PUBLIC COMMENTS
FOR THE
AMERICAN WORKFORCE
PUBLIC ADVISORY BOARD

PLEDGE TO AMERICA'S WORKERS

American Workforce Policy Advisory Board
June 18, 2019 Meeting Public Comments

Contents

AWPAB Public Comments - received prior to June 12, 2019, 5:00 p.m. (EST) deadline

1. Michelle Mosey, CEO North America, WithYouWithMe

From: Michelle Mosey <michelle@withyouwithme.com>

Sent: Monday, June 10, 2019 3:04 PM

To: AmericanWorkforcePolicyAdvisoryBoard

Cc: Sam Baynes; Cody Hoefer

Subject: June 2019 Advisory Board Meeting Public Comment

Dear Sir/Madam,

Please find attached WithYouWIthMe statement to the June 2019 Advisory Board Meeting on Workforce Policy - specifically relating to:

- Develop a Campaign to Promote Multiple Pathways to Career Success;
- Increase Data Transparency to Better Match American Workers with American Jobs;
- Modernize Candidate Recruitment and Training Practices; and
- Measure and Encourage Employer-led Training Investments

I look forward to engaging with you further on this critical issue.

Cheers,

Michelle

Michelle Mosey

CEO North America

WithYouWithMe
M: +1 202 492 2244

Attachments:

1. WithYouWIthMe statement on WhiteHouse Advisory Board.PDF
2. 190129_Crumpler_Cybersecurity_FINAL.pdf
3. Urgent actions for cyberskills crisis.pdf
4. Accurate categorization of positions.pdf
5. About Us – WithYouWithMe Jun 2019

WITH
YOU
WITH
ME

To Whom it May Concern,

In response to the call for submission to the Under Secretary for Economic Affairs and the second meeting of the American Workforce Policy Advisory Board. WithYouWithMe thanks the Board for the opportunity to contribute to this solution.

WithYouWithMe is a company that builds talent, based on data and driven by data. We have developed a unique approach that assists individuals to upskill and reskill in high-tech training that is driven by data. We link training and courses to labor market job data to ensure the right skills are being delivered into the workforce.

WithYouWithMe submits an outline for consideration of the Board on how the challenges and solutions to build an effective campaign to meet the outcomes identified in the Cyber Executive Order, dated May 2, 2019. Specifically items:

(i) To launch a national Call to Action to draw attention to and mobilize public- and private-sector resources to address cybersecurity workforce needs;

(ii) To transform, elevate, and sustain the cybersecurity learning environment to grow a dynamic and diverse cybersecurity workforce;

(iii) To align education and training with employers' cybersecurity workforce needs, improve coordination, and prepare individuals for lifelong careers; and

(iv) To establish and use measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

Responses:

Goal 1: Multiple Pathways to Career Success. Companies, workers, parents, and policymakers have traditionally assumed that a university degree is the best, or only, path to a middle-class career. Employers and job seekers should be aware of multiple career pathways and skill development opportunities outside of traditional 4-year degrees.

WithYouWithMe fervently disagree with the notion that a university degree is the one, if not the only, path to the middle class. We disagree with this for a few reasons:

- Evident in data. Look at any entry level job post. Those requiring high-tech skills start at a minimum salary of $60-90k. Most entry level jobs for students graduating from traditional university areas of study, start at ~$35-45k.

- Skills vs education. As mature service economies advance, high-tech skills constitute the bulk of in-demand skills in the labor market. These include skills in software engineering, cybersecurity, robotic process automation, data science, IT management and cloud. Education cannot keep pace with technological improvement, so resort to teaching high-level policy and theory. These insights are not required in the workplace until middle-senior management. You cannot earn an entry level position with an education – for entry level positions, you need skills.

- Technological evolution cycle. Technology is accelerating in its evolution. Meaning, high-tech professionals need to continue to study and upskill every year to remain current. You no longer study at the beginning of your career. You must annually study and upskill throughout your entire career.

- University model broken. Universities take on average about four years from decision to build a new course to graduation of first cohort. By the time the first cohort graduates, the curriculum, designed three years ago, is out of date because technology advances to quickly. Universities must teach high-level, slower moving policy therefore or shorten their courses significantly and drop their prices; no one will pay $100,000 for a six week course.

- Mass-market education. All education providers train as many people as they can as their business model is centered around student payment. Mass market education results in the training of far more people than there are jobs available. Additionally courses and training are not linked to job market gaps. This generates a glut of people with debt and no income, causing increase in youth depression. For example, Australia trains and graduates 12,000 lawyers a year. There are only 1200 positions in law, filled and non filled, in Australia at any one time.

- Senior level positions require skills. To be a senior level manager at a company that uses technology in its services (almost all in 2019), senior managers must understand the technology in order to make informed business decision. In 2019, a degree in high-tech is almost more valuable to a mid-level manager looking to jump to the senior level, than an MBA.

Goal 2: Increase Data Transparency to Better Match American Workers with American Jobs. High-quality, transparent, and timely data can significantly improve the ability of employers, students, job seekers, education providers, and policymakers to make informed choices about education and employment—especially for matching education and training programs to in-demand jobs and the skills needed to fill them.

WithYouWithMe agrees that all stakeholders need drastically more data upon which to make informed decision and allocation of resources (time, money, effort). Let’s break it down by demographic:

Employers. Employers benefit from the following data:

- Where is the skilled labor? Helps them choose where to locate office buildings in order to attract the talent they need to deliver their services to their clients.

- How much does the skilled labor cost? This assists so they can set competitive, yet fair salary caps for their roles.

Students. Students benefit from the following data:

- What skills are in demand? What skills are employers looking to hire.

- How do I develop in-demand skills? Where can I go and what resources can I use to develop in-demand skills?

- How much does education and training cost? How much will it cost to develop in-demand skills?

- Where are the jobs? If I develop the in-demand skills, where are the jobs? I want to develop skills that are in-demand in the place I want/need to live.

- Salaries. How much will I be paid if invest in learning these in-demand skills? Will it pay off any debt I must accept to develop skills?

Education providers. Education providers benefit from the following data:

- What skills are in demand? What skills are employers looking to hire so they can build education content to supply the demand.

- How many jobs are there available? Universities should not train more people than the market needs. Otherwise they will cause mass unemployment which results in decreases in mental health.

- Where do my students come from and where are they going? Universities should be aligning their intake of students with the job market they are planning to enter on graduation. This allows them to deliver education aligned to the labor markets in need. If they only study the US labor market in general, they cannot robustly develop educational content aligned with employment outcomes.

Policy Makers. Policy makers benefit from the following data:

- Skill gaps. What are the major skills gaps in the labor market? Where is there a huge demand for skills by employers and undersupply of skilled labor?

- Required skills. Once skill gaps are identified, what actual skills do entry level people need to do the jobs required by employers? What actual skills will ensure the entry level graduate is a contributing member of the team to the employer form day 1, and thus revenue generating?

- How big is the skills gap? The way we historically and currently assess skills shortages is wrong. Tax and census data, combined with market growth reports, can no longer be used to assess workforce needs because; job titles vary too much to develop robust data pools; job title change every year as technology develops so you can't link years together to develop accurate skill shortage trajectories/cones; most high-tech hasn't been around long enough to fill a reliable statistical model to develop future projections off; etc. The alternative approach which is to scrape job boards is not accurate either because the ecosystem of recruiters and job boards results in one job being advertised 30 times, and so 100 jobs in reality are believed to be 3000 jobs. Either way, all modern efforts to assess skills shortages are wildly inaccurate.

- Institutions to support. Which education and training institutions are actually teaching these identified skills, and how much funding do they need to scale their program to train people at the rate needed to enable the economy?

WithYouWithMe is working to provide all four stakeholders with this information through the following means:

- **Labor market reports**. WYWM develops and publishes labor market reports from information garnered by WYWM staff from working closely with small, medium and large companies project and client facing team to determine who many jobs they will need in the future, and what skills are needed now and in the future.

- **Labor market media**. WYWM produces weekly podcasts on the lessons they have learned about the labor market in their exploration. This includes interviewing employers, job seekers, WYWM staff, etc. and asking about what they learned about what skills are needed, where those skill are in high demand and where they aren't, and what people can do to earn those skills quickly and cheaply.

- **Testing platform**. Systematically testing people across al sectors to identify the aptitude and psychometric profile indicative of someone best suited to specific roles. For example, we know what concoction of aptitude and psychometric results are best suited to be successful as a cybersecurity analyst versus a cybersecurity penetration tester. By identifying these data profiles, we can match people form non-high-tech backgrounds to training that will excel and enter that labor market. This greatly expands the scope of people you can recruit from, rather than just software engineering students from university.

- **Training platform**. WYWM has built it owns successful services companies in high-tech trades. This allows us to win work and learn for ourselves exactly what skills are needed in the labor market. We then build short hard skills courses to rapidly upskill people matched to that career to work in our companies. Once validated, we open our training to other companies to test their won staff and retrain their staff from within.

- **Build labor forces**. For companies looking to expand rather than retrain their existing staff, employers can crate job ads through our SaaS platform, click 'match' and be matched to local graduates of WYWM's training that have been matched to that company by skill and cultural fit. If there are no local WYWM graduates WYWM will build the talent pool in location for the client for a small fee.

- **Study labor markets**. We constantly study labor markets, test and validate our courses and update them as needed as technology and thus the required skills evolves. This ensures we are constantly producing the talent employers need.

Goal 3: Modernize Candidate Recruitment and Training Practices. Employers often struggle to fill job vacancies, yet their hiring practices may actually reduce the pool of qualified job applicants. To acquire a talented workforce, employers must better identify the skills needed for specific jobs and communicate those needs to education providers, job seekers, and students.

WithYouWithMe has identified the following problems with modern recruitment practices, that combined, are causing an artificial skill shortage.

- **HR and recruiter education**. These personnel are not trained in high-tech and more often than not, do not work closely enough with the hiring managers to understand what is needed in the next hire.

- **Job ads are wrong**. The high-tech knowledge gap in HR and recruiters results in copying and pasting jobs ads from other public job ads, or, building jobs ads with far more minimum requirements than needed to de-risk themselves. Either way, the barrier to entry to these jobs becomes far too high for recent graduates and so the labor pool for these jobs becomes smaller and smaller as the few that got in early are traded between companies like baseball cards; this also results in higher costs to employers who have to pay increases salary limits for the diminishing labor pool and thus increase in demand for them.

- **Recruiter business model**. Recruiters make money out of trading people between companies like a commodity. If they place someone in one company, recruiters will remain in touch with the person until the are ready to leave and the help them get their next job. All the while increasing their commission as the persons value in the market increases. This model rewards a limited supply of skilled labor as the less there is, the higher the salary and thus the higher commission. Recruiters do not want more labor in the market, and as they are often the 'subject matter experts' that guide employers on what skills are needed and how much they are worth, they suffocate the market.

- **Perception**. High-tech is still perceived to be difficult. It used to be, over ten years ago when none of the infrastructure existed to make high-tech easy. For example, you used to have to be a software engineer to build an application for your network to manage it. Today, you can buy a tool out of the box that once installed you can manage your network. This has changed the skills required to be successful in a role today. What is needed is an understanding of what to use the tool for and an aptitude to learn how to use it. This is far easier than learning to be a software engineer and can be taught in as little at four to six weeks. This fact hasn't become modern, wide spread perception yet however, deterring many from entering these trades.

WithYouWithMe is solving all these problems by doing the following:

- Building a course to 'demystify high-tech' for HR and Recruitment professionals. This should educate them on the mistakes they have been making and how to really evaluate skills aligned to high-tech careers.

- Eradicating resumes. WYWM built a SaaS platform that HR and recruitment staff can use to identify both internal staff and candidates interested in working for them, that have the aptitude to learn the skills they require or have already learned the skills, as well as matching them to the company by cultural fit. This empowers employers to hire people based on demonstration of required skills and cultural fit to the team. No more resumes.

- Educating the public. Running robust media campaigns to change the perception that high-tech is hard to do for a job.

- Training thousands of veterans and job-seekers. We have applied our adaptive, data-driven model and are training thousands of people around the globe in high-tech in 4-6 weeks to fill all the entry level jobs that employers cannot find people for.

Goal 4: Measure and Encourage Employer-led Training Investments. The size, scope, and impacts of education and skills training investments are still not fully understood. There is a lack of consistent data on company balance sheets and in federal statistics. Business and policy makers need to know how much is spent on training, the types of workers receiving training, and the long-term value of the money and time spent in classroom and on-the-job training.

WithYouWithMe has proven across four different countries that it is possible to train someone with no experience in high-tech to a job-ready standard in 4-6 weeks, for only $5000USD. Any more expensive, for any longer period of time, is an inefficient program.

Attached are reports from major institutions that support the issues and challenges outlined and the need to address these significant skill-gaps that create a national security issue for the United States. WithYouWithMe has an approach and solution that can contribute significantly to solving these challenges.

Kind regards,

Michelle Mosey
CEO WithYouWithMe North America

michelle@withyouwithme.com
+1 202 492 224

Attachments:
WithYouWithMe – Who are We, Jun 2019

CyberSecurity Workforce – Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs, Report to Congressional Committees, United States Government Accounting Office, Mar 2019

The Cybersecurity Workforce Gap, William Crumpler & James A. Lewis, Jan 2019

Urgent Actions Are Needed to Add Cybersecurity Challenges Facings the Nation, Report to Congressional Committees, United States Government Accounting Office, Sep 2018

United States Government Accountability Office

Report to Congressional Committees

September 2018

HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

GAO Highlights

Highlights of GAO-18-622, a report to congressional committees

September 2018

HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

Why GAO Did This Study

Federal agencies and the nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being.

The risks to these systems are increasing as security threats evolve and become more sophisticated. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

This report provides an update to the information security high-risk area. To do so, GAO identified the actions the federal government and other entities need to take to address cybersecurity challenges. GAO primarily reviewed prior work issued since the start of fiscal year 2016 related to privacy, critical federal functions, and cybersecurity incidents, among other areas. GAO also reviewed recent cybersecurity policy and strategy documents, as well as information security industry reports of recent cyberattacks and security breaches.

What GAO Recommends

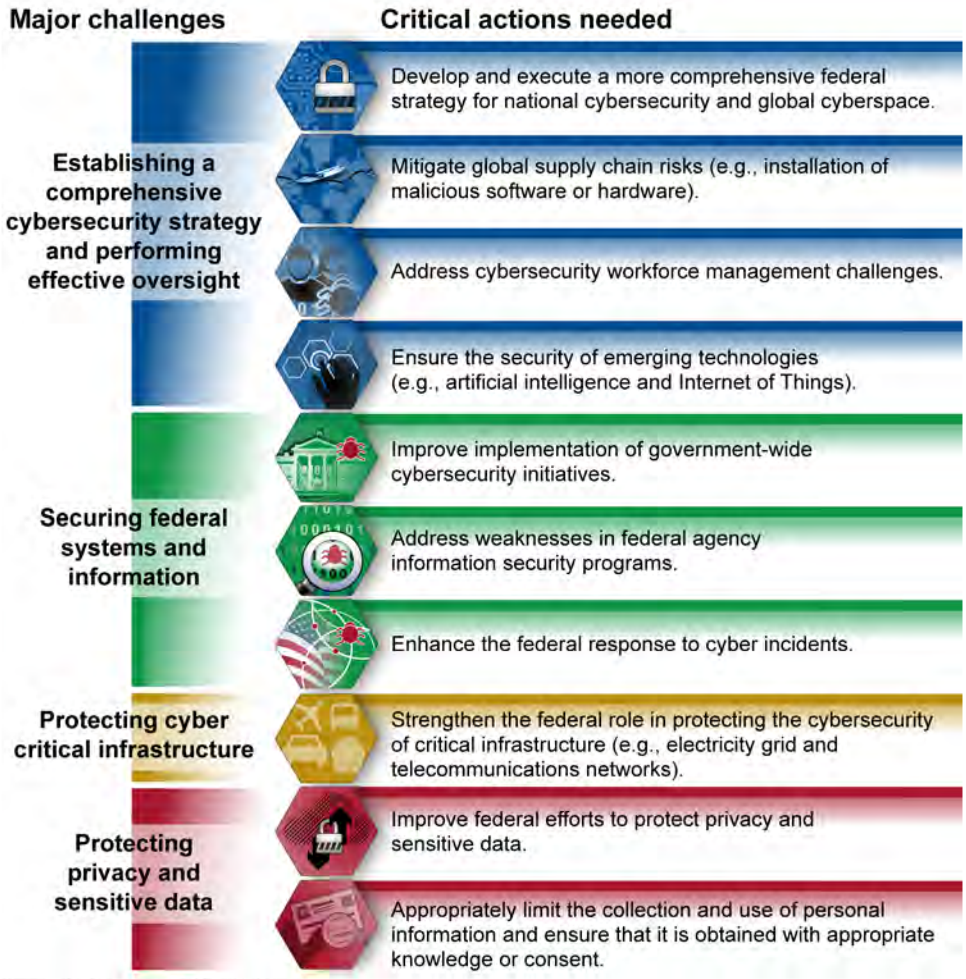
GAO has made over 3,000 recommendations to agencies since 2010 aimed at addressing cybersecurity shortcomings. As of August 2018, about 1,000 still needed to be implemented.

