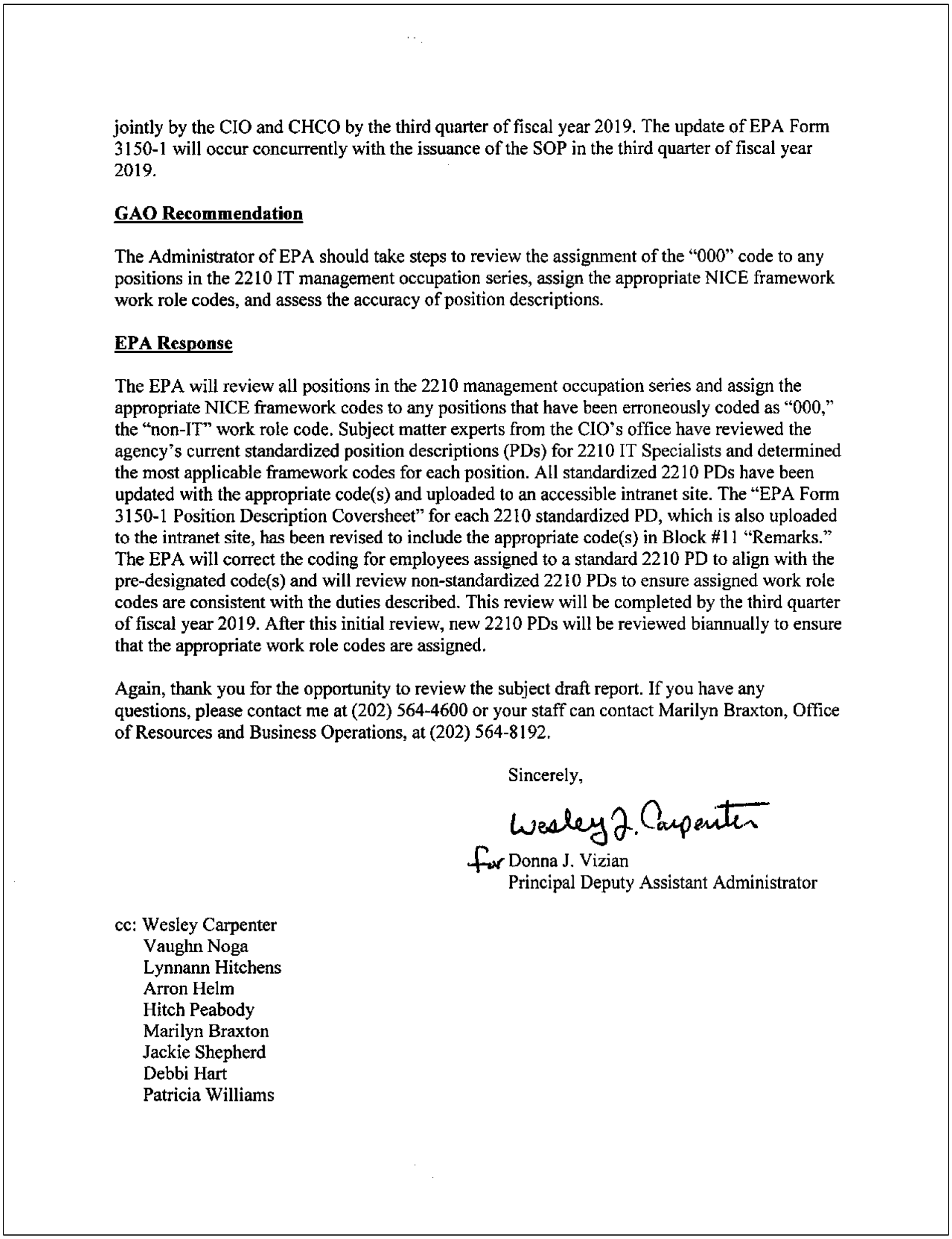
In this report, GAO analyzed and monitored the extent to which federal agencies have assigned work roles for positions performing information technology (IT), cybersecurity, or cyber-related functions required by the Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA). The GAO selected six of the 24 agencies covered by the Chief Financial Officers Act of 1990 for additional review of the assigned work role codes.

GAO Recommendation

The Administrator of EPA should complete identification and coding of vacant positions performing IT cybersecurity or cyber-related functions.

EPA Response

In accordance with the FCWAA, the EPA developed and issued the "EPA IT, Cybersecurity, Cyber-related Workforce Coding Standard Operating Procedure" (SOP) on April 4, 2017, to provide direction on coding encumbered positions performing the applicable functions. The EPA is in the process of updating the SOP using the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework and the National Institute of Standards and Technology Special Publication 800-181 to define and document the cybersecurity workforce. The updated SOP will include the requirement of coding vacant positions during the position classification process. To facilitate this requirement, EPA's HR shared servicing centers are actively working toward updating "EPA Form 3150-1 Position Description Coversheet" to include a section for the appropriate NICE framework work role codes. The SOP will be issued



jointly by the CIO and CHCO by the third quarter of fiscal year 2019. The update of EPA Form 3150-1 will occur concurrently with the issuance of the SOP in the third quarter of fiscal year 2019.

GAO Recommendation

The Administrator of EPA should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series, assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions.

EPA Response

The EPA will review all positions in the 2210 management occupation series and assign the appropriate NICE framework codes to any positions that have been erroneously coded as "000," the "non-IT" work role code. Subject matter experts from the CIO's office have reviewed the agency's current standardized position descriptions (PDs) for 2210 IT Specialists and determined the most applicable framework codes for each position. All standardized 2210 PDs have been updated with the appropriate code(s) and uploaded to an accessible intranet site. The "EPA Form 3150-1 Position Description Coversheet" for each 2210 standardized PD, which is also uploaded to the intranet site, has been revised to include the appropriate code(s) in Block #11 "Remarks." The EPA will correct the coding for employees assigned to a standard 2210 PD to align with the pre-designated code(s) and will review non-standardized 2210 PDs to ensure assigned work role codes are consistent with the duties described. This review will be completed by the third quarter of fiscal year 2019. After this initial review, new 2210 PDs will be reviewed biannually to ensure that the appropriate work role codes are assigned.

Again, thank you for the opportunity to review the subject draft report. If you have any questions, please contact me at (202) 564-4600 or your staff can contact Marilyn Braxton, Office of Resources and Business Operations, at (202) 564-8192.

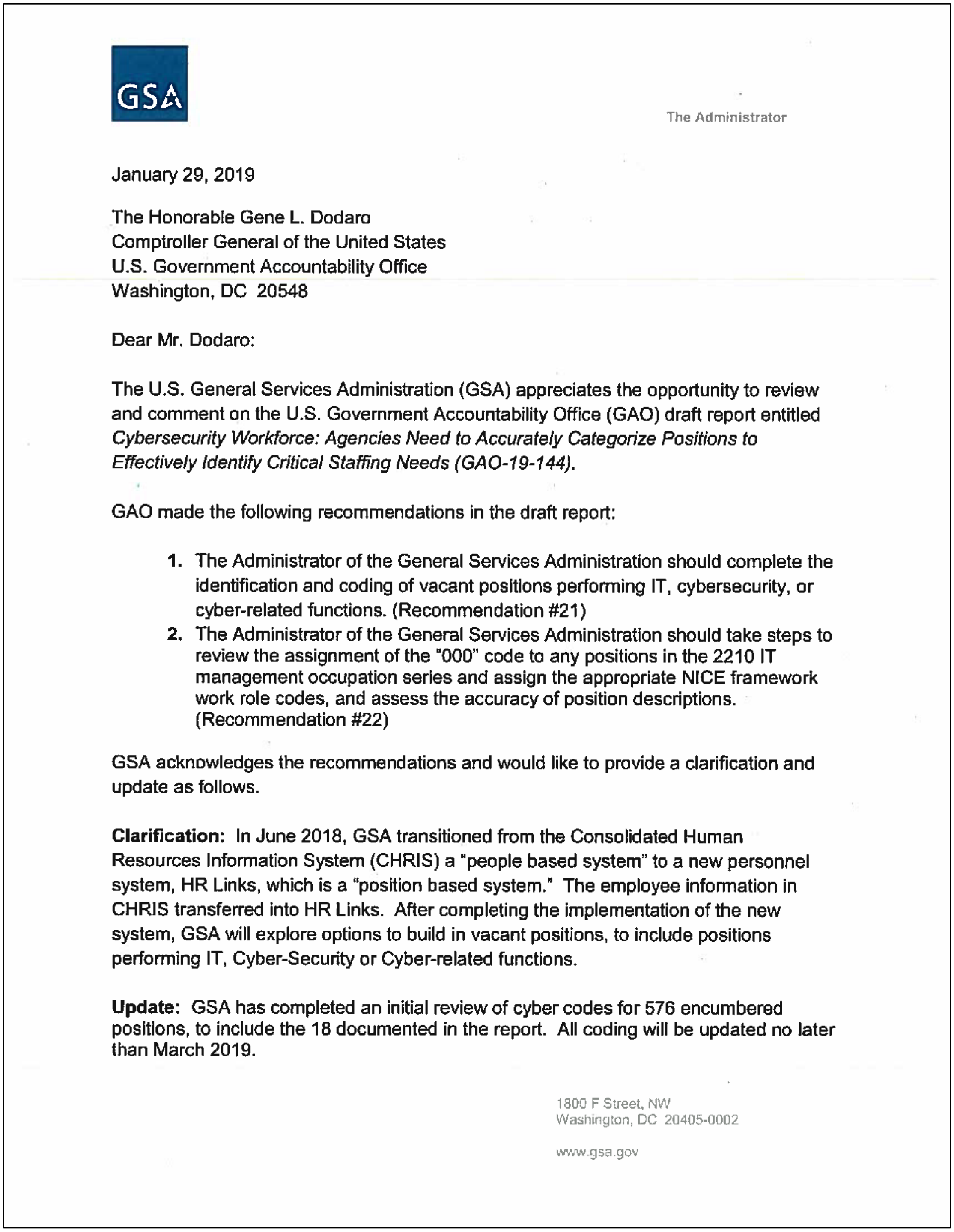
Sincerely,

Wesley J. Carpenter

for Donna J. Vizian
Principal Deputy Assistant Administrator

cc: Wesley Carpenter
Vaughn Noga
Lynnann Hitchens
Arron Helm
Hitch Peabody
Marilyn Braxton
Jackie Shepherd
Debbi Hart
Patricia Williams

Appendix XVI: Comments from the General Services Administration



The Administrator

January 29, 2019

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the U.S. Government Accountability Office (GAO) draft report entitled *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs (GAO-19-144).*

GAO made the following recommendations in the draft report:

1. The Administrator of the General Services Administration should complete the identification and coding of vacant positions performing IT, cybersecurity, or cyber-related functions. (Recommendation #21)
2. The Administrator of the General Services Administration should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series and assign the appropriate NICE framework work role codes, and assess the accuracy of position descriptions. (Recommendation #22)

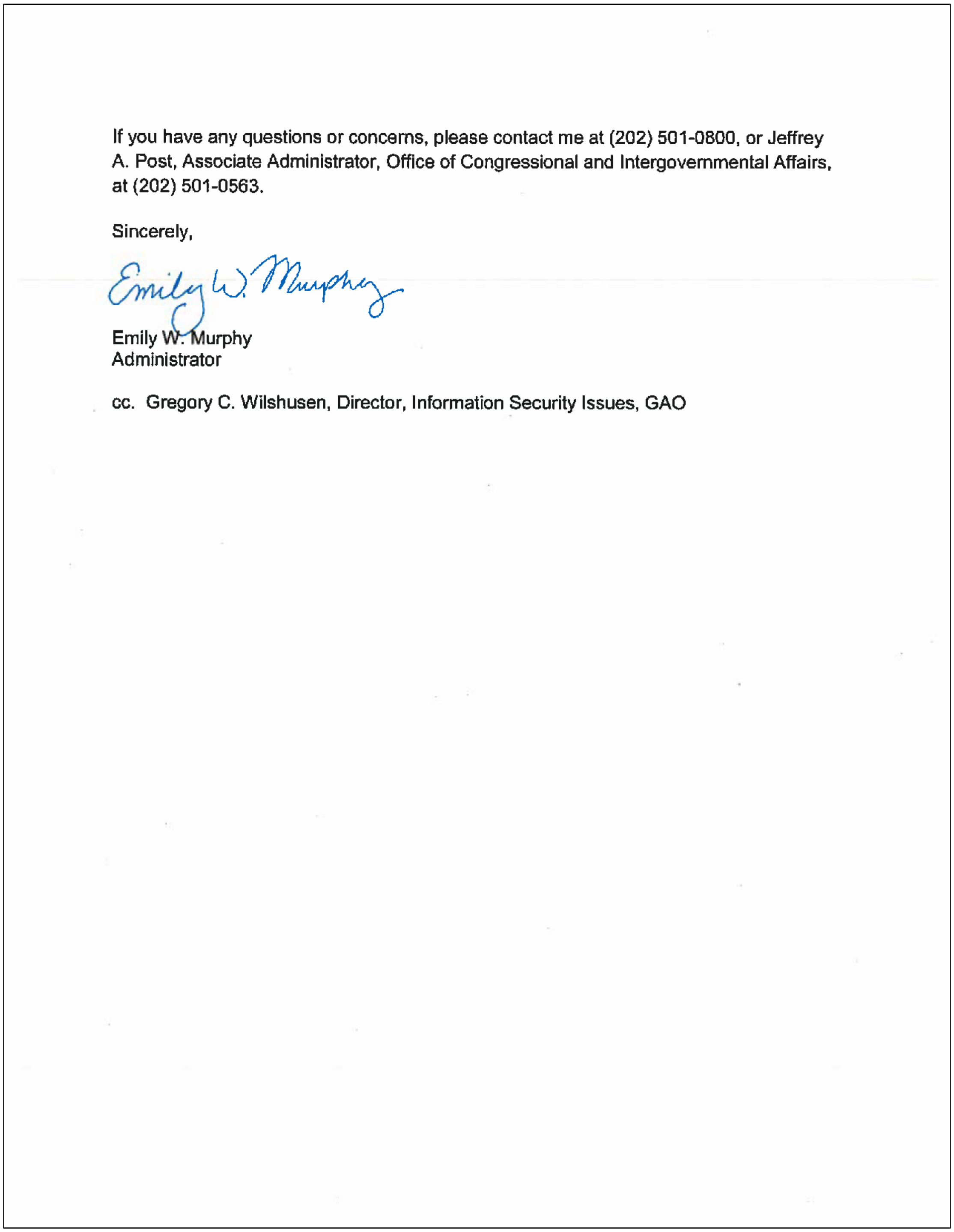
GSA acknowledges the recommendations and would like to provide a clarification and update as follows.