View GAO-18-622. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO has identified four major cybersecurity challenges and 10 critical actions that the federal government and other entities need to take to address them. GAO continues to designate information security as a government-wide high-risk area due to increasing cyber-based threats and the persistent nature of security vulnerabilities.

Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges



Major challenges	Critical actions needed
Establishing a comprehensive cybersecurity strategy and performing effective oversight	Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.
	Mitigate global supply chain risks (e.g., installation of malicious software or hardware).
	Address cybersecurity workforce management challenges.
	Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).
Securing federal systems and information	Improve implementation of government-wide cybersecurity initiatives.
	Address weaknesses in federal agency information security programs.
	Enhance the federal response to cyber incidents.
Protecting cyber critical infrastructure	Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).
Protecting privacy and sensitive data	Improve federal efforts to protect privacy and sensitive data.
	Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Source: GAO analysis. | GAO-18-622

GAO has made over 3,000 recommendations to agencies aimed at addressing cybersecurity shortcomings in each of these action areas, including protecting cyber critical infrastructure, managing the cybersecurity workforce, and responding to cybersecurity incidents. Although many recommendations have been addressed, about 1,000 have not yet been implemented. Until these shortcomings are addressed, federal agencies' information and systems will be increasingly susceptible to the multitude of cyber-related threats that exist.

Contents

Tables

Figures

Abbreviations

CFO	Chief Financial Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare and Medicaid Services
DHS	Department of Homeland Security
DOD	Department of Defense
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
HHS	Department of Health and Human Services
IRS	Internal Revenue Service
IT	information technology
IoT	Internet of Things
NCCIC	National Cybersecurity and Communications Integration Center
NCPS	National Cybersecurity Protection System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	personally identifiable information
SSN	Social Security number
US-CERT	United States Computer Emergency Readiness Team

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

September 6, 2018

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

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

Federal agencies and our nation's critical infrastructures[1]—such as energy, transportation systems, communications, and financial services—are dependent on information technology (IT) systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and national security, prosperity, and well-being.

Many of these systems contain vast amounts of personally identifiable information (PII),[2] thus making it imperative to protect the confidentiality, integrity, and availability of this information and effectively respond to data breaches and security incidents, when they occur. Underscoring the importance of this issue, we continue to designate information security as

[1] The term "critical infrastructure" as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. §5195c(e). Federal policy identifies 16 critical infrastructures: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2] PII is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number, and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

a government-wide high-risk area in our most recent biennial report to Congress—a designation we have made in each report since 1997.[3]

The risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing as security threats continue to evolve and become more sophisticated. These risks include insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks.

In particular, foreign nations—where adversaries may possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks. Rapid developments in new technologies, such as artificial intelligence and the Internet of Things (IoT),[4] makes the threat landscape even more complex and can also potentially introduce security, privacy, and safety issues that were previously unknown.

Compounding these risks, IT systems are often riddled with security vulnerabilities—both known and unknown. These vulnerabilities can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety. This is illustrated by significant security breaches reported by the Office of Personnel Management (OPM) in 2015 that resulted in the loss of PII for an estimated 22.1 million individuals and, more recently, in 2017, a security breach reported by Equifax—one of the nation's largest credit bureaus—that resulted in the loss of PII for an estimated 148 million U.S. consumers.

[3] See GAO, *High-Risk Series: An Update*, GAO-17-317 (Washington, D.C.: February 2017) and *High Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[4] IoT refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information.

This report provides an update to the information security high-risk area by identifying actions that the federal government and other entities need to take to address cybersecurity challenges facing the nation. To do so, this report reflects work we conducted since the prior high-risk update was issued in February 2017, among other things.[5] We also plan to issue an updated assessment of this high-risk area in February 2019.

In conducting the work for this update, we first identified cybersecurity areas in which the federal government has experienced challenges. To do so, we primarily reviewed our prior work issued since the start of fiscal year 2016 related to privacy, critical federal functions, and cybersecurity incidents, among other areas (see appendix I for a list of our prior work).

We also reviewed recent cybersecurity policy and strategy documents issued by the current administration, such as Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*;[6] the National Security Strategy;[7] and the Department of Homeland Security's (DHS) May 2018 cybersecurity strategy.[8] We then analyzed these documents to determine the extent to which they included GAO's desirable characteristics of a national strategy.[9] We also reviewed recent media and information security industry reports of cyberattacks and security breaches. Based on these actions, we identified four cybersecurity areas in which federal agencies had experienced challenges.

[5] GAO-17-317.

[6] Exec. Order No. 13800, 82 Fed Reg. 22391 (May 16, 2017).

[7] The President of the United States, *National Security Strategy of the United States of America*, (Washington, D.C.: Dec. 2017).

[8] DHS, *U.S. Department of Homeland Security Cybersecurity Strategy*, (Washington, D.C.: May 2018). DHS has broad authorities to improve and promote cybersecurity of federal and private-sector networks. Specifically, long-standing federal policy as promulgated by a presidential policy directive, executive orders, and the National Infrastructure Protection Plan have designated DHS as a lead federal agency for coordinating, assisting, and sharing information with the private-sector to protect critical infrastructure from cyber threats.

[9] In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. (GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

To identify the actions needed to address each challenge area, we reviewed the findings of our work specific to each challenge, the status of our prior recommendations to the Executive Office of the President and federal agencies, and any actions taken by these entities to address our recommendations. In reviewing the status of prior recommendations, we also determined which recommendations had not been implemented and what additional actions, if any, the Executive Office of the President and federal agencies needed to take in order to address them. We then summarized the actions needed and the status of our prior recommendations. We also identified our ongoing work related to each action.

We performed our work at the initiative of the U.S. Comptroller General. We conducted this performance audit from February 2018 to September 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

IT systems supporting federal agencies and our nation's critical infrastructures are inherently at risk. These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks.

Compounding the risk, federal systems and networks are also often interconnected with other internal and external systems and networks, including the Internet. This increases the number of avenues of attack and expands their attack surface. As systems become more integrated, cyber threats will pose an increasing risk to national security, economic well-being, and public health and safety.

Advancements in technology, such as data analytics software for searching and collecting information, have also made it easier for individuals and organizations to correlate data (including PII) and track it across large and numerous databases. For example, social media has been used as a mass communication tool where PII can be gathered in vast amounts. In addition, ubiquitous Internet and cellular connectivity makes it easier to track individuals by allowing easy access to information pinpointing their locations. These advances—combined with the increasing sophistication of hackers and others with malicious intent, and the extent to which both federal agencies and private companies collect sensitive information about individuals—have increased the risk of PII being exposed and compromised.

Cybersecurity incidents continue to impact entities across various critical infrastructure sectors. For example, in its 2018 annual data breach investigations report,[10] Verizon reported that 53,308 security incidents and 2,216 data breaches were identified across 65 countries in the 12 months since its prior report. Further, the report noted that cybercriminals can often compromise a system in just a matter of minutes—or even seconds, but that it can take an organization significantly longer to discover the breach. Specifically, the report stated nearly 90 percent of the reported breaches occurred within minutes, while nearly 70 percent went undiscovered for months.

These concerns are further highlighted by the number of information security incidents reported by federal executive branch civilian agencies to DHS's U.S. Computer Emergency Readiness Team (US-CERT).[11] For fiscal year 2017, 35,277 such incidents were reported by the Office of Management and Budget (OMB) in its 2018 annual report to Congress, as mandated by the Federal Information Security Modernization Act (FISMA).[12] These incidents include, for example, web-based attacks, phishing,[13] and the loss or theft of computing equipment.

[10] Verizon, *2018 Data Breach Investigation Report-11th Edition* (April 2018).

[11] US-CERT, a branch of DHS's National Cybersecurity and Communications Integration Center, is a central Federal information security incident center that compiles and analyzes information about incidents that threaten information security. Federal agencies are required to report such incidents to US-CERT.

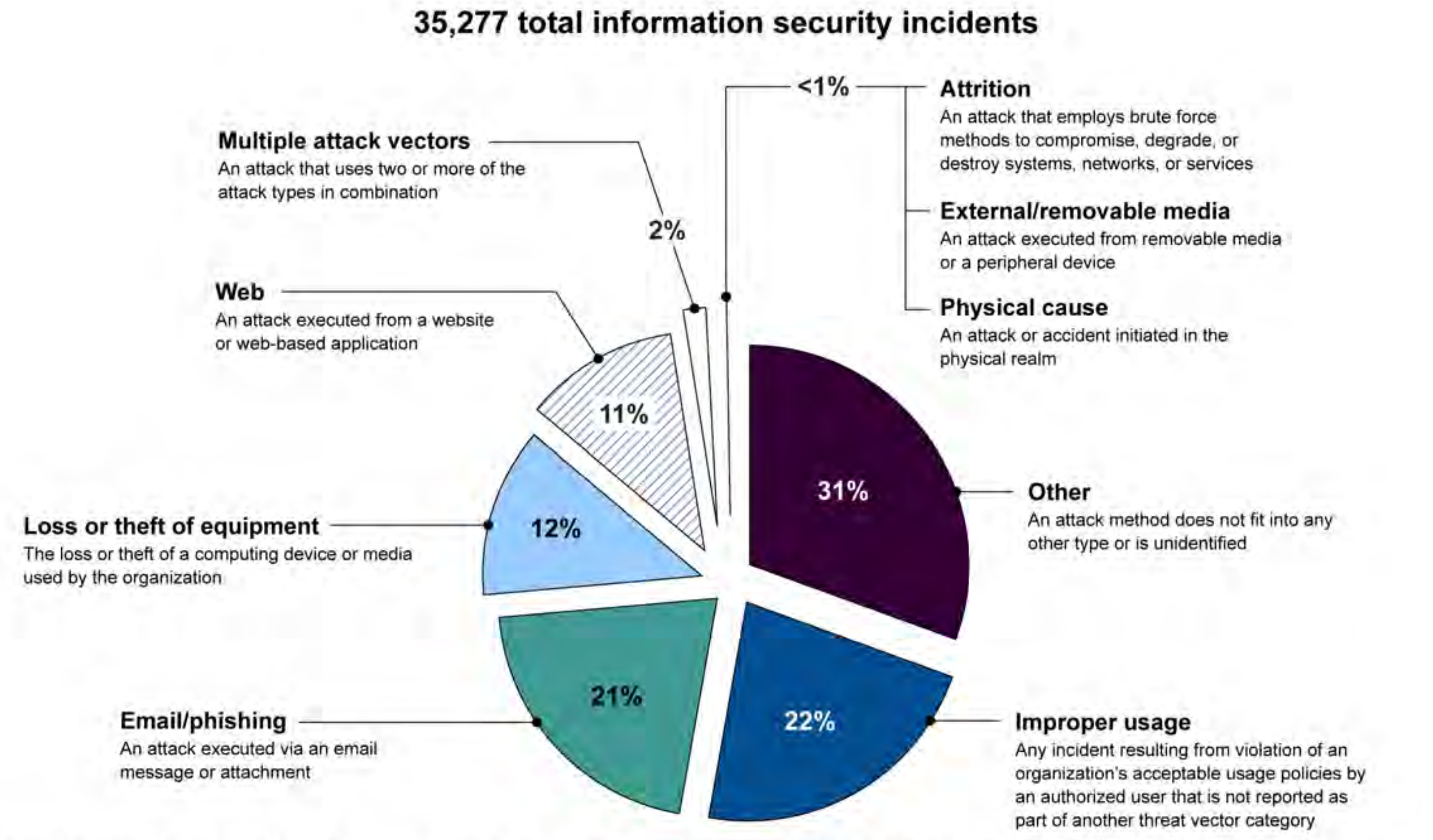
[12] The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[13] Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

Different types of incidents merit different response strategies. However, if an agency cannot identify the threat vector (or avenue of attack),[14] it could be difficult for that agency to define more specific handling procedures to respond to the incident and take actions to minimize similar future attacks. In this regard, incidents with a threat vector categorized as “other” (which includes avenues of attacks that are unidentified) made up 31 percent of the various incidents reported to US-CERT. Figure 1 shows the percentage of the different types of incidents reported across each of the nine threat vector categories for fiscal year 2017, as reported by OMB.

[14] A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyberattack. US-CERT’s Federal Incident Notification Guidelines specify nine potential attack vectors agencies should use to describe incident security incidents during reporting.

Figure 1: Federal Information Security Incidents by Threat Vector Category, Fiscal Year 2017



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal year 2017. | GAO-18-622

These incidents and others like them can pose a serious challenge to economic, national, and personal privacy and security. The following examples highlight the impact of such incidents:

- In March 2018, the Mayor of Atlanta, Georgia, reported that the city was victimized by a ransomware[15] cyberattack. As a result, city government officials stated that customers were not able to access

[15] According to DHS, ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

multiple applications that are used to pay bills or access court related information. In response to the attack, the officials noted that they were working with numerous private and governmental partners, including DHS, to assess what occurred and determine how best to protect the city from future attacks.

- In March 2018, the Department of Justice reported that it had indicted nine Iranians for conducting a massive cybersecurity theft campaign on behalf of the Islamic Revolutionary Guard Corps. According to the department, the nine Iranians allegedly stole more than 31 terabytes of documents and data from more than 140 American universities, 30 U.S. companies, and five federal government agencies, among other entities.
- In March 2018, a joint alert from DHS and the Federal Bureau of Investigation (FBI)[16] stated that, since at least March 2016, Russian government actors had targeted the systems of multiple U.S. government entities and critical infrastructure sectors. Specifically, the alert stated that Russian government actors had affected multiple organizations in the energy, nuclear, water, aviation, construction, and critical manufacturing sectors.
- In July 2017, a breach at Equifax resulted in the loss of PII for an estimated 148 million U.S. consumers. According to Equifax, the hackers accessed people's names, Social Security numbers (SSN), birth dates, addresses and, in some instances, driver's license numbers.
- In April 2017, the Commissioner of the Internal Revenue Service (IRS) testified that the IRS had disabled its data retrieval tool in early March 2017 after becoming concerned about the misuse of taxpayer data. Specifically, the agency suspected that PII obtained outside the agency's tax system was used to access the agency's online federal student aid application in an attempt to secure tax information through the data retrieval tool. In April 2017, the agency began notifying taxpayers who could have been affected by the breach.
- In June 2015, OPM reported that an intrusion into its systems had affected the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a separate, but related, incident had compromised its systems and the

[16] The FBI is the lead federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists. The agency's Cyber Division leads efforts to investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud.

files related to background investigations for 21.5 million individuals. In total, OPM estimated 22.1 million individuals had some form of PII stolen, with 3.6 million being a victim of both breaches.

Federal Information Security Included on GAO's High-Risk List Since 1997

Safeguarding federal IT systems and the systems that support critical infrastructures has been a long-standing concern of GAO. Due to increasing cyber-based threats and the persistent nature of information security vulnerabilities, we have designated information security as a government-wide high-risk area since 1997.[17] In 2003, we expanded the information security high-risk area to include the protection of critical cyber infrastructure.[18] At that time, we highlighted the need to manage critical infrastructure protection activities that enhance the security of the cyber and physical public and private infrastructures that are essential to national security, national economic security, and/or national public health and safety.

We further expanded the information security high-risk area in 2015[19] to include protecting the privacy of PII. Since then, advances in technology have enhanced the ability of government and private sector entities to collect and process extensive amounts of PII, which has posed challenges to ensuring the privacy of such information. In addition, high-profile PII breaches at commercial entities, such as Equifax, heightened concerns that personal privacy is not being adequately protected.

Our experience has shown that the key elements needed to make progress toward being removed from the High-Risk List are top-level attention by the administration and agency leaders grounded in the five criteria for removal, as well as any needed congressional action. The five criteria for removal that we identified in November 2000 are as follows:[20]

- **Leadership Commitment.** Demonstrated strong commitment and top leadership support.

[17] GAO-HR-97-1.