Clarification: In June 2018, GSA transitioned from the Consolidated Human Resources Information System (CHRIS) a "people based system" to a new personnel system, HR Links, which is a "position based system." The employee information in CHRIS transferred into HR Links. After completing the implementation of the new system, GSA will explore options to build in vacant positions, to include positions performing IT, Cyber-Security or Cyber-related functions.

Update: GSA has completed an initial review of cyber codes for 576 encumbered positions, to include the 18 documented in the report. All coding will be updated no later than March 2019.

1800 F Street, NW
Washington, DC 20405-0002

www.gsa.gov



If you have any questions or concerns, please contact me at (202) 501-0800, or Jeffrey A. Post, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

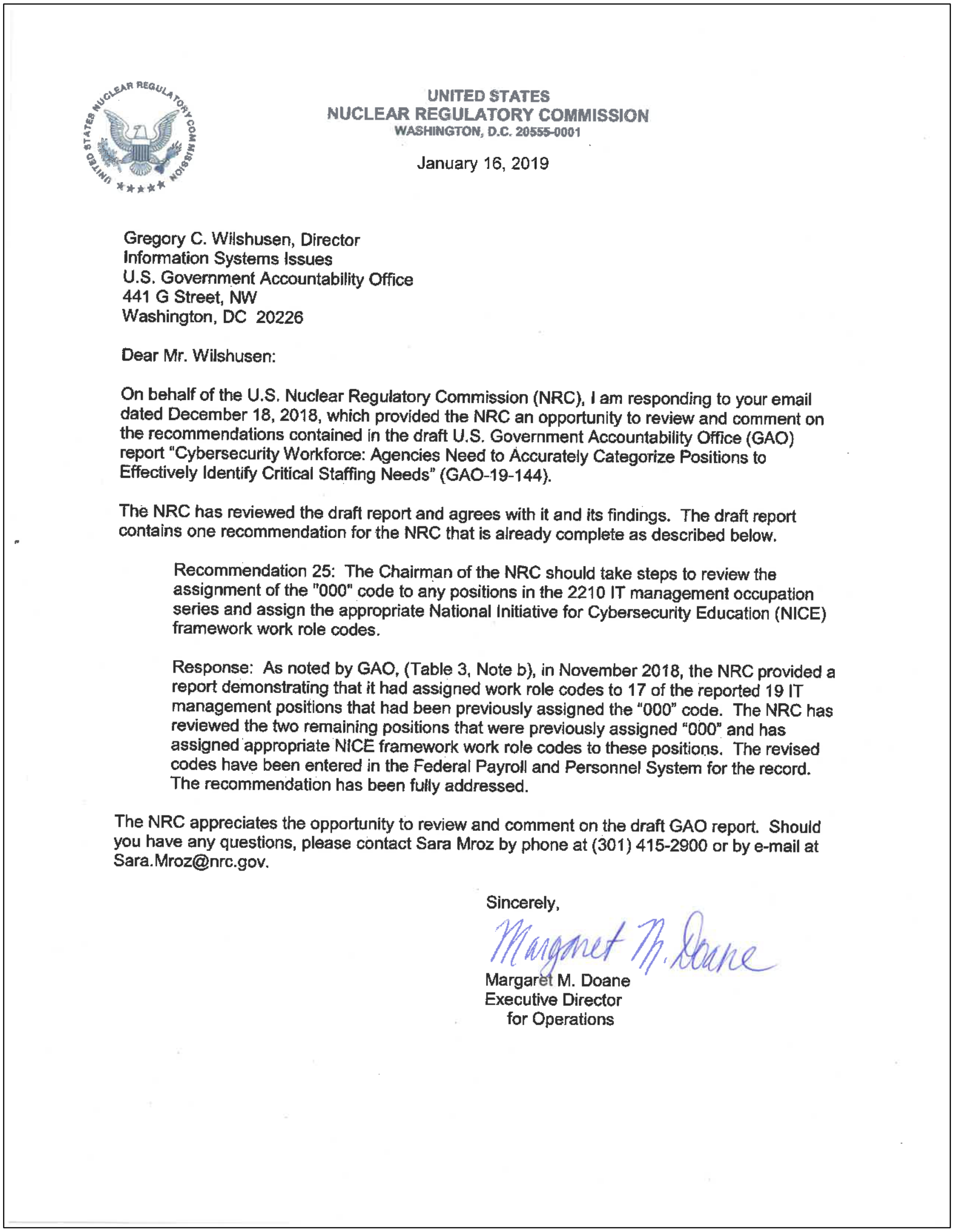
Sincerely,

Emily W. Murphy

Emily W. Murphy
Administrator

cc. Gregory C. Wilshusen, Director, Information Security Issues, GAO

Appendix XVII: Comments from the Nuclear Regulatory Commission



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

January 16, 2019

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

Dear Mr. Wilshusen:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to your email dated December 18, 2018, which provided the NRC an opportunity to review and comment on the recommendations contained in the draft U.S. Government Accountability Office (GAO) report "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs" (GAO-19-144).

The NRC has reviewed the draft report and agrees with it and its findings. The draft report contains one recommendation for the NRC that is already complete as described below.