[18] See GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

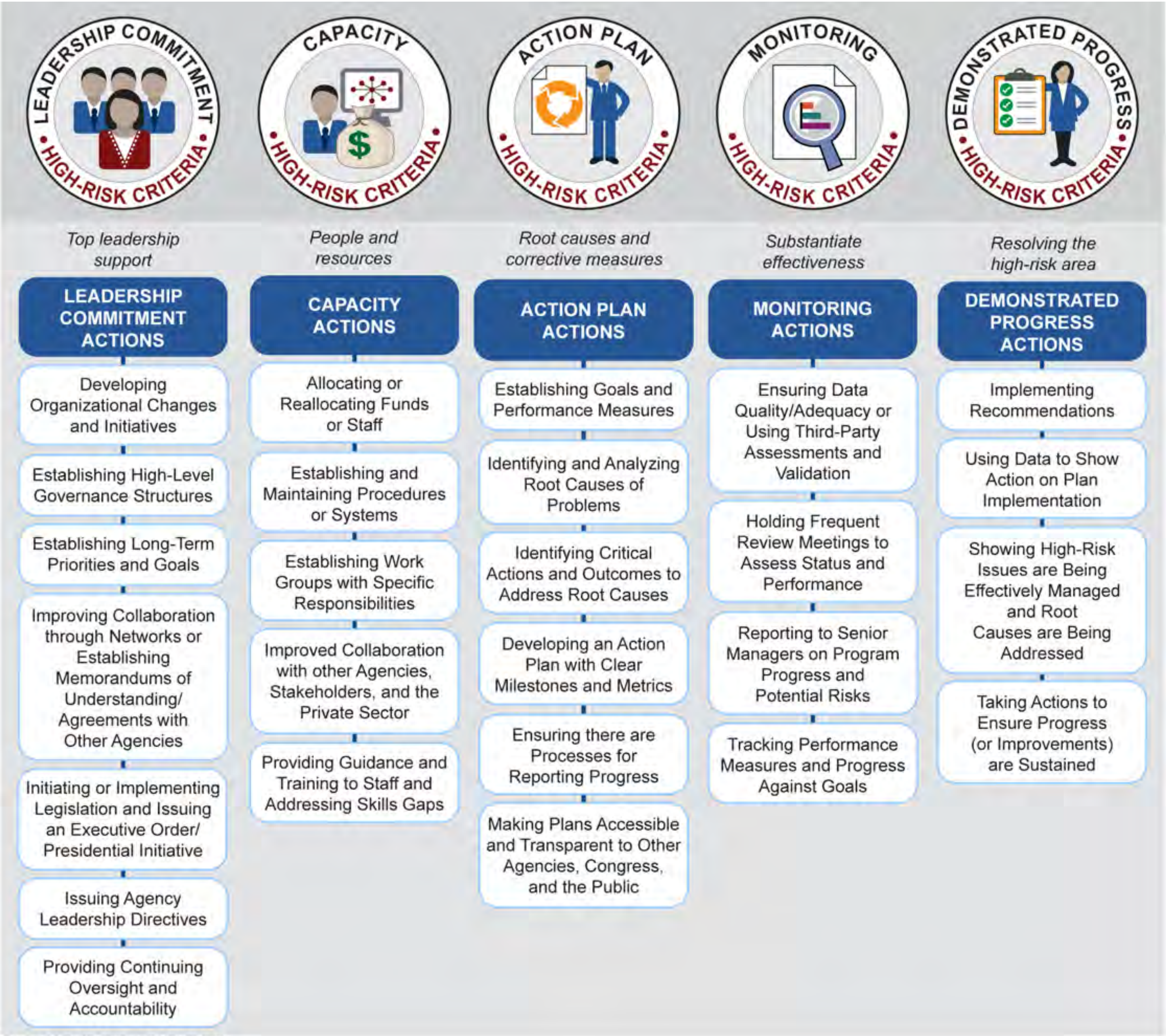
[19] See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 2015).

[20] GAO, *Determining Performance and Accountability Challenges and High Risks*, GAO-01-159SP (Washington, D.C.: November 2000).

- **Capacity**. The agency has the capacity (i.e., people and resources) to resolve the risk(s).
- **Action Plan**. A corrective action plan exists that defines the root cause, solutions, and provides for substantially completing corrective measures, including steps necessary to implement solutions we recommended.
- **Monitoring.** A program has been instituted to monitor and independently validate the effectiveness and sustainability of corrective measures.
- **Demonstrated Progress.** Ability to demonstrate progress in implementing corrective measures and in resolving the high-risk area.

These five criteria form a road map for efforts to improve and ultimately address high-risk issues. Addressing some of the criteria leads to progress, while satisfying all of the criteria is central to removal from the list. Figure 2 shows the five criteria and illustrative actions taken by agencies to address the criteria. Importantly, the actions listed are not “stand alone” efforts taken in isolation from other actions to address high-risk issues. That is, actions taken under one criterion may be important to meeting other criteria as well. For example, top leadership can demonstrate its commitment by establishing a corrective action plan including long-term priorities and goals to address the high-risk issue and using data to gauge progress—actions which are also vital to monitoring criteria.

Figure 2: Criteria for Removal from the High-Risk List and Examples of Actions Leading to Progress



LEADERSHIP COMMITMENT • HIGH-RISK CRITERIA •
CAPACITY • HIGH-RISK CRITERIA •
ACTION PLAN • HIGH-RISK CRITERIA •
MONITORING • HIGH-RISK CRITERIA •
DEMONSTRATED PROGRESS • HIGH-RISK CRITERIA •
$

Top leadership support

LEADERSHIP COMMITMENT ACTIONS

- Developing Organizational Changes and Initiatives
- Establishing High-Level Governance Structures
- Establishing Long-Term Priorities and Goals
- Improving Collaboration through Networks or Establishing Memorandums of Understanding/ Agreements with Other Agencies
- Initiating or Implementing Legislation and Issuing an Executive Order/ Presidential Initiative
- Issuing Agency Leadership Directives
- Providing Continuing Oversight and Accountability

People and resources

CAPACITY ACTIONS

- Allocating or Reallocating Funds or Staff
- Establishing and Maintaining Procedures or Systems
- Establishing Work Groups with Specific Responsibilities
- Improved Collaboration with other Agencies, Stakeholders, and the Private Sector
- Providing Guidance and Training to Staff and Addressing Skills Gaps

Root causes and corrective measures

ACTION PLAN ACTIONS

- Establishing Goals and Performance Measures
- Identifying and Analyzing Root Causes of Problems
- Identifying Critical Actions and Outcomes to Address Root Causes
- Developing an Action Plan with Clear Milestones and Metrics
- Ensuring there are Processes for Reporting Progress
- Making Plans Accessible and Transparent to Other Agencies, Congress, and the Public

Substantiate effectiveness

MONITORING ACTIONS

- Ensuring Data Quality/Adequacy or Using Third-Party Assessments and Validation
- Holding Frequent Review Meetings to Assess Status and Performance
- Reporting to Senior Managers on Program Progress and Potential Risks
- Tracking Performance Measures and Progress Against Goals

Resolving the high-risk area

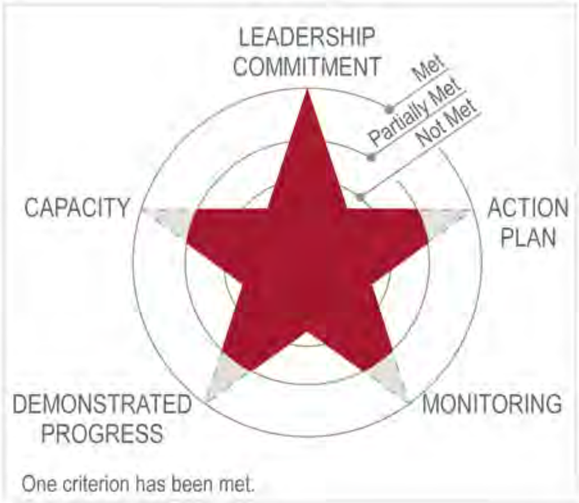
DEMONSTRATED PROGRESS ACTIONS

- Implementing Recommendations
- Using Data to Show Action on Plan Implementation
- Showing High-Risk Issues are Being Effectively Managed and Root Causes are Being Addressed
- Taking Actions to Ensure Progress (or Improvements) are Sustained

Source: GAO-16-480R. | GAO-18-622

As we reported in the February 2017 high-risk report,[21] the federal government's efforts to address information security deficiencies had fully met one of the five criteria for removal from the High-Risk List—leadership commitment—and partially met the other four, as shown in figure 3. We plan to update our assessment of this high-risk area against the five criteria in February 2019.

Figure 3: Status of High-Risk Area for Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information, as of February 2017



Source: GAO analysis. | GAO-18-622

Note: Each point of the star represents one of the five criteria for removal from the High-Risk List and each ring represents one of the three designations: not met, partially met, or met. An unshaded point at the innermost ring means that the criterion has not been met, a partially shaded point at the middle ring means that the criterion has been partially met, and a fully shaded point at the outermost ring means that the criterion has been met.

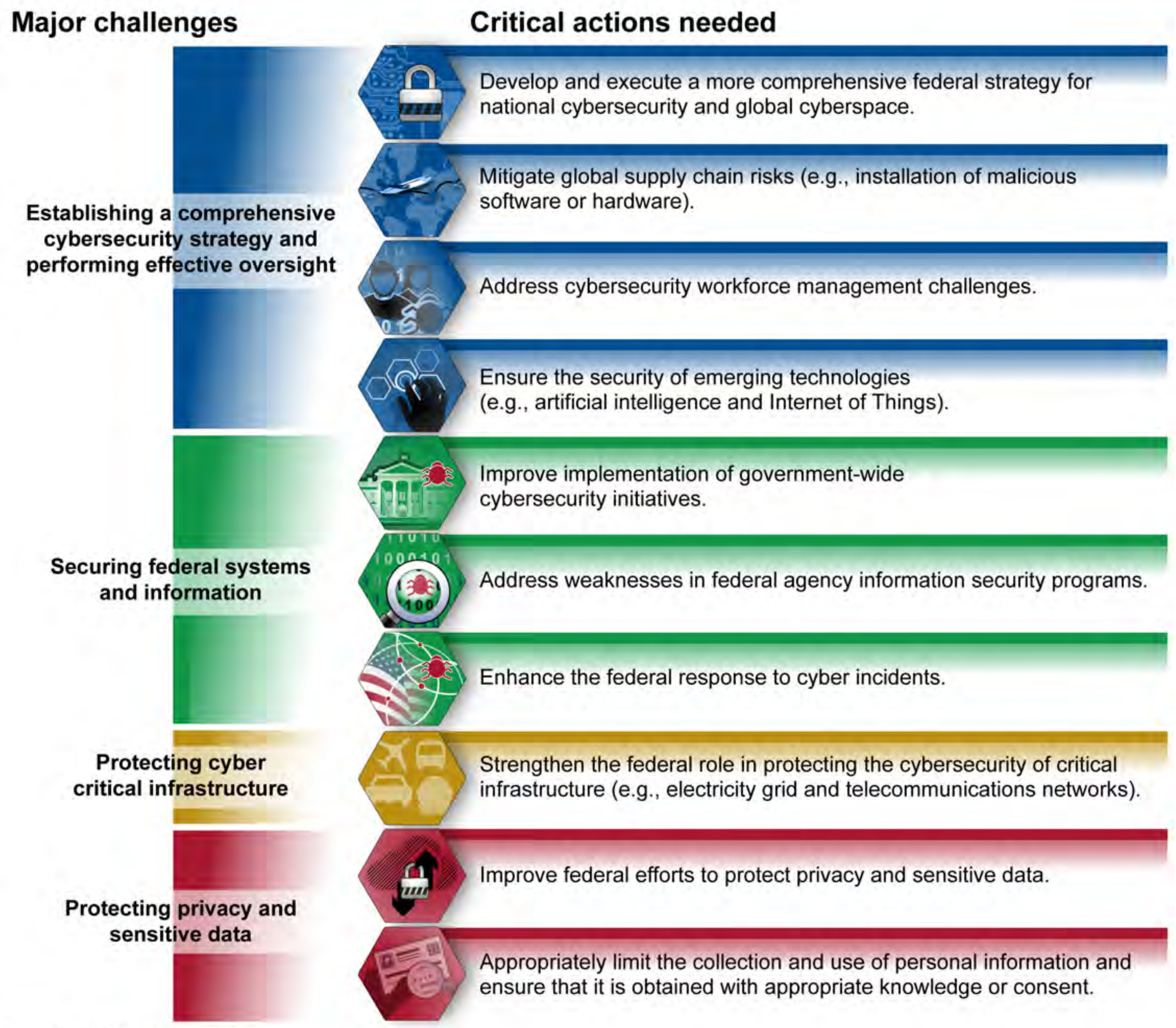
Ten Critical Actions Needed to Address Major Cybersecurity Challenges

Based on our prior work, we have identified four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. To address these challenges, we have identified 10 critical actions that the federal government and other entities need to take (see figure 4). The four challenges and the 10 actions

[21] GAO-17-317.

needed to address them are summarized following the table. In addition, we also discuss in more detail each of the 10 actions in appendices II through XI.

Figure 4: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges


Major challenges
Critical actions needed
Establishing a comprehensive cybersecurity strategy and performing effective oversight
Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.
Mitigate global supply chain risks (e.g., installation of malicious software or hardware).
Address cybersecurity workforce management challenges.
Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).
Securing federal systems and information
Improve implementation of government-wide cybersecurity initiatives.
Address weaknesses in federal agency information security programs.
Enhance the federal response to cyber incidents.
Protecting cyber critical infrastructure
Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).
Protecting privacy and sensitive data
Improve federal efforts to protect privacy and sensitive data.
Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Source: GAO analysis. | GAO-18-622

Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight

The federal government has been challenged in establishing a comprehensive cybersecurity strategy and in performing effective oversight as called for by federal law and policy.[22] Specifically, we have previously reported that the federal government has faced challenges in establishing a comprehensive strategy to provide a framework for how the United States will engage both domestically and internationally on cybersecurity related matters.[23] We have also reported on challenges in performing oversight, including monitoring the global supply chain, ensuring a highly skilled cyber workforce, and addressing risks associated with emerging technologies. The federal government can take four key actions to improve the nation's strategic approach to, and oversight of, cybersecurity.

- **Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.** In February 2013 we reported that the government had issued a variety of strategy-related documents that addressed priorities for enhancing cybersecurity within the federal government as well as for encouraging improvements in the cybersecurity of critical infrastructure within the private sector; however, no overarching cybersecurity strategy had been developed that articulated priority actions, assigned responsibilities for performing them, and set time frames for their completion.[24]

  In October 2015, in response to our recommendation to develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a national strategy,[25] the Director of OMB and the Federal Chief Information Officer issued a *Cybersecurity Strategy and Implementation Plan for the Federal*

[22] This includes the Federal Information Security Modernization Act of 2014, Revision of the Office of Management and Budget's Circular No. A-130, "*Managing Information as a Strategic Resource*" and Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

[23] GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

[24] GAO-13-187.

[25] In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. (GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004)).

Civilian Government.[26] The plan directed a series of actions to improve capabilities for identifying and detecting vulnerabilities and threats, enhance protections of government assets and information, and further develop robust response and recovery capabilities to ensure readiness and resilience when incidents inevitably occur. The plan also identified key milestones for major activities, resources needed to accomplish milestones, and specific roles and responsibilities of federal organizations related to the strategy's milestones.

Since that time, the executive branch has made progress toward outlining a federal strategy for confronting cyber threats. For example, a May 2017 presidential executive order required federal agencies to take a variety of actions, including better manage their cybersecurity risks and coordinate to meet reporting requirements related to cybersecurity of federal networks, critical infrastructure, and the nation.[27] Additionally, the December 2017 National Security Strategy[28] cites cybersecurity as a national priority and identifies related needed actions, such as including identifying and prioritizing risk, and building defensible government networks.

Further, DHS issued a cybersecurity strategy in May 2018,[29] which articulated seven goals the department plans to accomplish in support of its mission related to managing national cybersecurity risks. The strategy is intended to provide DHS with a framework to execute its cybersecurity responsibilities during the next 5 years to keep pace with the evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient.

[26] OMB, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, M-16-04 (Washington, D.C.: Oct. 30, 2015).

[27] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, *Executive Order 13800* (Washington, D.C.: May 11, 2017).

[28] The President of the United States, *National Security Strategy of the United States of America*, (Washington, D.C.: December 2017).

[29] DHS, *U.S. Department of Homeland Security Cybersecurity Strategy*, (Washington, D.C.: May 2018).

These efforts provide a good foundation toward establishing a more comprehensive strategy, but more effort is needed to address all of the desirable characteristics of a national strategy that we have previously recommended. The recently issued executive branch strategy documents did not include key elements of desirable characteristics that can enhance the usefulness of a national strategy as guidance for decision makers in allocating resources, defining policies, and helping to ensure accountability. Specifically, the documents generally did not include milestones and performance measures to gauge results, nor did they describe the resources needed to carry out the goals and objective. Further, most of the strategy documents lacked clearly defined roles and responsibilities for key agencies, such as DHS, the Department of Defense (DOD), and OMB, who contribute substantially to the nation's cybersecurity programs.

Ultimately, a more clearly defined, coordinated, and comprehensive approach to planning and executing an overall strategy would likely lead to significant progress in furthering strategic goals and lessening persistent weaknesses. For more information on this action area, see appendix II.

- **Mitigate global supply chain risks.** The global, geographically disperse nature of the producers and suppliers of IT products is a growing concern. We have previously reported on potential issues associated with IT supply chain and risks originating from foreign-manufactured equipment. For example, in July 2017, we reported that the Department of State had relied on certain device manufacturers, software developers, and contractor support which had suppliers that were reported to be headquartered in a cyber-threat nation (e.g., China and Russia).[30] We further pointed out that the reliance on complex, global IT supply chains introduces multiple risks to federal agencies, including insertion of counterfeits, tampering, or installation of malicious software or hardware.

  In July 2018, we testified that if such global IT supply chain risks are realized, they could jeopardize the confidentiality, integrity, and availability of federal information systems.[31] Thus, the potential exists

[30] GAO, *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations,* GAO-17-688R (Washington, D.C.: July 27, 2017).

[31] GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies,* GAO-18-667T (Washington, D.C.: July 12, 2018).

for serious adverse impact on an agency's operations, assets, and employees. These factors highlight the importance and urgency of federal agencies appropriately assessing, managing, and monitoring IT supply chain risk as part of their agency-wide information security programs. For more information on this action area, see appendix III.

- **Address cybersecurity workforce management challenges.** The federal government faces challenges in ensuring that the nation's cybersecurity workforce has the appropriate skills. For example, in June 2018, we reported on federal efforts to implement the requirements of the *Federal Cybersecurity Workforce Assessment Act of 2015*.[32] We determined that most of the Chief Financial Officers (CFO) Act[33] agencies had not fully implemented all statutory requirements, such as developing procedures for assigning codes to cybersecurity positions. Further, we have previously reported that DHS and DOD had not addressed cybersecurity workforce management requirements set forth in federal laws.[34] In addition, we have reported in the last 2 years that federal agencies (1) had not identified and closed cybersecurity skills gaps,[35] (2) had been

[32] GAO, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions*, GAO-18-466 (Washington, D.C.: June 14, 2018). 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, 129 Stat. 2242, 2975-77 (Dec. 18, 2015).

[33] There are 24 agencies identified in the Chief Financial Officers Act: 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.

[34] GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements,* GAO-18-175 (Washington, D.C.: Feb. 6, 2018); and *Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements,* GAO-18-47 (Washington, D.C.: Nov. 30, 2017).

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

challenged with recruiting and retaining qualified staff,[36] and (3) had difficulty navigating the federal hiring process.[37]

A recent executive branch report also discussed challenges associated with the cybersecurity workforce. Specifically, in response to Executive Order 13800, the Department of Commerce and DHS led an interagency working group exploring how to support the growth and sustainment of future cybersecurity employees in the public and private sectors. In May 2018, the departments issued a report[38] that identified key findings, including:

- the U.S. cybersecurity workforce needs immediate and sustained improvements;
- the pool of cybersecurity candidates needs to be expanded through retraining and by increasing the participation of women, minorities, and veterans;
- a shortage exists of cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors; and
- comprehensive and reliable data about cybersecurity workforce position needs and education and training programs are lacking.

The report also included recommendations and proposed actions to address the findings, including that private and public sectors should (1) align education and training with employers' cybersecurity workforce needs by applying the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework; (2) develop cybersecurity career model paths; and (3) establish a clearinghouse of information on cybersecurity workforce development education, training, and workforce development programs and initiatives.

In addition, in June 2018, the executive branch issued a government reform plan and reorganization recommendations that included,

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

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

[38] The Secretaries of Commerce and Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*, (Washington, D.C.: May 2018).

among other things, proposals for solving the federal cybersecurity workforce shortage.[39] In particular, the plan notes that the administration intends to prioritize and accelerate ongoing efforts to reform the way that the federal government recruits, evaluates, selects, pays, and places cyber talent across the enterprise. The plan further states that, by the end of the first quarter of fiscal year 2019, all CFO Act agencies, in coordination with DHS and OMB, are to develop a critical list of vacancies across their organizations. Subsequently, OMB and DHS are to analyze these lists and work with OPM to develop a government-wide approach to identifying or recruiting new employees or reskilling existing employees. Regarding cybersecurity training, the plan notes that OMB is to consult with DHS to standardize training for cybersecurity employees, and should work to develop an enterprise-wide training process for government cybersecurity employees. For more information on this action area, see appendix IV.

- **Ensure the security of emerging technologies.** As the devices used in daily life become increasingly integrated with technology, the risk to sensitive data and PII also grows. Over the last several years, we have reported on weaknesses in addressing vulnerabilities associated with emerging technologies, including:
  - IoT devices, such as fitness trackers, cameras, and thermostats, that continuously collect and process information are potentially vulnerable to cyber-attacks;[40]
  - IoT devices, such as those acquired and used by DOD employees or that DOD itself acquires (e.g., smartphones), may increase the security risks to the department;[41]
  - vehicles that are potentially susceptible to cyber-attack through technology, such as Bluetooth;[42]

[39] Executive Office of the President of the United States, *Delivering Government Solutions in the 21st Century: Reform Plan and Reorganization Recommendations* (Washington, D.C.: June 2018).

[40] GAO, *Technology Assessment: Internet of Things: Status and implications of an increasingly connected world*, GAO-17-75 (Washington, D.C.: May 15, 2017).

[41] GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-668 (Washington, D.C.: July 27, 2017).

- the unknown impact of artificial intelligence cybersecurity; and[43]
- advances in cryptocurrencies and blockchain technologies.[44]

Executive branch agencies have also highlighted the challenges associated with ensuring the security of emerging technologies. Specifically, in a May 2018 report issued in response to Executive Order 13800, the Department of Commerce and DHS issued a report on the opportunities and challenges in reducing the botnet threat.[45] The opportunities and challenges are centered on six principal themes, including the global nature of automated, distributed attacks; effective tools; and awareness and education. The report also provides recommended actions, including that federal agencies should increase their understanding of what software components have been incorporated into acquired products and establish a public campaign to support awareness of IoT security. For more information on this action area, see appendix V.

In our previously discussed reports related to this cybersecurity challenge, we made a total of 50 recommendations to federal agencies to address the weaknesses identified. As of August 2018, 48 recommendations had not been implemented. These outstanding recommendations include 8 priority recommendations, meaning that we believe that they warrant priority attention from heads of key departments and agencies. These priority recommendations include addressing weaknesses associated with, among other things, agency-specific cybersecurity workforce challenges and agency responsibilities for supporting mitigation of vehicle network attacks. Until our recommendations are fully implemented, federal agencies may be limited in their ability to provide effective oversight of critical government-wide

[42] GAO, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack*, GAO-16-350 (Washington, D.C.: Apr. 25, 2016).

[43] GAO, *Technology Assessment: Artificial Intelligence, Emerging Opportunities, Challenges, and Implications*, GAO-18-142SP (Washington, D.C.: Mar. 28, 2018).

[44] GAO, *GAO Strategic Plan 2018-2023: Trends Affecting Government and Society*, GAO-18-396SP (Washington, D.C.: Feb. 22, 2018).

[45] The Secretaries of Commerce and Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, (Washington, D.C.: May 22, 2018).

initiatives, address challenges with cybersecurity workforce management, and better ensure the security of emerging technologies.

In addition to our prior work related to the federal government's efforts to establish key strategy documents and implement effective oversight, we also have several ongoing reviews related to this challenge. These include reviews of:

- the CFO Act agencies' efforts to submit complete and reliable baseline assessment reports of their cybersecurity workforces;
- the extent to which DOD has established training standards for cyber mission force personnel, and efforts the department has made to achieve its goal of a trained cyber mission force; and
- selected agencies' ability to implement cloud service technologies and notable benefits this might have on agencies.

Securing Federal Systems and Information

The federal government has been challenged in securing federal systems and information. Specifically, we have reported that federal agencies have experienced challenges in implementing government-wide cybersecurity initiatives, addressing weaknesses in their information systems and responding to cyber incidents on their systems. This is particularly concerning given that the emergence of increasingly sophisticated threats and continuous reporting of cyber incidents underscores the continuing and urgent need for effective information security. As such, it is important that federal agencies take appropriate steps to better ensure they have effectively implemented programs to protect their information and systems. We have identified three actions that the agencies can take.

- **Improve implementation of government-wide cybersecurity initiatives.** Specifically, in January 2016, we reported that DHS had not ensured that the National Cybersecurity Protection System (NCPS) had fully satisfied all intended system objectives related to intrusion detection and prevention, information sharing, and analytics.[46] In addition, in February 2017, we reported[47] that the DHS

[46] GAO*, Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System,* GAO-16-294 (Washington, D.C.: Jan. 28, 2016). NCPS is intended to provide DHS with capabilities to detect malicious traffic traversing federal agencies' computer networks, prevent intrusions, and support data analytics and information sharing.

National Cybersecurity and Communications Integration Center's (NCCIC)[48] functions were not being performed in adherence with the principles set forth in federal laws.[49] We noted that, although NCCIC was sharing information about cyber threats in the way it should, the center did not have metrics to measure that the information was timely, relevant and actionable, as prescribed by law. For more information on this action area, see appendix VI.

- **Address weaknesses in federal information security programs.** We have previously identified a number of weaknesses in agencies' protection of their information and information systems. For example, over the past 2 years, we have reported that:
  - most of the 24 agencies covered by the CFO Act had weaknesses in each of the five major categories of information system controls (i.e., access controls, configuration management controls, segregation of duties, contingency planning, and agency-wide security management);[50]
  - three agencies—the Securities Exchange Commission, the Federal Deposit Insurance Corporation, and the Food and Drug Administration—had not effectively implemented aspects of their

[47] GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely,* GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

[48] DHS established the NCCIC as to serve as the 24/7 cyber monitoring, incident response, and management center. The center provides a central place for the various federal and private-sector organizations to coordinate efforts to address and respond to cyber threats.

[49] *The National Cybersecurity Protection Act of 2014* and *Cybersecurity Act of 2015* require NCCIC to carry out 11 cybersecurity functions, to the extent practicable, in accordance with nine principles. Pub. L. No. 113-282, Dec. 18, 2014. The Cybersecurity Act of 2015 was enacted as Division N of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Dec. 18, 2015.

[50] GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices,* GAO-17-549 (Washington, D.C.: Sept. 28, 2017).

information security programs, which resulted in weaknesses in these agencies' security controls;[51]

- information security weaknesses in selected high-impact systems at four agencies—the National Aeronautics and Space Administration, the Nuclear Regulatory Commission, OPM, and the Department of Veterans Affairs—were cited as a key reason that the agencies had not effectively implemented elements of their information security programs;[52]
- DOD's process for monitoring the implementation of cybersecurity guidance had weaknesses and resulted in the closure of certain tasks (such as completing cyber risk assessments) before they were fully implemented;[53] and
- agencies had not fully defined the role of their Chief Information Security Officers, as required by FISMA.[54]

We also recently testified that, although the government had acted to protect federal information systems, additional work was needed to improve agency security programs and cyber capabilities.[55] In particular, we noted that further efforts were needed by agencies to implement our prior recommendations in order to strengthen their information security programs and technical controls over their computer networks and systems. For more information on this action area, see appendix VII.

[51] GAO, *Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions,* GAO-17-469 (Washington, D.C.: July 27, 2017); *Information Security: FDIC Needs to Improve Controls over Financial Systems and Information,* GAO-17-436 (Washington, D.C.: May 31, 2017); and *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk,* GAO-16-513 (Washington, D.C.: Aug. 30, 2016).

[52] GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016).

[53] GAO, *Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened,* GAO-17-512 (Washington, D.C.: Aug. 1, 2017).

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

[55] GAO, *Information Technology: Continued Implementation of High-Risk Recommendations Is Needed to Better Manage Acquisitions, Operations, and Cybersecurity*, GAO-18-566T (Washington, D.C.: May 23, 2018).

- **Enhance the federal response to cyber incidents.** We have reported that certain agencies have had weaknesses in responding to cyber incidents. For example,
  - as of August 2017, OPM had not fully implemented controls to address deficiencies identified as a result of its 2015 cyber incidents;[56]
  - DOD had not identified the National Guard's cyber capabilities (e.g., computer network defense teams) or addressed challenges in its exercises;[57]
  - as of April 2016, DOD had not identified, clarified, or implemented all components of its support of civil authorities during cyber incidents;[58] and
  - as of January 2016, DHS's NCPS had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information.

  For more information on this action area, see appendix VIII.

In the public versions of the reports previously discussed for this challenge area, we made a total of 101 recommendations to federal agencies to address the weaknesses identified.[59] As of August 2018, 61 recommendations had not been implemented. These outstanding recommendations include 14 priority recommendations to address weaknesses associated with, among other things, the information security programs at the National Aeronautics and Space Administration, OPM, and the Security Exchange Commission. Until these recommendations are implemented, these federal agencies will be limited in their ability to

[56] GAO, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed,* GAO-17-614 (Washington, D.C.: Aug. 3, 2017).

[57] GAO, *Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises,* GAO-16-574 (Washington, D.C.: Sept. 6, 2016).

[58] GAO, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents,* GAO-16-332 (Washington, D.C.: Apr. 4, 2016).

[59] GAO often issues two versions of its audit reports on the security of federal systems and information. One version is publicly available, and one version is not available to the public because of the sensitive security information it contains. GAO has made hundreds of recommendations to agencies to rectify technical security control deficiencies identified in these non-publicly available reports.

ensure the effectiveness of their programs for protecting information and systems.

In addition to our prior work, we also have several ongoing reviews related to the federal government's efforts to protect its information and systems. These include reviews of:

- Federal Risk and Authorization Management Program (FedRAMP)[60] implementation, including an assessment of the implementation of the program's authorization process for protecting federal data in cloud environments;
- the Equifax data breach, including an assessment of federal oversight of credit reporting agencies' collection, use, and protection of consumer PII;
- the Federal Communication Commission's Electronic Comment Filing System security, to include a review of the agency's detection of and response to a May 2017 incident that reportedly impacted the system;
- DOD's efforts to improve the cybersecurity of its major weapon systems;
- DOD's whistleblower program, including an assessment of the policies, procedures, and controls related to the access and storage of sensitive and classified information needed for the program;
- IRS's efforts to (1) implement security controls and the agency's information security program, (2) authenticate taxpayers, and (3) secure tax information; and
- the federal approach and strategy to securing agency information systems, to include federal intrusion detection and prevention capabilities and the intrusion assessment plan.

Protecting Cyber Critical Infrastructure

The federal government has been challenged in working with the private sector to protect critical infrastructure. This infrastructure includes both public and private systems vital to national security and other efforts, such as providing the essential services that underpin American society. As the cybersecurity threat to these systems continues to grow, federal agencies have millions of sensitive records that must be protected. Specifically, this

[60] In December 2011, OMB established FEDRAMP—a government-wide program intended to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud computing products and services.

critical infrastructure threat could have national security implications and more efforts should be made to ensure that it is not breached.

To help address this issue, the National Institute of Standards and Technology (NIST) developed the cybersecurity framework—a voluntary set of cybersecurity standards and procedures for industry to adopt as a means of taking a risk-based approach to managing cybersecurity.[61]

However, additional action is needed to strengthen the federal role in protecting the critical infrastructure. Specifically, we have reported on other critical infrastructure protection issues that need to be addressed. For example:

- DHS did not track vulnerability reduction from the implementation and verification of planned security measures at the high-risk chemical facilities that engage with the department, as a basis for assessing performance.[62]
- Entities within the 16 critical infrastructure sectors reported encountering four challenges to adopting the cybersecurity framework, such as being limited in their ability to commit necessary resources towards framework adoption and not having the necessary knowledge and skills to effectively implement the framework.[63]
- DOD and the Federal Aviation Administration identified a variety of operations and physical security risks that could adversely affect DOD missions.[64]
- Major challenges existed to securing the electricity grid against cyber threats.[65] These challenges included monitoring implementation of

[61] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: Feb. 12, 2014). The cybersecurity framework was updated on April 16, 2018.

[62] GAO, *Critical Infrastructure Protection: DHS Should Take Actions to Measure Reduction in Chemical Facility Vulnerability and Share Information with First Responders*, GAO-18-538 (Washington, D.C.: Aug. 8, 2018).

[63] GAO, *Critical Infrastructure Protection: Additional Actions are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018).

[64] GAO, *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft,* GAO-18-177 (Washington, D.C.: Jan. 18, 2018).

[65] GAO, *Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention*, GAO-16-174T (Washington, D.C.: Oct. 21, 2015).

cybersecurity standards, ensuring security features are built into smart grid systems, and establishing metrics for cybersecurity.

- DHS and other agencies needed to enhance cybersecurity in the maritime environment. Specifically, DHS did not include cyber risks in its risk assessments that were already in place nor did it address cyber risks in guidance for port security plans.[66]
- Sector-specific agencies[67] were not properly addressing progress or metrics to measure their progress in cybersecurity.[68]

For more information on this action area, see appendix IX.

We made a total of 21 recommendations to federal agencies to address these weaknesses and others. These recommendations include, for example, a total of 9 recommendations to 9 sector-specific agencies to develop methods to determine the level and type of cybersecurity framework adoption across their respective sectors.[69] As of August 2018, all 21 recommendations had not been implemented. Until these recommendations are implemented, the federal government will continue to be challenged in fulfilling its role in protecting the nation's critical infrastructure.

In addition to our prior work related to the federal government's efforts to protect critical infrastructure, we also have several ongoing reviews focusing on:

- the physical and cybersecurity risks to pipelines across the country responsible for transmitting oil, natural gas, and other hazardous liquids;
- the cybersecurity risks to the electric grid; and

[66] GAO, *Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity*, GAO-16-116T (Washington, D.C.: Oct. 8, 2015).

[67] Sector-specific agencies are federal departments or agencies with responsibility for providing institutional knowledge and specialized expertise. They accomplish this by leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the environment.

[68] GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015). The government facilities sector was excluded from the scope of this review due to its uniquely governmental focus.

[69] GAO-18-211.

- the privatization of utilities at DOD installations.

Protecting Privacy and Sensitive Data

The federal government has been challenged in protecting privacy and sensitive data. Advances in technology, including powerful search technology and data analytics software, have made it easy to correlate information about individuals across large and numerous databases, which have become very inexpensive to maintain. In addition, ubiquitous Internet connectivity has facilitated sophisticated tracking of individuals and their activities through mobile devices such as smartphones and fitness trackers.

Given that access to data is so pervasive, personal privacy hinges on ensuring that databases of PII maintained by government agencies or on their behalf are protected both from inappropriate access (i.e., data breaches) as well as inappropriate use (i.e., for purposes not originally specified when the information was collected). Likewise, the trend in the private sector of collecting extensive and detailed information about individuals needs appropriate limits. The vast number of individuals potentially affected by data breaches at federal agencies and private sector entities in recent years increases concerns that PII is not being properly protected.