> Recommendation 25: The Chairman of the NRC should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series and assign the appropriate National Initiative for Cybersecurity Education (NICE) framework work role codes.
>
> Response: As noted by GAO, (Table 3, Note b), in November 2018, the NRC provided a report demonstrating that it had assigned work role codes to 17 of the reported 19 IT management positions that had been previously assigned the "000" code. The NRC has reviewed the two remaining positions that were previously assigned "000" and has assigned appropriate NICE framework work role codes to these positions. The revised codes have been entered in the Federal Payroll and Personnel System for the record. The recommendation has been fully addressed.

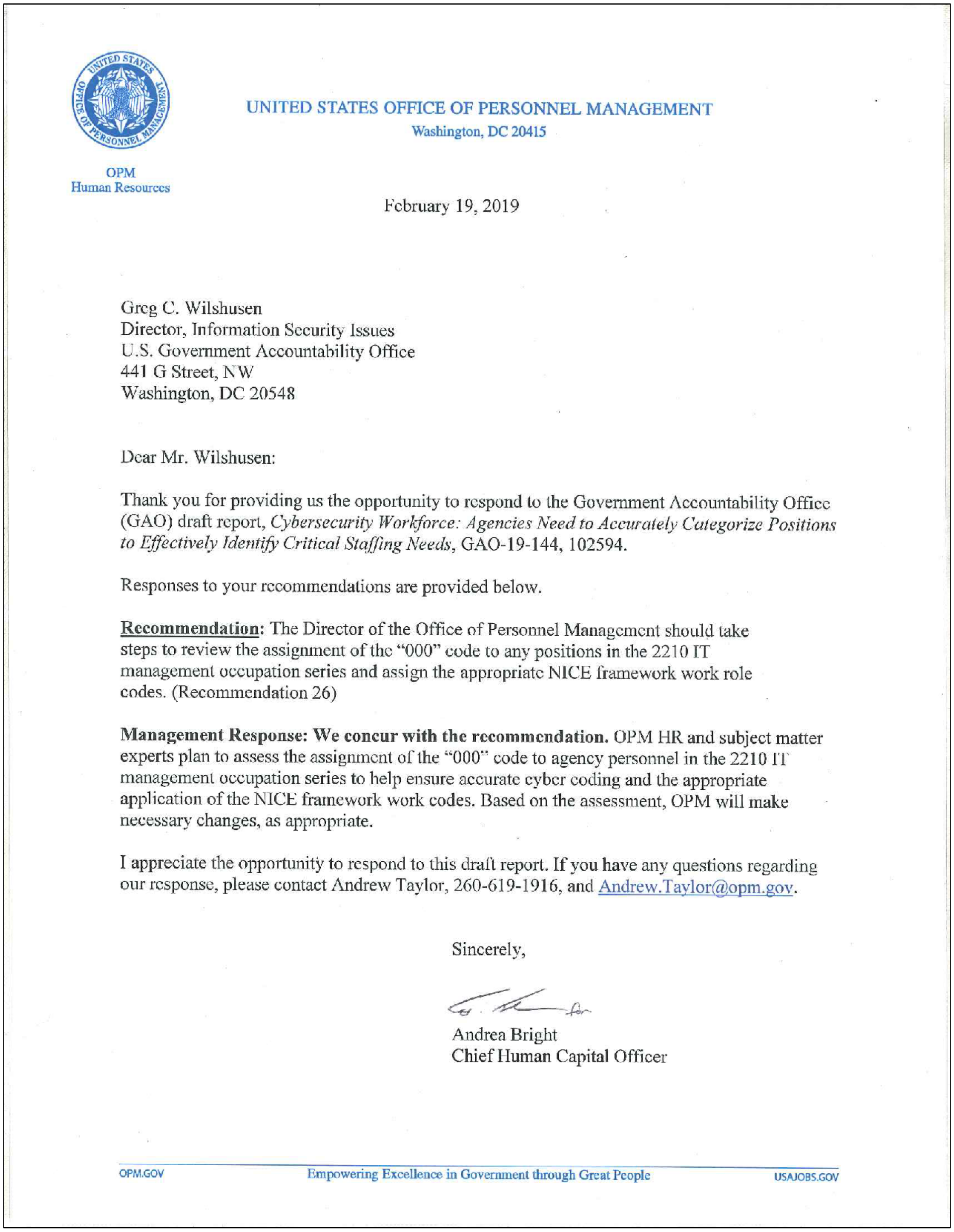
The NRC appreciates the opportunity to review and comment on the draft GAO report. Should you have any questions, please contact Sara Mroz by phone at (301) 415-2900 or by e-mail at Sara.Mroz@nrc.gov.

Sincerely,

Margaret M. Doane

Margaret M. Doane
Executive Director
for Operations

Appendix XVIII: Comments from the Office of Personnel Management



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

OPM
Human Resources

February 19, 2019

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

Dear Mr. Wilshusen:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144, 102594.

Responses to your recommendations are provided below.

Recommendation: The Director of the Office of Personnel Management should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series and assign the appropriate NICE framework work role codes. (Recommendation 26)

Management Response: We concur with the recommendation. OPM HR and subject matter experts plan to assess the assignment of the "000" code to agency personnel in the 2210 IT management occupation series to help ensure accurate cyber coding and the appropriate application of the NICE framework work codes. Based on the assessment, OPM will make necessary changes, as appropriate.