Federal agencies should take two types of actions to address this challenge area. In addition, we have previously proposed two matters for congressional consideration aimed toward better protecting PII.

- **Improve federal efforts to protect privacy and sensitive data.** We have issued several reports noting that agencies had deficiencies in protecting privacy and sensitive data that needed to be addressed. For example:
  - The Department of Health and Human Services' (HHS) Centers for Medicare and Medicaid Services (CMS) and external entities were at risk of compromising Medicare Beneficiary Data due to a lack of guidance and proper oversight.[70]

[70] GAO, *Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement*, GAO-18-210 (Washington, D.C.: March 6, 2018).

- The Department of Education's Office of Federal Student Aid had not properly overseen its school partners' records or information security programs.[71]
- HHS had not fully addressed key security elements in its guidance for protecting the security and privacy of electronic health information.[72]
- CMS had not fully protected the privacy of users' data on state-based marketplaces.[73]
- Poor planning and ineffective monitoring had resulted in the unsuccessful implementation of government initiatives aimed at eliminating the unnecessary collection, use, and display of SSNs.[74]

For more information on this action area, see appendix X.

- **Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.** We have issued a series of reports that highlight a number of the key concerns in this area. For example:
  - The emergence of IoT devices can facilitate the collection of information about individuals without their knowledge or consent;[75]
  - Federal laws for smartphone tracking applications have not generally been well enforced;[76]
  - The FBI has not fully ensured privacy and accuracy related to the use of face recognition technology.[77]

[71] GAO, *Federal Student Aid: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information,* GAO-18-121 (Washington, D.C.: Dec. 15, 2017).

[72] GAO, *Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight*, GAO-16-771 (Washington, D.C.: Aug. 26, 2016).

[73] GAO, *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls,* GAO-16-265 (Washington, D.C.: Mar. 23, 2016).

[74] GAO, *Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display,* GAO-17-553 (Washington, D.C.: July 25, 2017).

[75] GAO-17-75.

[76] GAO, *Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking*, GAO-16-317 (Washington, D.C.: Apr. 21, 2016).

For more information on this action area, see appendix XI.

We have previously suggested that Congress consider amending laws, such as the Privacy Act of 1974[78] and the E-Government Act of 2002,[79] because they may not consistently protect PII.[80] Specifically, we found that while these laws and guidance set minimum requirements for agencies, they may not consistently protect PII in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. However, revisions to the Privacy Act and the E-Government Act have not yet been enacted.

Further, we also suggested that Congress consider strengthening the consumer privacy framework[81] and review issues such as the adequacy of consumers' ability to access, correct, and control their personal information; and privacy controls related to new technologies such as web tracking and mobile devices.[82] However, these suggested changes have not yet been enacted.

We also made a total of 29 recommendations to federal agencies to address the weaknesses identified. As of August 2018, 28 recommendations had not been implemented. These outstanding recommendations include 6 priority recommendations to address weaknesses associated with, among other things, publishing privacy impact assessments[83] and improving the accuracy of the FBI's face recognition services. Until these recommendations are implemented,

[77] GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016).

[78] Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

[79] Pub. L. No. 107-347, 116 Stat. 2899.

[80] GAO, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 (Washington, D.C.: May 19, 2008).

[81] This framework presents a consumer privacy bill of rights, describes a stakeholder process to specify how the principles in that bill of rights would apply, and encourages Congress to provide the Federal Trade Commission with enforcement authorities for the bill of rights.

[82] GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

[83] Privacy impact assessments include an analysis of how personal information is collected, stored, shared, and managed in a federal system.

federal agencies will be challenged in their ability to protect privacy and sensitive data and ensure that its collection and use is appropriately limited.

In addition to our prior work, we have several ongoing reviews related to protecting privacy and sensitive data. These include reviews of:

- IRS's taxpayer authentication efforts, including what steps the agency is taking to monitor and improve its authentication methods;
- the extent to which the Department of Education's Office of Federal Student Aid's policies and procedures for overseeing non-school partners' protection of federal student aid data align with federal requirements and guidance;
- data security issues related to credit reporting agencies, including a review of the causes and impacts of the August 2017 Equifax data breach;
- the extent to which Equifax assessed, responded to, and recovered from its August 2017 data breach;
- federal agencies' efforts to remove PII from shared cyber threat indicators; and
- how the federal government has overseen Internet privacy, including the roles of the Federal Communications Commission and the Federal Trade Commission, and strengths and weaknesses of the current oversight authorities.

Continued Implementation of Our Recommendations Is Needed to Address Cybersecurity Weaknesses

In conclusion, since 2010, we have made over 3,000 recommendations to agencies aimed at addressing the four cybersecurity challenges. Nevertheless, many agencies continue to be challenged in safeguarding their information systems and information, in part because many of these recommendations have not been implemented. Of the roughly 3,000 recommendations made since 2010, nearly 1,000 had not been implemented as of August 2018. We have also designated 35 as priority recommendations, and as of August 2018, 31 had not been implemented.

The federal government and the nation's critical infrastructure are dependent on IT systems and electronic data, which make them highly vulnerable to a wide and evolving array of cyber-based threats. Securing these systems and data is vital to the nation's security, prosperity, and well-being. Nevertheless, the security over these systems and data is inconsistent and urgent actions are needed to address ongoing cybersecurity and privacy challenges. Specifically, the federal government needs to implement a more comprehensive cybersecurity strategy and improve its oversight, including maintaining a qualified cybersecurity workforce; address security weaknesses in federal systems and information and enhance cyber incident response efforts; bolster the protection of cyber critical infrastructure; and prioritize efforts to protect individual’s privacy and PII. Until our recommendations are addressed and actions are taken to address the four challenges we identified, the federal government, the national critical infrastructure, and the personal information of U.S. citizens will be increasingly susceptible to the multitude of cyber-related threats that exist.

We are sending copies of this report to the appropriate congressional committees. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Gregory C. Wilshusen 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. GAO staff who made key contributions to this report are listed in appendix XII.

Nick Marinos

Nick Marinos
Director, Cybersecurity and Data Protection Issues

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Related GAO Reports

Critical Infrastructure Protection: DHS Should Take Actions to Measure Reduction in Chemical Facility Vulnerability and Share Information with First Responders. GAO-18-538. Washington, D.C.: August 8, 2018.

High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation. GAO-18-645T. Washington, D.C.: July 25, 2018.

Information Security: Supply Chain Risks Affecting Federal Agencies. GAO-18-667T. Washington, D.C.: July 12, 2018.

Information Technology: Continued Implementation of High-Risk Recommendations Is Needed to Better Manage Acquisitions, Operations, and Cybersecurity. GAO-18-566T. Washington, D.C.: May 23, 2018.

Cybersecurity: DHS Needs to Enhance Efforts to Improve and Promote the Security of Federal and Private-Sector Networks, GAO-18-520T. Washington, D.C.: April 24, 2018.

Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement. GAO-18-210. Washington, D.C.: March 6, 2018.

Technology Assessment: Artificial Intelligence, Emerging Opportunities, Challenges, and Implications. GAO-18-142SP. Washington, D.C.: March 28, 2018.

GAO Strategic Plan 2018-2023: Trends Affecting Government and Society. GAO-18-396SP. Washington, D.C.: February 22, 2018.

Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption. GAO-18-211. Washington, D.C.: February 15, 2018.

Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements. GAO-18-175. Washington, D.C.: February 6, 2018.

Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft. GAO-18-177. Washington, D.C.: January 18, 2018.

Federal Student Aid: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information. GAO-18-121. Washington, D.C.: December 15, 2017.

Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements. GAO-18-47. Washington, D.C.: November 30, 2017.

Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices. GAO-17-549. Washington, D.C.: September 28, 2017.

Information Security: OPM Has Improved Controls, but Further Efforts Are Needed. GAO-17-614. Washington, D.C.: August 3, 2017.

Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened. GAO-17-512. Washington, D.C.: August 1, 2017.

State Department Telecommunications: Information on Vendors and Cyber-Threat Nations. GAO-17-688R. Washington, D.C.: July 27, 2017.

Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD. GAO-17-668. Washington, D.C.: July 27, 2017.

Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions. GAO-17-469. Washington, D.C.: July 27, 2017.

Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data. GAO-17-395. Washington, D.C.: July 26, 2017.

Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display. GAO-17-553. Washington, D.C.: July 25, 2017.

Information Security: FDIC Needs to Improve Controls over Financial Systems and Information. GAO-17-436. Washington, D.C.: May 31, 2017.

Technology Assessment: Internet of Things: Status and implications of an increasingly connected world. GAO-17-75. Washington, D.C.: May 15, 2017.

Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely. GAO-17-163. Washington, D.C.: February 1, 2017.

High-Risk Series: An Update. GAO-17-317. Washington, D.C.: February 2017.

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

Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight. GAO-16-771. Washington, D.C.: September 26, 2016.

Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises. GAO-16-574. Washington, D.C.: September 6, 2016.

Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk. GAO-16-513. Washington, D.C.: August 30, 2016.

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

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

Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems. GAO-16-501. Washington, D.C.: May 18, 2016.

Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy. GAO-16-267. Washington, D.C.: May 16, 2016.

Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking. GAO-16-317. Washington, D.C.: May 9, 2016.

Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack. GAO-16-350. Washington, D.C.: April 25, 2016.

Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents. GAO-16-332. Washington, D.C.: April 4, 2016.

Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls. GAO-16-265. Washington, D.C.: March 23, 2016.

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

Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress. GAO-16-79. Washington, D.C.: November 19, 2015.

Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention. GAO-16-174T. Washington, D.C.: October 21, 2015.

Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity. GAO-16-116T. Washington, D.C.: October 8, 2015.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO-13-187. Washington, D.C.: February 14, 2014.

Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace. GAO-13-663. Washington, D.C.: September 25, 2013.

Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information. GAO-08-536. Washington, D.C.: May 19, 2008.

Appendix II: Action 1—Develop and Execute a More Comprehensive Federal Strategy for National Cybersecurity and Global Cyberspace

Federal law and policy call for a risk-based approach to managing cybersecurity within the government, as well as globally.[1] We have previously reported that the federal government has faced challenges in establishing a comprehensive strategy to provide a framework for how the United States will engage both domestically and internationally on cybersecurity related matters.

More specifically, in February 2013, we reported that the government had issued a variety of strategy-related documents that addressed priorities for enhancing cybersecurity within the federal government as well as for encouraging improvements in the cybersecurity of critical infrastructure within the private sector; however, no overarching cybersecurity strategy had been developed that articulated priority actions, assigned responsibilities for performing them, and set time frames for their completion.[2] Accordingly, we recommended that the White House Cybersecurity Coordinator[3] in the Executive Office of the President develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a national strategy[4] including, among other things, milestones and performance measures for major activities to address stated priorities; cost and resources needed to accomplish stated priorities; and specific roles and responsibilities of federal organizations related to the strategy's stated priorities.

In response to our recommendation, in October 2015, the Director of OMB and the Federal Chief Information Officer, issued a *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*.[5]

[1] This includes the Federal Information Security Modernization Act of 2014, Revision of the Office of Management and Budget's Circular No. A-130, "*Managing Information as a Strategic Resource*" and Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

[2] GAO-13-187.

[3] In December 2009, a Special Assistant to the President was appointed as Cybersecurity Coordinator to address the recommendations made in the Cyberspace Policy Review, including coordinating interagency cybersecurity policies and strategies and developing a comprehensive national strategy to secure the nation's digital infrastructure.

[4] In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. (GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004)).

[5] OMB, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, M-16-04 (Washington, D.C.: Oct. 30, 2015).

The plan directed a series of actions to improve capabilities for identifying and detecting vulnerabilities and threats, enhance protections of government assets and information, and further develop robust response and recovery capabilities to ensure readiness and resilience when incidents inevitably occur. The plan also identified key milestones for major activities, resources needed to accomplish milestones, and specific roles and responsibilities of federal organizations related to the strategy's milestones.

Since that time, the executive branch has made progress toward outlining a federal strategy for confronting cyber threats. Table 1 identifies these recent efforts and a description of their related contents.

Table 1: Recent Executive Branch Initiatives That Identify Cybersecurity Priorities for the Federal Government

Executive branch initiative	Date of issuance	Description
Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	May 2017	The Presidential executive order required federal agencies to take a variety of actions, including better manage their cybersecurity risks and coordinate to meet reporting requirements related to cybersecurity of federal networks, critical infrastructure, and the nation.[a] As of August 2018, the executive branch had publicly released several reports, including a high-level assessment by the Office of Management and Budget (OMB) of the cybersecurity risk management capabilities of the federal government.[b] The assessment stated that OMB and the Department of Homeland Security (DHS) examined the capabilities of 96 civilian agencies across 76 cybersecurity metrics and found that 71 agencies had cybersecurity programs that were either at risk or high risk.[c] The report also stated agencies were not equipped to determine how malicious actors seek to gain access to their information systems and data. The report identified core actions to address cybersecurity risks across the federal enterprise.
National Security Strategy	December 2017	The National Security Strategy[d] identified four vital national interests: protecting the homeland, the American people, and American way of life; promoting American prosperity; preserving peace through strength; and advance American influence. The strategy also cites cybersecurity as a national priority and identifies related needed actions, including identifying and prioritizing risk, building defensible government networks, determining and disrupting malicious cyber actors, improving information sharing and deploying layered defenses.
DHS Cybersecurity Strategy	May 2018	The DHS cybersecurity strategy[e] articulated seven goals the department plans to accomplish in support of its mission related to managing national cybersecurity risks. The goals were spread across five pillars that correspond to DHS-wide risk management, including risk identification, vulnerability reduction, threat reduction, consequence mitigation, and enabling cybersecurity outcomes. The strategy is intended to provide DHS with a framework to execute its cybersecurity responsibilities during the next 5 years to keep pace with the evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient.

Source: GAO analysis of agency documents. | GAO-18-622

[a] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Executive Order 13800 (Washington, D.C.: May 11, 2017).

[b] OMB, *Federal Cybersecurity Risk Determination Report and Action Plan*, (Washington, D.C.: May 2018).

[c] OMB and DHS designated agencies as "at risk" if agencies had some essential policies, processes, and tools in place to mitigate overall cybersecurity risks. OMB and DHS designated agencies as "high risk" if agencies did not have essential policies, processes, and tools in place to mitigate overall cybersecurity risks.

[d] The President of the United States, *National Security Strategy of the United States of America*, (Washington, D.C.: Dec. 2017).

[e] DHS, *U.S. Department of Homeland Security Cybersecurity Strategy*, (Washington, D.C.: May 2018).

These efforts provide a good foundation toward establishing a more comprehensive strategy, but more effort is needed to address all of the desirable characteristics of a national strategy that we recommended. The recently issued executive branch strategy documents did not include key elements of desirable characteristics that can enhance the usefulness of a national strategy as guidance for decision makers in allocating resources, defining policies, and helping to ensure accountability. Specifically:

- Milestones and performance measures to gauge results were generally not included in strategy documents. For example, although the DHS Cybersecurity Strategy stated that its implementation would be assessed on an annual basis, it did not describe the milestones and performance measures for tracking the effectiveness of the activities intended to meet the stated goals (e.g., protecting critical infrastructure and responding effectively to cyber incidents). Without such performance measures, DHS will lack a means to ensure that the goals and objectives discussed in the document are accomplished and that responsible parties are held accountable.

  According to officials from DHS's Office of Cybersecurity and Communications, the department is developing a plan for implementing the DHS Cybersecurity Strategy and expects to issue the plan by the end of calendar year 2018. The officials stated that the plan is expected to identify milestones, roles, and responsibilities across DHS to inform the prioritization of future efforts.

- The strategy documents generally did not include information regarding the resources needed to carry out the goals and objectives. For example, although the DHS Cybersecurity Strategy identified a variety of actions the agency planned to take to perform their cybersecurity mission, it did not articulate the resources needed to carry out these actions and requirements. Without information on the specific resources needed, federal agencies may not be positioned to allocate such resources and investments and, therefore, may be hindered in their ability meet national priorities.

- Most of the strategy documents lacked clearly defined roles and responsibilities for key agencies, such as DHS, DOD, and OMB. These agencies contribute substantially to the nation's cybersecurity programs. For example, although the National Security Strategy discusses multiple priority actions needed to address the nation's cybersecurity challenges (e.g., building defensible government networks, and deterring and disrupting malicious cyber actors), it does not describe the roles, responsibilities, or the expected coordination of any specific federal agencies, including DHS, DOD, or OMB, or other non-federal entities needed to carry out those actions. Without this information, the federal government may not be able foster effective coordination, particularly where there is overlap in responsibilities, or hold agencies accountable for carrying out planned activities.

Ultimately, a more clearly defined, coordinated, and comprehensive approach to planning and executing an overall strategy would likely lead to significant progress in furthering strategic goals and lessening persistent weaknesses.

Appendix III: Action 2—Mitigate Global Supply Chain Risks

The exploitation of information technology (IT) products and services through the supply chain is an emerging threat. IT supply chain-related threats can be introduced in the manufacturing, assembly, and distribution of hardware, software, and services. Moreover, these threats can appear at each phase of the system development life cycle, when an agency initiates, develops, implements, maintains, and disposes of an information system. As a result, the compromise of an agency's IT supply chain can degrade the confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.

Federal regulation and guidance issued by the National Institute of Standards and Technology (NIST) set requirements and best practices for mitigating supply chain risks. The Federal Acquisition Regulation established codification and publication of uniform policies and procedures for acquisition by all executive branch agencies. Agencies are required by the Federal Acquisition Regulation to ensure that contracts include quality requirements that are determined necessary to protect the government's interest. In addition, the NIST guidance on supply chain risk management practices for federal information systems and organizations intends to assist federal agencies with identifying, assessing, and mitigating information and communications technology supply chain risks at all levels of their organizations.

We have previously reported on risks to the IT supply chain and risks originating from foreign-manufactured equipment. For example:

- In July 2018, we testified that if global IT supply chain risks are realized, they could jeopardize the confidentiality, integrity, and availability of federal information systems.[1] Thus, the potential exists for serious adverse impact on an agency's operations, assets, and employees. We further stated that in 2012 we determined that four national security-related agencies—the Departments of Defense, Justice, Energy, Homeland Security (DHS)—varied in the extent to which they had addressed supply chain risks.[2] We recommended that three agencies take eight actions, as needed, to develop and document policies, procedures, and monitoring capabilities that address IT supply chain risk. The agencies generally concurred with

[1] GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies,* GAO-18-667T (Washington, D.C.: July 12, 2018).

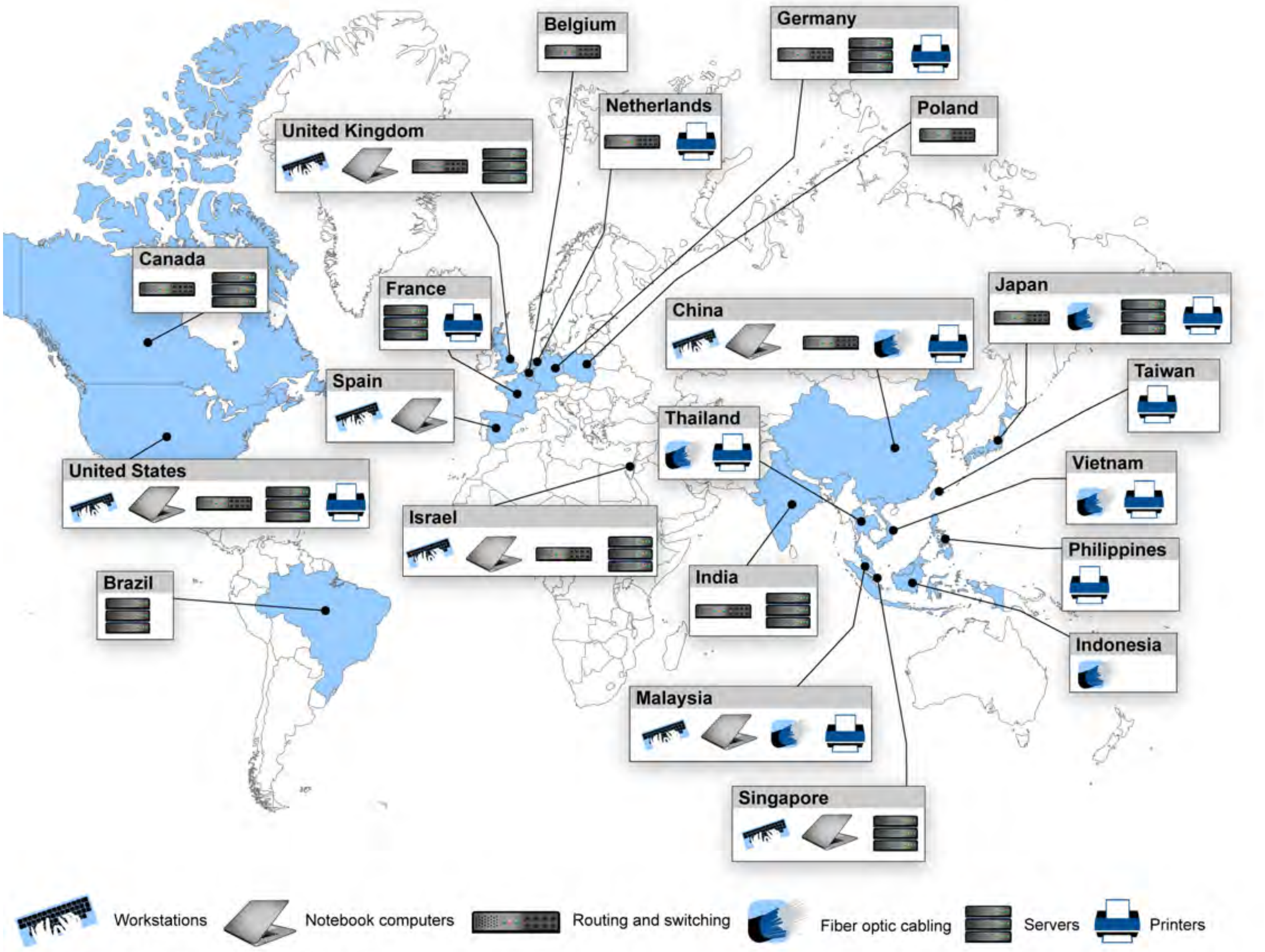
[2] GAO, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361 (Washington, D.C.: Mar. 23, 2012).

the recommendations and subsequently implemented seven recommendations and partially implemented the eighth recommendation.

- In July 2017, we reported that, based on a review of a sample of organizations within the Department of State's telecommunications supply chain, we were able to identify instances in which device manufacturers, software developers and contractor support were reported to be headquartered in a leading cyber-threat nation.[3] For example, of the 52 telecommunications device manufacturers and software developers in our sample, we were able to identify 12 that had 1 or more suppliers that were reported to be headquartered in a leading cyber-threat nation. We noted that the reliance on complex, global IT supply chains introduces multiple risks to federal agencies, including insertion of counterfeits, tampering, or installation of malicious software or hardware. Figure 5 illustrates possible manufacturing locations of typical network components.

[3] GAO, *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations,* GAO-17-688R (Washington, D.C.: July 27, 2017).

Figure 5: Possible Manufacturing Locations of Typical Network Components



Source: GAO analysis of public information. | GAO-18-622

Although federal agencies have taken steps to address IT supply chain deficiencies that we previously identified, this area continues to be a potential threat vector for malicious actors to target the federal government. For example, in September 2017, DHS issued a binding operating directive which calls on departments and agencies to identify any use or presence of Kaspersky products on their information systems and to develop detailed plans to remove and discontinue present and future use of the products. DHS expressed concern about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks.

Appendix IV: Action 3—Address Cybersecurity Workforce Management Challenges

On May 11, 2017, the President issued an executive order on strengthening the cybersecurity of federal networks and critical infrastructure.[1] The order makes it the policy of the United States to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace. It directed the Secretaries of Commerce and Homeland Security (DHS), in consultation with other federal agencies, to assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education.

Nevertheless, the federal government continues to face challenges in addressing the nation's cybersecurity workforce.

- **Agencies had not effectively conducted baseline assessments of their cybersecurity workforce or fully developed procedures for coding positions.** In June 2018, we reported[2] that 21 of the 24 agencies covered by the Chief Financial Officer's Act[3] had conducted and submitted to Congress a baseline assessment identifying the extent to which their cybersecurity employees held professional certifications, as required by the *Federal Cybersecurity Workforce Assessment Act of 2015*.[4] However, we found that the results of these assessments may not have been reliable because agencies did not address all of the reportable information and agencies were limited in their ability to obtain complete and consistent information about their cybersecurity employees and the certifications they held. We

[1] *Presidential Executive Order on Strengthening the* Cybersecurity *of Federal Networks and Critical Infrastructure*. Executive Order 13800 (Washington, D.C.: May 11, 2017).

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

[3] There are 24 agencies identified in the Chief Financial Officers Act: 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.

[4] 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. 303 (Dec. 18, 2015); 129 Stat. 2242, 2975-77.

determined that this was because agencies had not yet fully identified all members of their cybersecurity workforces or did not have a consistent list of appropriate certifications for cybersecurity positions.

Further, 23 of the agencies reviewed had established procedures for identifying and assigning the appropriate employment codes to their civilian cybersecurity positions, as called for by the act. However, 6 of the 23 did not address one or more of 7 activities required by OPM in their procedures, such as reviewing all filled and vacant positions and annotating reviewed position descriptions with the appropriate employment code. Accordingly, we made 30 recommendations to 13 agencies to fully implement two of the act's requirements on baseline assessments and coding procedures. The extent to which these agencies agreed with the recommendations varied.

- **DHS and the Department of Defense (DOD) had not addressed cybersecurity workforce management requirements set forth in federal laws.** In February 2018, we reported[5] that, while DHS had taken actions to identify, categorize, and assign employment codes to its cybersecurity positions,[6] as required by the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*,[7] its actions were not timely and complete. For example, DHS did not establish timely and complete procedures to identify, categorize, and code its cybersecurity position vacancies and responsibilities. Further, DHS had not yet completed its efforts to identify all of its cybersecurity positions and accurately assign codes to all filled and vacant cybersecurity positions. Table 2 shows DHS's progress in implementing the requirements of the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, as of December 2017.

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

[6] These employment codes define work roles and tasks for cybersecurity specialty areas such as program management and system administration.

[7] *The Homeland Security Workforce Assessment Act of 2014*, enacted a part of the *Border Patrol Agent Pay Reform Act of 2014*, was passed by Congress in December 2014. This law requires DHS to identify all cybersecurity workforce positions within the department, determine the cybersecurity work category and specialty area of such positions, and assign the corresponding data element employment code to each cybersecurity position. After completing these activities, DHS was to identify its cybersecurity work categories and specialty areas of critical need within a year of identifying and assigning employment codes, and report these needs annually to OPM. Pub. L. No. 113-277, § 3,128 Stat. 2995, 3008-3010 (Dec. 18, 2014), 6 U.S.C. § 146.

Table 2: The Department of Homeland Security's Progress in Implementing Requirements of the Homeland Security Cybersecurity Workforce Assessment Act of 2014, as of December 2017

Required activity		Due date	Completion date
1.	Establish procedures to identify, categorize, and code cybersecurity positions.	Mar. 2015	Apr. 2016
2.	Identify all positions with cybersecurity functions and determine work category and specialty areas of each position.	Sept. 2015	Ongoing
3.	Assign codes to all filled and vacant cybersecurity positions.	Sept. 2015	Ongoing
4.	Identify and report critical needs in specialty areas to Congress.	Jun. 2016	Not addressed
5.	Report critical needs annually to the Office of Personnel Management.	Sept. 2016	Not addressed

Source: GAO analysis of Department of Homeland Security documentation and the Homeland Security Cybersecurity Workforce Assessment Act of 2014. | GAO-18-622

Accordingly, we recommended that DHS take six actions, including ensuring that its cybersecurity workforce procedures identify position vacancies and responsibilities; reported workforce data are complete and accurate; and plans for reporting on critical needs are developed. DHS agreed with our six recommendations, but had not implemented them as of August 2018.

Regarding DOD, in November 2017, we reported[8] that instead of developing a comprehensive plan for U.S. Cyber Command, the department submitted a report consisting of a collection of documents that did not fully address the required six elements set forth in Section 1648 of the *National Defense Authorization Act for Fiscal Year 2016*.[9] More specifically, DOD's 1648 report did not address an element related to cyber incident training. In addition to not addressing the training element in the report, DOD had not ensured that staff were trained as required by the *Presidential Policy Directive on United*

[8] GAO, *Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements,* GAO-18-47 (Washington, D.C.: Nov. 30, 2017).

[9] Section 1648 of the *National Defense Authorization Act for Fiscal Year 2016* included a provision that DOD develop a comprehensive plan for U.S. Cyber Command to support civil authorities in responding to cyberattacks by foreign powers against the United States. Among the elements required in the plan is a description of internal DOD collective training activities that are integrated with exercises conducted with other agencies and state and local governments. Pub. L. No. 114-92, § 1648(a) (2015).

States Cyber Incident Coordination[10] or DOD's Significant Cyber Incident Coordination Procedures.

Accordingly, we made two recommendations to DOD to address these issues. DOD agreed with one of the recommendations and partially agreed with the other, citing ongoing activities related to cyber incident coordination training it believed were sufficient. However, we continued to believe the recommendation was warranted. As of August 2018, both recommendations had not yet been implemented.

- **Agencies had not identified and closed cybersecurity skills gaps.** In November 2016, we reported that five selected agencies[11] had made mixed progress in assessing their information technology (IT) skill gaps.[12] These agencies had started focusing on identifying cybersecurity staffing gaps, but more work remained in assessing competency gaps and in broadening the focus to include the entire IT community. Accordingly, we made a total of five recommendations to the agencies to address these issues. Four agencies agreed and one, DOD, partially agreed with our recommendations citing progress made in improving its IT workforce planning. However, we continued to believe our recommendation was warranted. As of August 2018, all five of the recommendations had not been implemented.
- **Agencies had been challenged with recruiting and retaining qualified staff.** In August 2016, we reported on the current authorities chief information security officers (CISO) at 24 agencies.[13] Among other things, CISOs identified key challenges they faced in fulfilling

[10] *Presidential Policy Directive – United States Cyber Incident Coordination/PPD-41* (July 26, 2016). PPD-41 requires federal agencies, including DOD, to update cyber incident coordination training to incorporate the tenets of PPD-41 by December 2016 and to identify and maintain a cadre of personnel qualified and trained in the National Incident Management System and unified coordination to manage and respond to a significant cyber incident.

[11] The five selected agencies reviewed were the Department of Commerce, the Department of Defense, the Department of Health and Human Services, the Department of Transportation, and the Department of the Treasury.

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

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

their responsibilities. Several of these challenges were related to the cybersecurity workforce, such as not having enough personnel to oversee the implementation of the number and scope of security requirements. In addition, CISOs stated that they were not able to offer salaries that were competitive with the private sector for candidates with high-demand technical skills. Furthermore, CISOs stated that certain security personnel lacked the skill sets needed or were not sufficiently trained. To assist CISOs in carrying out their responsibilities and better define their roles, we made a total of 34 recommendations to the Office of Management and Budget (OMB) and 13 agencies in our review. Agency responses to the recommendations varied; as of August 2018, 18 of the 34 recommendations had not been implemented.

- **Agencies have had difficulty navigating the federal hiring process.** In August 2016, we reported on the extent to which federal hiring authorities were meeting agency needs.[14] Although competitive hiring has been the traditional method of hiring, agencies can use additional hiring authorities to expedite the hiring process or achieve certain public policy goals. Among other things, we noted that agencies rely on a relatively small number of hiring authorities (as established by law, executive order, or regulation) to fill the vast majority of hires into the federal civil service.

  Further, while OPM collects a variety of data to assess the federal hiring process, neither it nor agencies used this information to assess the effectiveness of hiring authorities. Conducting such assessments would be a critical first step in making more strategic use of the available hiring authorities to more effectively meet their hiring needs. Accordingly, we made three recommendations to OPM to work with agencies to strengthen hiring efforts. OPM generally agreed with the recommendations; however, as of August 2018, two of them had not been implemented.

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

Appendix V: Action 4—Ensure the Security of Emerging Technologies

The emergence of new technologies can potentially introduce security vulnerabilities for those technologies which were previous unknown. As we have previously reported, additional processes and controls will need to be developed to potentially address these new vulnerabilities. While some progress has been made to address the security and privacy issues associated with these technologies, such as the Internet of Things (IoT)[1] and vehicle networks, there is still much work to be done. For example:

- **IoT devices that continuously collect and process information are potentially vulnerable to cyber-attacks.** In May 2017, we reported that the IoT has become increasingly used to communicate and process vast amounts of information using "smart" devices (such as fitness trackers, cameras, and thermostats).[2] However, we noted that this emerging technology also presents new issues in areas such as information security, privacy, and safety. For example, IoT devices, networks, or the cloud servers where they store data can be compromised in a cyberattack. Table 3 provides examples of cyber-attacks that could affect IoT devices and networks.

[1] IoT refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information.

[2] GAO, *Technology Assessment: Internet of Things: Status and implications of an increasingly connected world*, GAO-17-75 (Washington, D.C.: May 15, 2017).