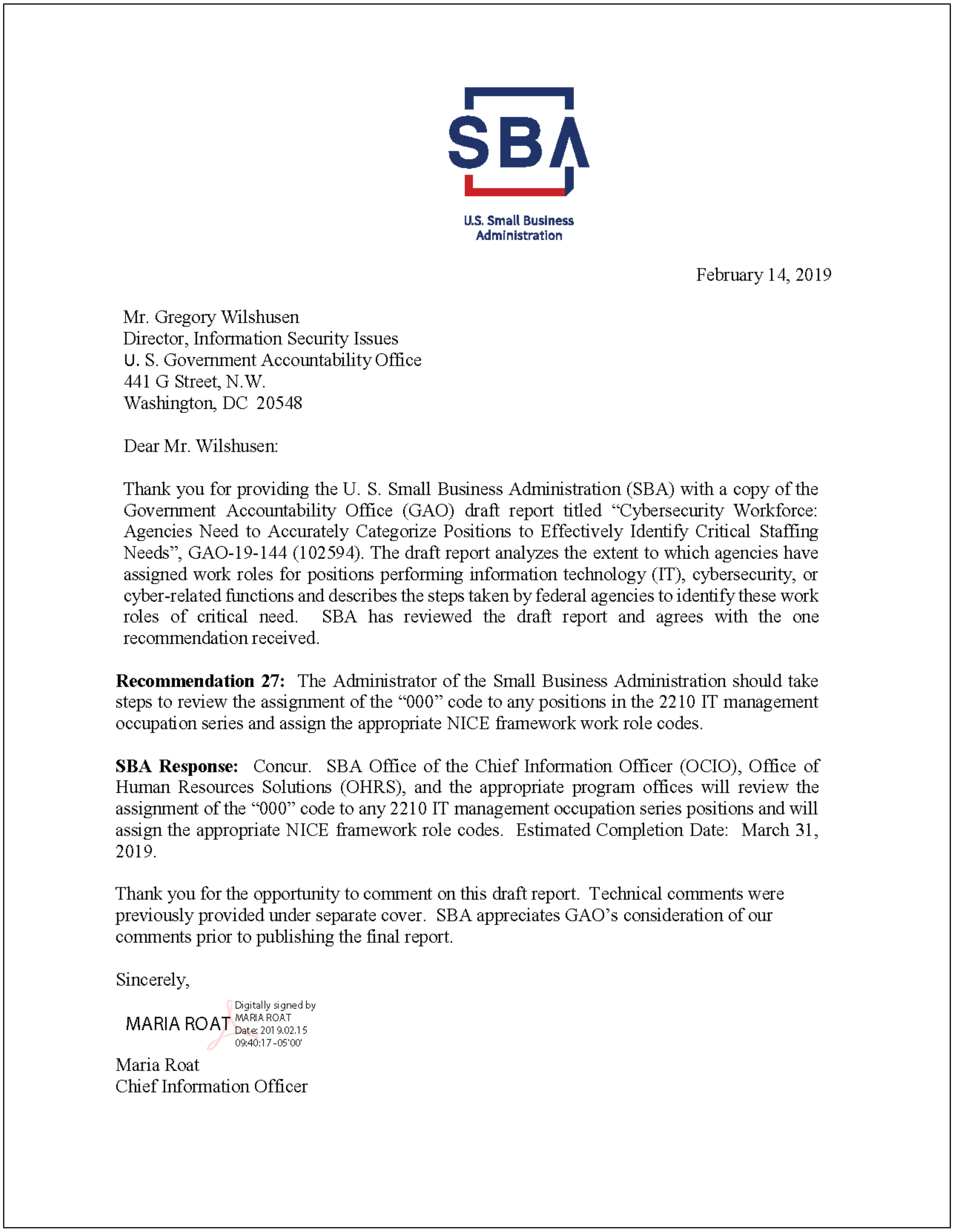
I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Andrew Taylor, 260-619-1916, and Andrew.Taylor@opm.gov.

Sincerely,

Andrea Bright
Chief Human Capital Officer

OPM.GOV   Empowering Excellence in Government through Great People   USAJOBS.GOV

Appendix XIX: Comments from the Small Business Administration



SBA

U.S. Small Business
Administration

February 14, 2019

Mr. Gregory Wilshusen
Director, Information Security Issues
U. S. Government Accountability Office
441 G Street, N.W.
Washington, DC 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 Accurately Categorize Positions to Effectively Identify Critical Staffing Needs", GAO-19-144 (102594). The draft report analyzes the extent to which agencies have assigned work roles for positions performing information technology (IT), cybersecurity, or cyber-related functions and describes the steps taken by federal agencies to identify these work roles of critical need. SBA has reviewed the draft report and agrees with the one recommendation received.

Recommendation 27: The Administrator of the Small Business Administration should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series and assign the appropriate NICE framework work role codes.

SBA Response: Concur. SBA Office of the Chief Information Officer (OCIO), Office of Human Resources Solutions (OHRS), and the appropriate program offices will review the assignment of the "000" code to any 2210 IT management occupation series positions and will assign the appropriate NICE framework role codes. Estimated Completion Date: March 31, 2019.

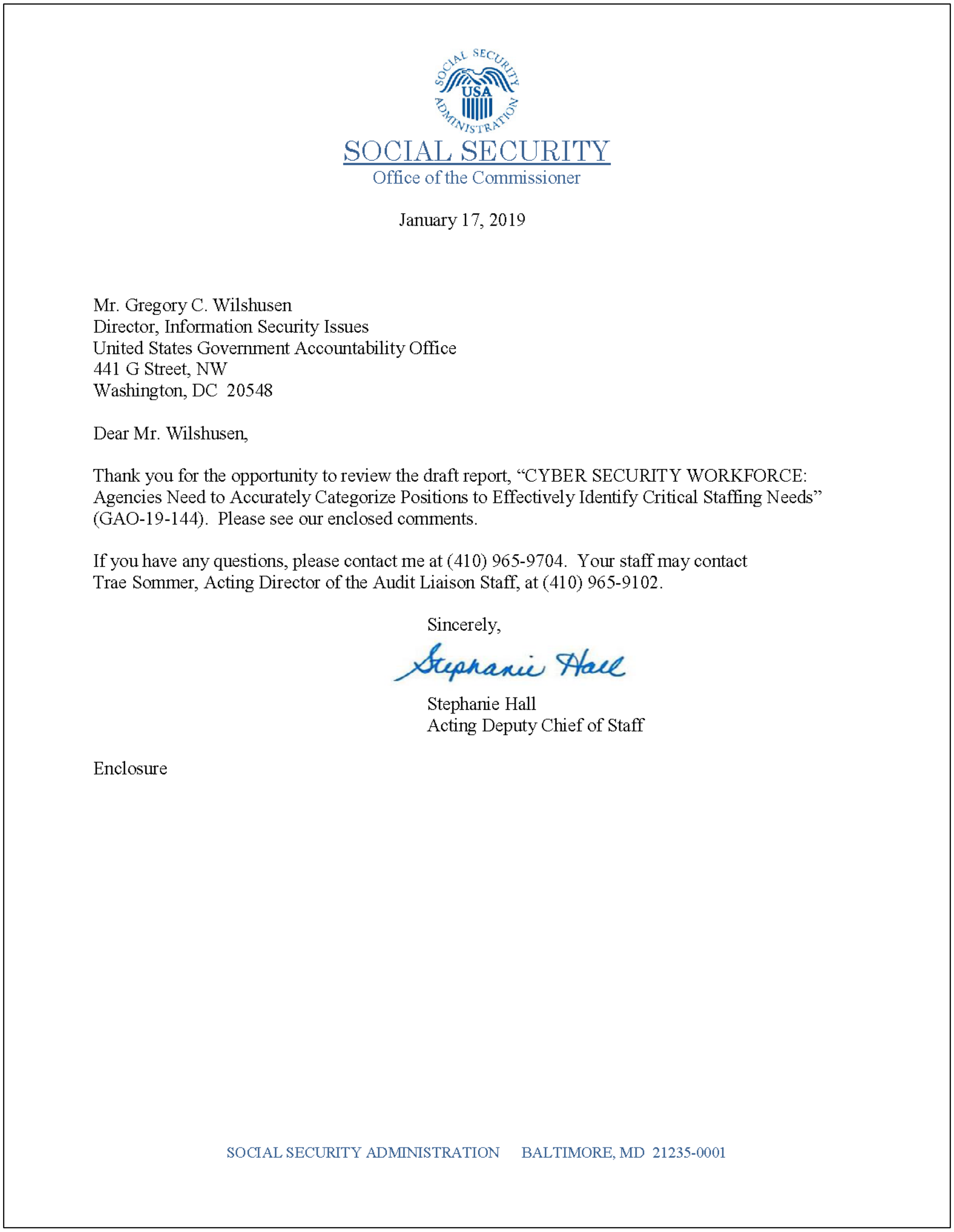
Thank you for the opportunity to comment on this draft report. Technical comments were previously provided under separate cover. SBA appreciates GAO's consideration of our comments prior to publishing the final report.