Table 3: Types of Attacks Possible with Internet of Things Devices

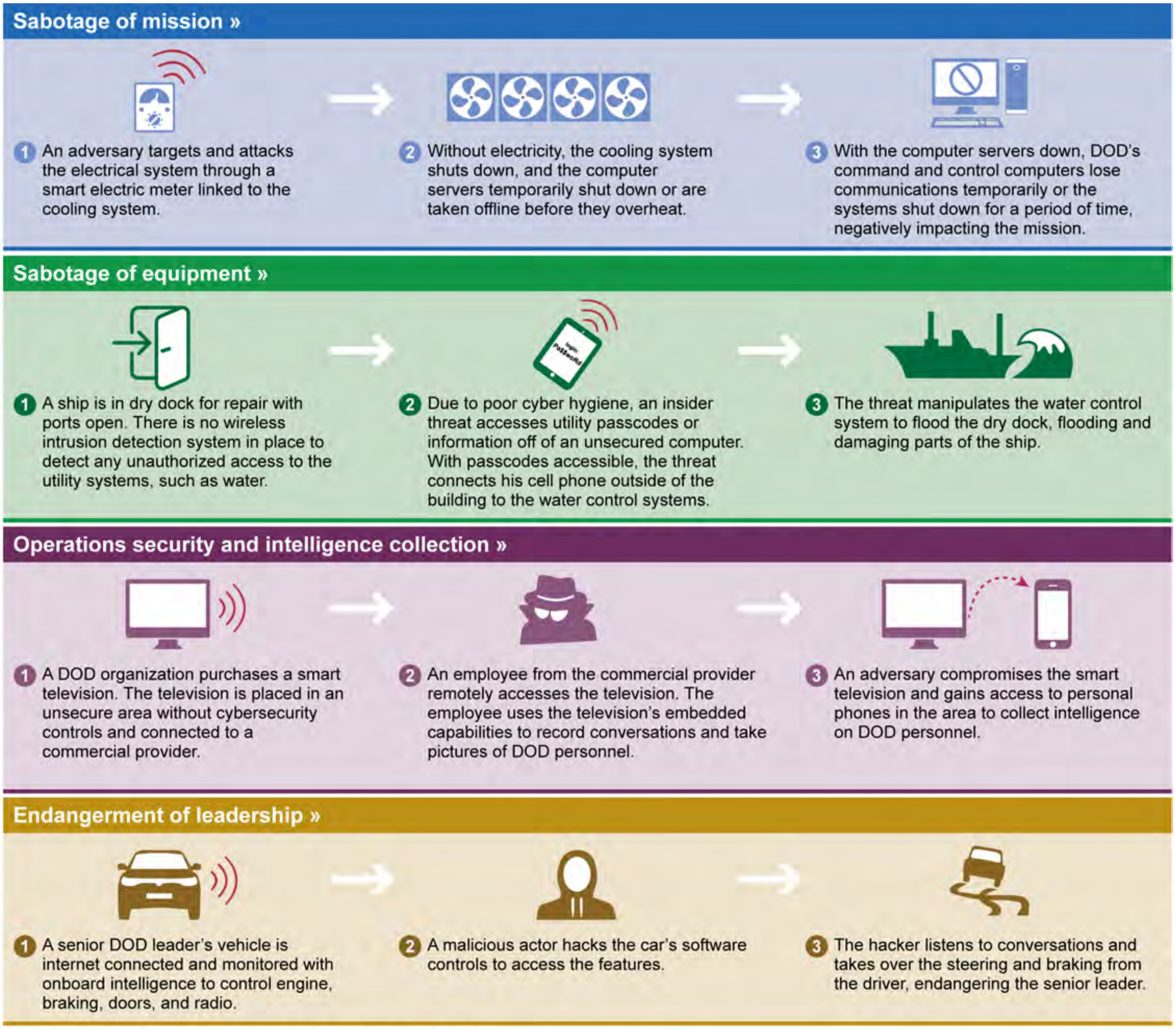
Type of attack	Description
Denial-of-Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial-of-service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Malware	Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples include logic bombs, Trojan horses, ransomware, viruses, and worms.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Structured query language injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and Industry Reports. | GAO-18-622

- **IoT devices may increase the security risks to federal agencies.** In July 2017, we reported that IoT devices, such as those acquired and used by Department of Defense (DOD) employees or that DOD itself acquires (e.g., smartphones), may increase the security risks to the department.[3] We noted that these risks can be divided into two categories, risks with the devices themselves, such as limited encryption, and risks with how they are used, such as unauthorized communication of information. The department has also identified notional threat scenarios, based on input from multiple DOD entities, which exemplify how these security risks could adversely impact DOD operations, equipment, or personnel. Figure 6 highlights a few examples of these scenarios.

[3] GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-668 (Washington, D.C.: July 27, 2017).

Figure 6: Notional Internet of Things (IoT) Scenarios Identified by Department of Defense (DOD)



Sabotage of mission »

1 An adversary targets and attacks the electrical system through a smart electric meter linked to the cooling system.

2 Without electricity, the cooling system shuts down, and the computer servers temporarily shut down or are taken offline before they overheat.

3 With the computer servers down, DOD's command and control computers lose communications temporarily or the systems shut down for a period of time, negatively impacting the mission.

Sabotage of equipment »

1 A ship is in dry dock for repair with ports open. There is no wireless intrusion detection system in place to detect any unauthorized access to the utility systems, such as water.

2 Due to poor cyber hygiene, an insider threat accesses utility passcodes or information off of an unsecured computer. With passcodes accessible, the threat connects his cell phone outside of the building to the water control systems.

3 The threat manipulates the water control system to flood the dry dock, flooding and damaging parts of the ship.

Operations security and intelligence collection »

1 A DOD organization purchases a smart television. The television is placed in an unsecure area without cybersecurity controls and connected to a commercial provider.

2 An employee from the commercial provider remotely accesses the television. The employee uses the television's embedded capabilities to record conversations and take pictures of DOD personnel.

3 An adversary compromises the smart television and gains access to personal phones in the area to collect intelligence on DOD personnel.

Endangerment of leadership »

1 A senior DOD leader's vehicle is internet connected and monitored with onboard intelligence to control engine, braking, doors, and radio.

2 A malicious actor hacks the car's software controls to access the features.

3 The hacker listens to conversations and takes over the steering and braking from the driver, endangering the senior leader.

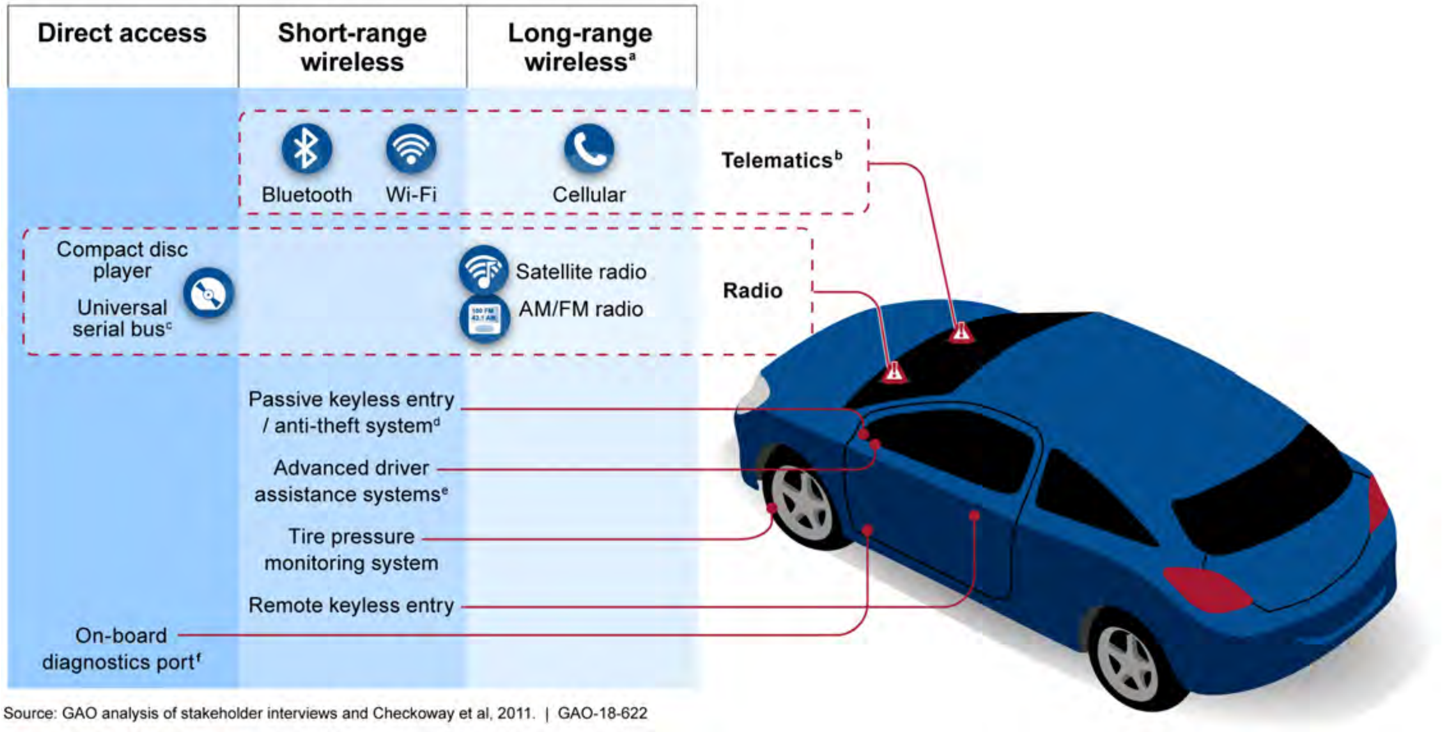
Source: GAO analysis of Department of Defense (DOD) information. | GAO-18-622

In addition, we reported that DOD had started to examine the security risks of IoT devices, but that the department had not conducted required assessments related to the security of its operations. Further, DOD had issued policies and guidance for these devices, but these did not clearly address all of the risks relating to these devices. To address these issues, we made two recommendations to DOD. The department agreed with our recommendations; however, as of August 2018, they had not yet been implemented.

- **Vehicles are potentially susceptible to cyber-attack through networks, such as Bluetooth.** In March 2016, we reported that many stakeholders in the automotive industry acknowledge that in-vehicle networks pose a threat to the safety of the driver, as an external attacker could gain control to critical systems in the car.[4] Further, these industry stakeholders agreed that critical systems and other vehicle systems, such as a Bluetooth connection, should be separate in-vehicle networks so they could not communicate or interfere with one another. Figure 7 identifies the key interfaces that could be exploited in a vehicle cyber-attack.

[4] GAO, *Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack*, GAO-16-350 (Washington, D.C.: Apr. 25, 2016).

Figure 7: Key Interfaces That Could Be Exploited in a Vehicle Cyberattack



Source: GAO analysis of stakeholder interviews and Checkoway et al, 2011. | GAO-18-622

[a] In this context, long-range refers to access at distances over 1 kilometer.

[b] Universal serial bus storage devices are used to store text, video, audio, and image information. By inserting such devices into the vehicle's universal serial bus port, users can access stored information through the vehicle's radio or other media systems.

[c] These systems can prevent the car from operating unless the correct key is present, as verified by the presence of the correct radio-frequency identification tag.

[d] This port is mandated in vehicles by regulation for emission-testing purposes and to facilitate diagnostic assessments of vehicles, such as by repair shops.

[e] These systems use on-board sensors and other cameras to assist the driver in undertaking certain functions, such as changing lanes or braking suddenly.

[f] Vehicle telematics systems—which include the dashboard, controls, and navigation systems—provide continuous connectivity to long- and short-range wireless connections.

To enhance the Department of Transportation's ability to effectively respond in the event of a real-world vehicle cyberattack, we made one recommendation to the department to better define its roles and responsibilities. The department agreed with the recommendation but, as of August 2018, had not yet taken action to implement it.

- **Artificial intelligence holds substantial promise for improving cybersecurity, but also posed new risks.** In March 2018, we reported on the results of a forum we convened to discuss emerging opportunities, challenges, and implications associated with artificial intelligence.[5] At the forum, participants from industry, government, academia, and nonprofit organizations discussed the potential implications of this emerging technology, including assisting with cybersecurity by helping to identify and patch vulnerabilities and defending against attacks; creating safer automated vehicles; improving the criminal justice system's allocation of resources; and improving how financial services govern investments.

  However, forum participants also highlighted a number of challenges and risks related to artificial intelligence. For example, if the data used by artificial intelligence are biased or become corrupted by hackers, the results could be biased or cause harm. Moreover, the collection and sharing of data needed to train artificial intelligence systems, a lack of access to computing resources, and adequate human capital were also challenges facing the development of artificial intelligence. Finally, forum participants noted that the widespread adoption raises questions about the adequacy of current laws and regulations.

- **Cryptocurrencies provide an alternative to traditional government-issued currencies, but have security implications.** In February 2018, we reported on trends affecting government and society, including the increased use of cryptocurrencies—digital representations of value that are not government-issued—that operate online and verify transactions using a public ledger called blockchain.[6] We highlighted the potential benefits of this technology, such as anonymity and lower transaction costs, as well as drawbacks, including making it harder to detect money laundering and other financial crimes. Because of these capabilities and others, we noted the potential for virtual currencies and blockchain technology to reshape financial services and affect the security of critical financial infrastructures. Lastly, we pointed out that the use of blockchain technology could have more security vulnerabilities as computing power increases as a result of new advancements in quantum computing, an area of quantum information science.

[5] GAO, *Technology Assessment: Artificial Intelligence, Emerging Opportunities, Challenges, and Implications*, GAO-18-142SP (Washington, D.C.: Mar. 28, 2018).

[6] GAO, *Strategic Plan 2018-2023; Trends Affecting Government and Society*, GAO-18-396SP (Washington, D.C.: Feb 28, 2018).

Appendix VI: Action 5—Improve Implementation of Government-wide Cybersecurity Initiatives

In January 2008, the President issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23. The directive established the Comprehensive National Cybersecurity Initiative, a set of projects with the objective of safeguarding federal executive branch government information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats against the federal government's networks. Under the initiative, the Department of Homeland Security (DHS) was to lead several projects to better secure civilian federal government networks. Specifically, the agency established the National Cybersecurity and Communications Integration Center (NCCIC), which functions as the 24/7 cyber monitoring, incident response, and management center. Figure 8 depicts the Watch Floor, which functions as a national focal point of cyber and communications incident integration.

Figure 8: The National Cybersecurity and Communications Integration Center Watch Floor

Source: Department of Homeland Security, National Cybersecurity and Communications Integration Center. | GAO-18-622

The United States Computer Emergency Readiness Team (US-CERT), one of several subcomponents of the NCCIC, is responsible for operating the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to entities across the federal government.

Although DHS is fulfilling its statutorily required mission by establishing the NCCIC and managing the operation of NCPS,[1] we have identified challenges in the agency's efforts to manage these programs:

- **DHS had not ensured that NCPS has fully satisfied all intended system objectives.** In January 2016, we reported that NCPS had a limited ability to detect intrusions across all types of network types.[2] In addition, we reported that the system's intrusion prevention capability was limited and its information-sharing capability was not fully developed. Furthermore, we reported that DHS's current metrics did not comprehensively measure the effectiveness of NCPS. Accordingly, we made nine recommendations to DHS to address these issues and others. The department agreed with our recommendations and has taken action to address one of them. However, as of August 2018, eight of these recommendations had not been implemented.
- **DHS had been challenged in measuring how the NCCIC was performing its functions in accordance with mandated implementing principles.** In February 2017, we reported[3] instances where, with certain products and services, NCCIC had implemented its functions in adherence with one or more of its principles, as required by the National Cybersecurity Protection Act of 2014 and Cybersecurity Act of 2015.[4] For example, consistent with the principle that it seek and receive appropriate consideration from industry sector-specific, academic, and national laboratory expertise, NCCIC coordinated with contacts from industry, academia, and the national laboratories to develop and disseminate vulnerability alerts.

[1] NCPS is intended to provide DHS with capabilities to detect malicious traffic traversing federal agencies' computer networks, prevent intrusions, and support data analytics and information sharing.

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

[3] GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely,* GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

[4] *The National Cybersecurity Protection Act of 2014* and *Cybersecurity Act of 2015* require NCCIC to carry out 11 cybersecurity functions, to the extent practicable, in accordance with nine principles. Pub. L. No. 113-282, Dec. 18, 2014. The Cybersecurity Act of 2015 was enacted as Division N of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Dec. 18, 2015.

However, we also identified instances where the cybersecurity functions were not performed in adherence with the principles. For example, NCCIC is to provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities, but it had not established measures or other procedures for ensuring the timeliness of these assessments. Further, we reported that NCCIC faces impediments to performing its cybersecurity functions more efficiently, such as tracking security incidents and working across multiple network platforms. Accordingly, we made nine recommendations to DHS related to implementing the requirements identified in the National Cybersecurity Protection Act of 2014 and the Cybersecurity Act of 2015. The department agreed with our recommendations and has taken action to address two of them. However, as of August 2018, the remaining seven recommendations had not been implemented.

Appendix VII: Action 6—Address Weaknesses in Federal Agency Information Security Programs

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies in the executive branch to develop, document, and implement an information security program and evaluate it for effectiveness.[1] The act retains many of the requirements for federal agencies' information security programs previously set by the Federal Information Security Management Act of 2002.[2] These agency programs should include periodic risk assessments; information security policies and procedures; plans for protecting the security of networks, facilities, and systems; security awareness training; security control assessments; incident response procedures; a remedial action process, and continuity plans and procedures.

In addition, Executive Order 13800[3] states that the President will hold agency heads accountable for managing cybersecurity risk to their enterprises. In addition, according to the order, it is the policy of the United States to manage cybersecurity risk as an executive branch enterprise because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security.

Over the past several years, we have performed numerous security control audits to determine how well agencies are managing information security risk to federal information systems and data through the implementation of effective security controls. These audits have resulted in the identification of hundreds of deficiencies related to agencies' implementation of effective security controls. Accordingly, we provided agencies with limited official use only reports identifying technical security control deficiencies for their respective agency. In these reports, we made hundreds of recommendations related to improving agencies' implementation of those security control deficiencies.

In addition to systems and networks maintained by federal agencies, it is also important that agencies ensure the security of federal information systems operated by third party providers, including cloud service

[1] The *Federal Information Security Modernization Act of 2014* was enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014), and amended chapter 35 of Title 44, U.S. Code.