Sincerely,

MARIA ROAT
Digitally signed by
MARIA ROAT
Date: 2019.02.15
09:40:17 -05'00'

Maria Roat
Chief Information Officer

Appendix XX: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

January 17, 2019

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, “CYBER SECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs” (GAO-19-144). Please see our enclosed comments.

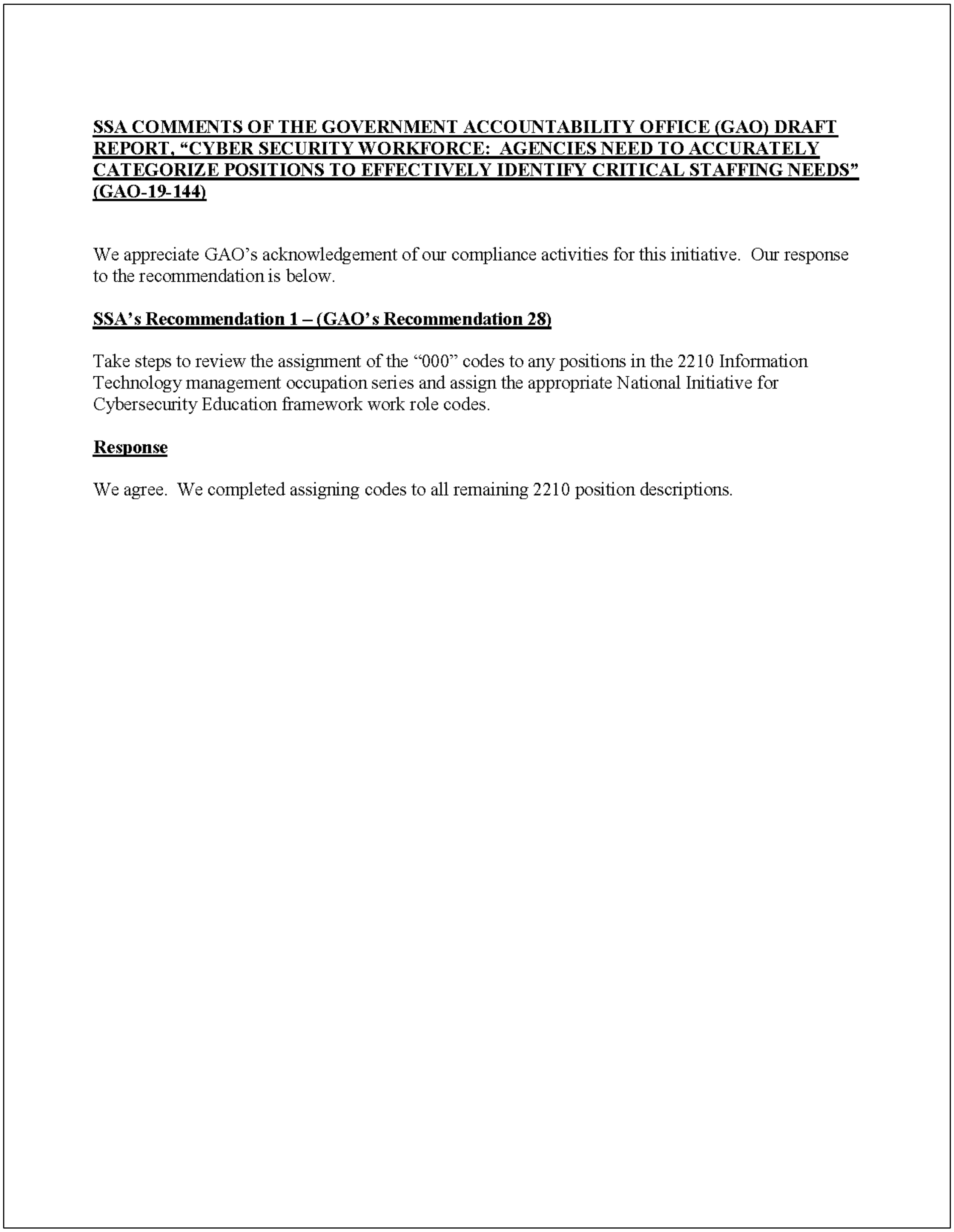
If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall

Stephanie Hall
Acting Deputy Chief of Staff

Enclosure



SSA COMMENTS OF THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT, "CYBER SECURITY WORKFORCE: AGENCIES NEED TO ACCURATELY CATEGORIZE POSITIONS TO EFFECTIVELY IDENTIFY CRITICAL STAFFING NEEDS" (GAO-19-144)

We appreciate GAO's acknowledgement of our compliance activities for this initiative. Our response to the recommendation is below.

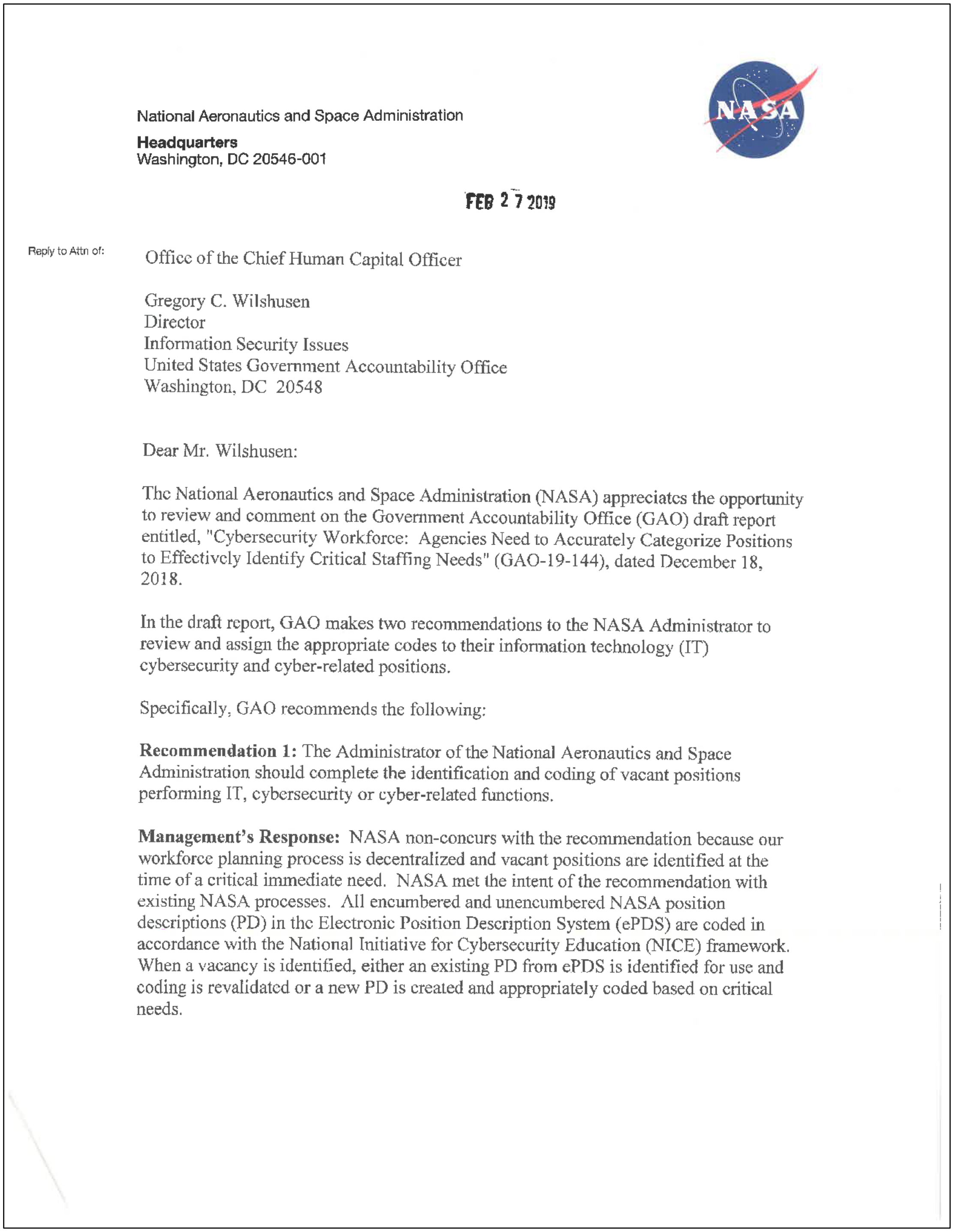
SSA's Recommendation 1 – (GAO's Recommendation 28)

Take steps to review the assignment of the "000" codes to any positions in the 2210 Information Technology management occupation series and assign the appropriate National Initiative for Cybersecurity Education framework work role codes.

Response

We agree. We completed assigning codes to all remaining 2210 position descriptions.

Appendix XXI: Comments from the National Aeronautics and Space Administration



National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-001

FEB 2 7 2019

Reply to Attn of: Office of the Chief Human Capital Officer

Gregory C. Wilshusen
Director
Information Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

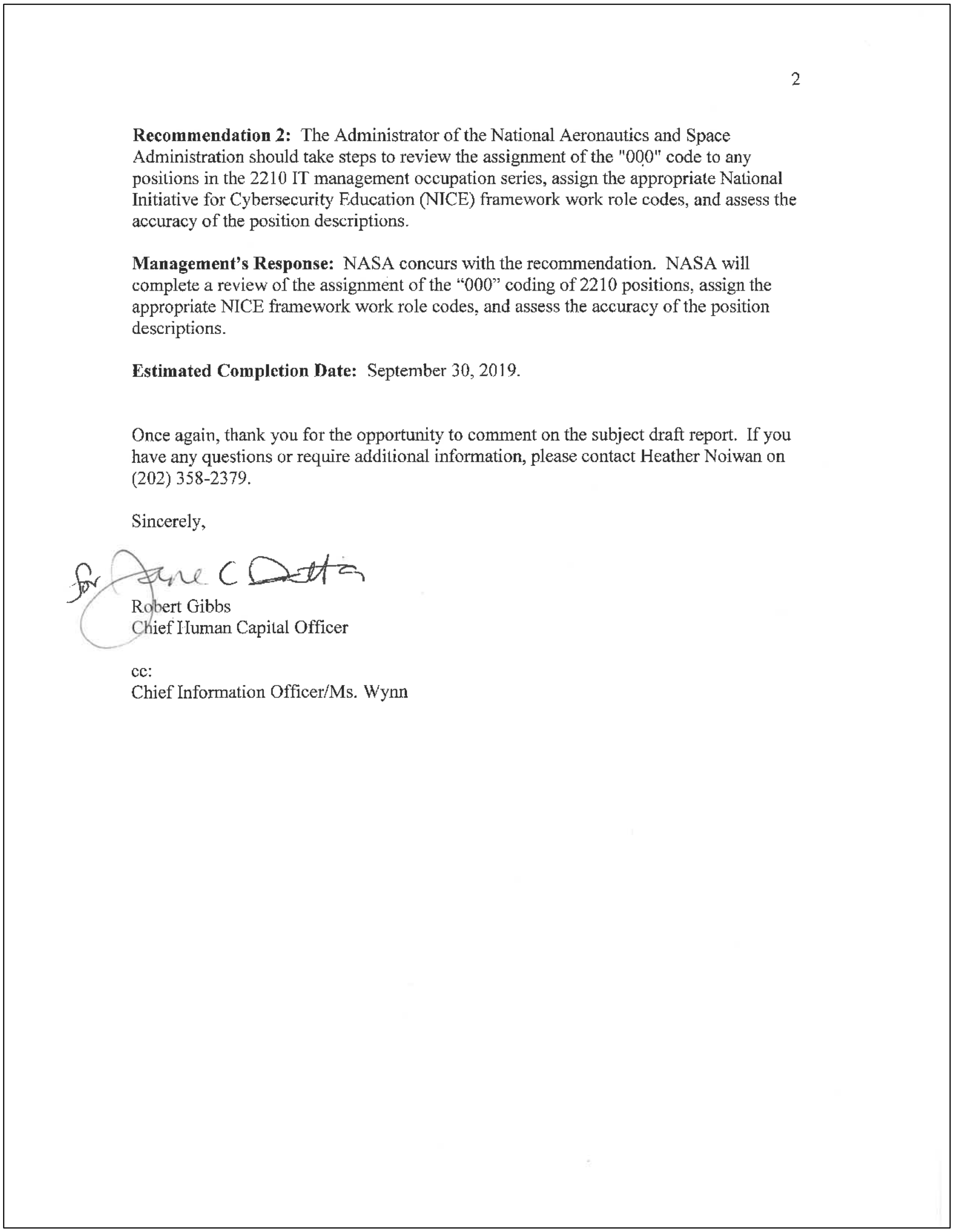
The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs" (GAO-19-144), dated December 18, 2018.

In the draft report, GAO makes two recommendations to the NASA Administrator to review and assign the appropriate codes to their information technology (IT) cybersecurity and cyber-related positions.

Specifically, GAO recommends the following:

Recommendation 1: The Administrator of the National Aeronautics and Space Administration should complete the identification and coding of vacant positions performing IT, cybersecurity or cyber-related functions.

Management's Response: NASA non-concurs with the recommendation because our workforce planning process is decentralized and vacant positions are identified at the time of a critical immediate need. NASA met the intent of the recommendation with existing NASA processes. All encumbered and unencumbered NASA position descriptions (PD) in the Electronic Position Description System (ePDS) are coded in accordance with the National Initiative for Cybersecurity Education (NICE) framework. When a vacancy is identified, either an existing PD from ePDS is identified for use and coding is revalidated or a new PD is created and appropriately coded based on critical needs.



Recommendation 2: The Administrator of the National Aeronautics and Space Administration should take steps to review the assignment of the "000" code to any positions in the 2210 IT management occupation series, assign the appropriate National Initiative for Cybersecurity Education (NICE) framework work role codes, and assess the accuracy of the position descriptions.

Management's Response: NASA concurs with the recommendation. NASA will complete a review of the assignment of the "000" coding of 2210 positions, assign the appropriate NICE framework work role codes, and assess the accuracy of the position descriptions.

Estimated Completion Date: September 30, 2019.

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.

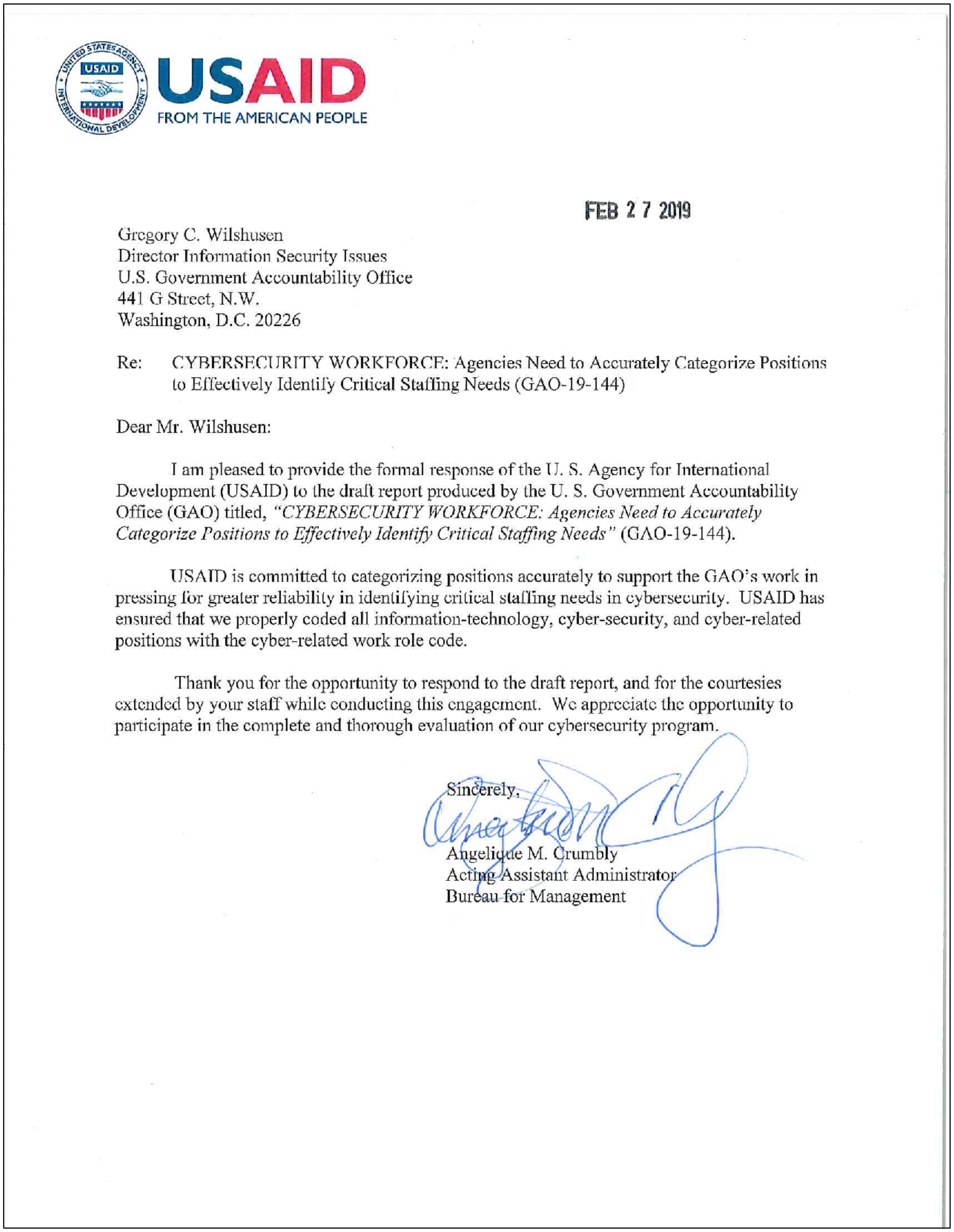
Sincerely,

for Jane C Datta

Robert Gibbs
Chief Human Capital Officer

cc:
Chief Information Officer/Ms. Wynn

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



USAID
FROM THE AMERICAN PEOPLE

FEB 27 2019

Gregory C. Wilshusen
Director Information Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

Re: CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs (GAO-19-144)

Dear Mr. Wilshusen:

I am pleased to provide the formal response of the U. S. Agency for International Development (USAID) to the draft report produced by the U. S. Government Accountability Office (GAO) titled, *"CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs"* (GAO-19-144).

USAID is committed to categorizing positions accurately to support the GAO's work in pressing for greater reliability in identifying critical staffing needs in cybersecurity. USAID has ensured that we properly coded all information-technology, cyber-security, and cyber-related positions with the cyber-related work role code.

Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our cybersecurity program.

Sincerely,

Angelique M. Crumbly
Acting Assistant Administrator
Bureau for Management

Appendix XXIII: 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, Tammi Kalugdan (Assistant Director), Merry Woo (Analyst-in-Charge), Carlos (Steven) Aguilar, Alexander Anderegg, Christina Bixby, Carl Barden, Chris Businsky, Virginia Chanley, Cynthia Grant, Paris Hawkins, Lee Hinga, James (Andrew) Howard, Assia Khadri, David Plocher, Steven Putansu, and Priscilla Smith made significant contributions to this report.

(102594)

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) 512-7700

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

Please Print on Recycled Paper.