[2] The *Federal information Security Management Act of 2002* was enacted as Pub.L. No. 107-347, Title III, 116 Stat.2899, 2946 (Dec. 17, 2002).

[3] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Executive Order 13800 (Washington, D.C.: May 11, 2017).

providers. Cloud computing is a means for delivering computing services via information technology networks. Since 2009, the government has encouraged agencies to use cloud-based services to store and process data as a cost-savings measure. In this regard, the Office of Management and Budget (OMB) established the Federal Risk and Authorization Management Program (FedRAMP) to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is intended to ensure that cloud computing services have adequate information security, eliminate duplicative efforts, and reduce costs.

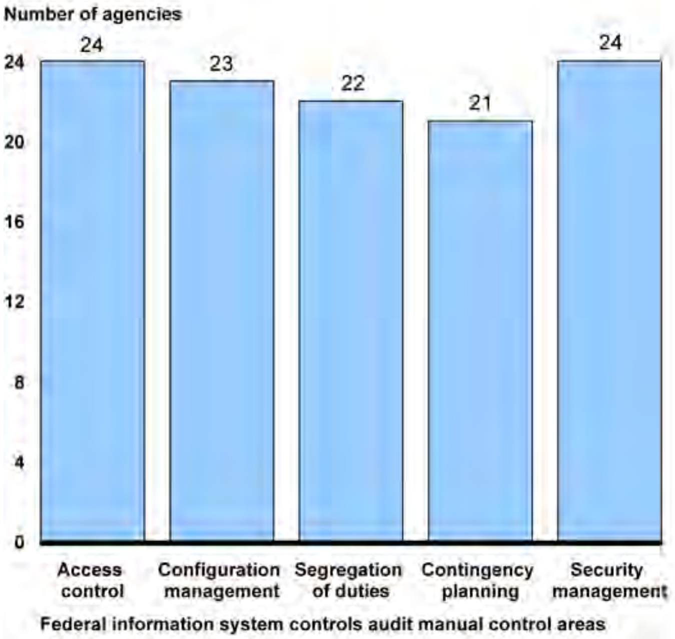
Although there are requirements and government-wide programs to assist with ensuring the security of federal information systems maintained by federal agencies and third party providers, we have identified weaknesses in agencies' implementation of information security programs.

- **Federal agencies continued to experience weaknesses in protecting their information and information systems due to ineffective implementation of information security policies and practices.** In September 2017, we reported that most of the 24 agencies covered by the Chief Financial Officers (CFO) Act[4] had weaknesses in each of the five major categories of information system controls (i.e., access controls, configuration management controls, segregation of duties, contingency planning, and agency-wide security management).[5] Weaknesses in these security controls indicate that agencies did not adequately or effectively implement information security policies and practices during fiscal year 2016. Figure 9 identifies the number of agencies with information security weaknesses in each of the five categories.

[4] There are 24 agencies identified in the Chief Financial Officers Act: 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.

[5] GAO, *Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices,* GAO-17-549 (Washington, D.C.: Sept. 28, 2017).

Figure 9: The 24 Chief Financial Officers Act Agencies with Information Security Weaknesses in the Major Information System Control Categories, Fiscal Year 2016



Source: GAO analysis of agency, inspectors general, and GAO reports on the 24 *Chief Financial Officers Act* agencies' information security practices and policies for fiscal year 2016. | GAO-18-622

Note: The 24 agencies identified in the Chief Financial Officers Act: 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.

In addition, we found that several agencies had not effectively implemented some aspects of its information security program, which resulted in weaknesses in these agencies' security controls.

- In July 2017, we reported that the Security Exchange Commission did not always keep system security plans complete and accurate or fully implement continuous monitoring, as required by agency policy.[6] We made two recommendations to the Security Exchange Commission to effectively manage its information security program. The agency

[6] GAO, *Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions,* GAO-17-469 (Washington, D.C.: July 27, 2017).

agreed with our recommendations; however, as of August 2018, they had not been implemented.

- In another July 2017 report, we noted that the Internal Revenue Service (IRS) did not effectively support a risk-based decision to accept system deficiencies; fully develop, document, or update information security policies and procedures; update system security plans to reflect changes to the operating environment; perform effective tests and evaluations of policies, procedures, and controls; or address shortcomings in the agency's remedial process.[7] Accordingly, we made 10 recommendations to IRS to more effectively implement security-related policies and plans. The agency neither agreed nor disagreed with the recommendations; as of August 2018, all 10 recommendations had not been implemented.
- In May 2017, we reported that the Federal Deposit Insurance Corporation did not include all necessary information in procedures for granting access to a key financial application; fully address its Inspector General findings that security control assessments of outsourced service providers had not been completed in a timely manner; fully address key previously identified weaknesses related to establishing agency-wide configuration baselines and monitoring changes to critical server files; or complete actions to address the Inspector General's finding that the Federal Deposit Insurance Corporation had not ensured that major security incidents are identified and reported in a timely manner.[8] We made one recommendation to the agency to more fully implement its information security program. The agency agreed with our recommendation and has taken steps to implement it.
- In August 2016, we reported that the Food and Drug Administration did not fully implement certain security practices involved with assessing risks to systems; complete or review security policies and procedures in a timely manner; complete and review system security plans annually; always track and fully train users with significant security responsibilities; fully test controls or monitor them; remediate identified security weaknesses in a timely fashion based on risk; or

[7] GAO, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data,* GAO-17-395 (Washington, D.C.: July 26, 2017).

[8] GAO, *Information Security: FDIC Needs to Improve Controls over Financial Systems and Information,* GAO-17-436 (Washington, D.C.: May 31, 2017).

fully implement elements of its incident response program.[9] Accordingly, we issued 15 recommendations to the Food and Drug Administration to fully implement its agency-wide information security program. The agency agreed with our recommendations. As of August 2018, all 15 recommendations had been implemented.

- In May 2016, we reported that a key reason for the information security weaknesses in selected high-impact systems at four agencies—National Aeronautics and Space Administration, Nuclear Regulatory Commission, the Office of Personnel Management, and Department of Veterans Affairs—was that they had not effectively implemented elements of their information security programs.[10] For example, most of the selected agencies had conducted information security control assessments for systems, but not all assessments were comprehensive. We also reported that remedial action plans developed by the agencies did not include all the required elements, and not all agencies had developed a continuous monitoring strategy. Table 4 identifies the extent to which the selected agencies implemented key aspects of their information security programs.

Table 4: Agency Implementation of Key Information Security Program Elements for Selected Systems

	National Aeronautics and Space Administration	Nuclear Regulatory Commission	Office of Personnel Management	Department of Veterans Affairs
Risk assessments	●	●	●	●
Security plans	●	◐	◐	◐
Controls assessments	◐	◐	◐	○
Remedial action plans	◐	◐	◐	◐

Note: ● – Met ◐ – Partially Met ○ – Did not meet

Source: GAO analysis of agency documentation. | GAO-18-622

Accordingly, we made 19 recommendations to the four selected agencies to correct these weaknesses. Agency responses to the recommendations varied. Further, as of August 2018, 16 of the 19 recommendations had not been implemented.

[9] GAO, *Information Security: FDA Needs to Rectify Control Weaknesses That Place Industry and Public Health Data at Risk,* GAO-16-513 (Washington, D.C.: Aug. 30, 2016).

[10] GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems,* GAO-16-501 (Washington, D.C.: May 18, 2016).

- **DOD's monitoring of progress in implementing cyber strategies varied.** In August 2017, we reported[11] that the DOD's progress in implementing key strategic cybersecurity guidance—the *DOD Cloud Computing Strategy*, *DOD Cyber Strategy*, and *DOD Cybersecurity Campaign*—has varied.[12] More specifically, we determined that the department had implemented the cybersecurity objectives identified in the *DOD Cloud Computing Strategy* and had made progress in implementing the *DOD Cyber Strategy* and *DOD Cybersecurity Campaign*. However, the department's process for monitoring implementation of the *DOD Cyber Strategy* had resulted in the closure of tasks as implemented before the tasks were fully implemented. In addition, the *DOD Cybersecurity Campaign* lacked time frames for completion and a process to monitor progress, which together provide accountability to ensure implementation.

  We made two recommendations to improve DOD's process of ensuring its cyber strategies are effectively implemented. The department partially concurred with these recommendations and identified actions it planned to take to address them. We noted that, if implemented, the actions would satisfy the intent of our recommendations. However, as of August 2018, DOD had not yet implemented our recommendations.

- **Agencies had not fully defined the role of their Chief Information Security Officers (CISO), as required by FISMA.** In August 2016, we reported[13] that 13 of 24 agencies covered by the CFO Act had not fully defined the role of their CISO.[14] For example, these agencies did not always identify a role for the CISO in ensuring that security controls are periodically tested; procedures are in place for detecting, reporting, and responding to security incidents; or contingency plans and procedures for agency information systems are in place. Thus,

[11] GAO, *Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened,* GAO-17-512 (Washington, D.C.: Aug. 1, 2017).

[12] Department of Defense Chief Information Officer, *Cloud Computing Strategy* (July 2012); Department of Defense. *DOD Cybersecurity Campaign* (June 2015) (For official use only); and Department of Defense, *The Department of Defense Cyber Strategy* (April 2015) (hereinafter cited as *The DOD Cyber Strategy*).

[13] GAO-16-686.

[14] Under the *Federal Information Security Modernization Act of 2014*, the agency CISO has the responsibility to ensure that the agency is meeting the requirements of the law, including developing, documenting, and implementing the agency-wide information security program.

we determined that the CISOs' ability to effectively oversee these agencies' information security activities can be limited.

To assist CISOs in carrying out their responsibilities and better define their roles, we made a total of 34 recommendations to OMB and 13 agencies in our review. Agency responses to the recommendations varied; as of August 2018, 18 of the 34 recommendations had not been implemented.

Appendix VIII: Action 7—Enhance the Federal Response to Cyber Incidents

Presidential Policy Directive-41[1] sets forth principles governing the federal government's response to any cyber incident, whether involving government or private sector entities. According to the directive, federal agencies shall undertake three concurrent lines of effort when responding to any cyber incident: threat response;[2] asset response;[3] and intelligence support and related activities.[4] In addition, when a federal agency is an affected entity, it shall undertake a fourth concurrent line of effort to manage the effects of the cyber incident on its operations, customers, and workforce.

We have reviewed federal agencies' preparation and response to cyber incidents and have identified the following weaknesses:

- **The Office of Personnel Management (OPM) had not fully implemented controls to address deficiencies identified as a result of a cyber incident**. In August 2017, we reported that OPM did not fully implement the 19 recommendations made by the Department of Homeland Security's (DHS) United States Computer Emergency

[1] The White House, *Presidential Policy Directive 41: United States Cyber Incident Coordination* (Washington, D.C.: July 2016).

[2] Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing an operational coordination with asset response.

[3] Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk of the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.

[4] Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.

Readiness Team (US-CERT)[5] after the data breaches in 2015.[6] Specifically, we noted that, after breaches of personnel and background investigation information were reported, US-CERT worked with the agency to resolve issues and develop a comprehensive mitigation strategy. In doing so, US-CERT made 19 recommendations[7] to OPM to help the agency improve its overall security posture and, thus, improve its ability to protect its systems and information from security breaches.

In our August 2017 report, we determined that OPM had fully implemented 11 of the 19 recommendations. For the remaining 8 recommendations, actions for 4 were still in progress. For the other 4 recommendations, OPM indicated that it had completed actions to address them, but we noted further improvements were needed. Further, OPM had not validated actions taken to address the recommendations in a timely manner.

As a result of our review, we made five other recommendations to OPM to improve its response to cyber incidents. The agency agreed with four of these and partially concurred with the one related to validating its corrective action. The agency did not cite a reason for its partial concurrence and we continued to believe that the recommendation was warranted. As of August 2018, three of the five recommendations had not been implemented.

- **The Department of Defense (DOD) had not identified the National Guard's cyber capabilities (e.g., computer network defense teams) or addressed challenges in its exercises.** In September 2016, we reported that DOD had not identified the National Guard's cyber capabilities or addressed challenges in its exercises.[8]

[5] US-CERT, a branch of DHS's National Cybersecurity and Communications Integration Center, is a central Federal information security incident center that compiles and analyzes information about incidents that threaten information security.

[6] GAO, *Information Security: OPM Has Improved Controls, but Further Efforts Are Needed,* GAO-17-614 (Washington, D.C.: Aug. 3, 2017).

[7] Due to the sensitive nature of the recommendations, we did not provide specific recommendations or specific examples associated with them in the related report. Generally, the recommendations pertained to strengthening activities and controls related to passwords, access permissions, patches, audit and monitoring, among other things.

[8] GAO, *Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises,* GAO-16-574 (Washington, D.C.: Sept. 6, 2016).

Specifically, DOD had not identified and did not have full visibility into National Guard cyber capabilities that could support civil authorities during a cyber incident because the department has not maintained a database that identifies National Guard cyber capabilities, as required by the *National Defense Authorization Act for Fiscal Year 2007*. In addition, we identified three types of challenges with DOD's cyber exercises that could limit the extent to which DOD is prepared to support civilian authorities in a cyber incident:

- limited access because of classified exercise environments;
- limited inclusion of other federal agencies and critical infrastructure owners; and
- inadequate incorporation of joint physical-cyber scenarios.

In our September 2016 report, we noted that DOD had not addressed these challenges. Furthermore, we stated that DOD had not addressed its goals by conducting a "tier 1" exercise (i.e., an exercise involving national-level organizations and combatant commanders and staff in highly complex environments), as stated in the *DOD Cyber Strategy*.[9]

Accordingly, we recommended that DOD (1) maintain a database that identifies National Guard cyber capabilities and (2) conduct a tier 1 exercise to prepare its forces in the event of a disaster with cyber effects. The department partially agreed with our recommendations, stating that its current mechanisms and exercises are sufficient to address the issues highlighted in our report. However, we continued to believe the recommendations were valid. As of August 2018, our two recommendations had not been implemented.

- **DOD had not identified, clarified, or implemented all components of its incident response program.** In April 2016, we also reported that DOD had not clarified its roles and responsibilities for defense support of civil authorities during cyber incidents.[10] Specifically, we

[9] DOD is to conduct tier 1 exercises that are designed to prepare national-level organizations and combatant commanders and staffs at the strategic and operational level to integrate interagency, non-governmental, and multinational partners in highly complex environments. The goal of these exercises is to integrate a diverse audience in a joint training environment and identify core competencies, procedural disconnects, and common ground to achieve U.S. unity of effort.

[10] GAO, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents,* GAO-16-332 (Washington, D.C.: Apr. 4, 2016).

found that DOD's overarching guidance about how it is to support civil authorities as part of its Defense Support of Civil Authorities mission did not clearly define the roles and responsibilities of key DOD entities, such as DOD components, the supported command, or the dual-status commander, if they are requested to support civil authorities in a cyber incident. Further, we found that, in some cases, DOD guidance provides specific details on other types of Defense Support of Civil Authorities-related responses, such as assigning roles and responsibilities for fire or emergency services support and medical support, but does not provide the same level of detail or assign roles and responsibilities for cyber support.

Accordingly, we recommended that DOD issue or update guidance that clarifies DOD roles and responsibilities to support civil authorities in a domestic cyber incident. DOD concurred with the recommendation and stated that the department will issue or update guidance. However, as of August 2018, the department had not implemented our recommendation.

- **DHS's NCPS had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information.** In January 2016, we reported that NCPS had a limited ability to detect intrusions across all types of network types.[11] In addition, we reported that the system's intrusion prevention capability was limited and its information-sharing capability was not fully developed. Furthermore, we reported that DHS's current metrics did not comprehensively measure the effectiveness of NCPS. Accordingly, we made nine recommendations to DHS to address these issues and others. The department agreed with our recommendations and has taken action to address one of them. However, as of August 2018, eight of these recommendations had not been implemented.

[11] GAO-16-294.

Appendix IX: Action 8—Strengthen the Federal Role in Protecting the Cybersecurity of Critical Infrastructure

The nation's critical infrastructure include both public and private systems vital to national security and other efforts including providing the essential services, such as banking, water, and electricity—that underpin American society. The cyber threat to critical infrastructure continues to grow and represents a national security challenge. To address this cyber risk, the President issued Executive Order 13636[1] in February 2013 to enhance the security and resilience of the nation's critical infrastructure and maintain a cyber environment that promotes safety, security, and privacy.

In accordance with requirements in the executive order which were enacted into law in 2014, the National Institute of Standards and Technology (NIST) facilitated the development of a set of voluntary standards and procedures for enhancing cybersecurity of critical infrastructure. This process, which involved stakeholders from the public and private sectors, resulted in NIST's *Framework for Improving Critical Infrastructure Cybersecurity.*[2] The framework is to provide a flexible and risk-based approach for entities within the nation's 16 critical infrastructure sectors to protect their vital assets from cyber-based threats. Since then, progress has been made to protect the critical infrastructure of the nation but we have reported that challenges to ensure the safety and security of our infrastructure exist.

- **The Department of Homeland Security (DHS) had not measured the impact of its efforts to support cyber risk reduction for high-risk chemical sector entities.** In August 2018, we reported that DHS had strengthened its processes for identifying high-risk chemical facilities and assigning them to tiers under its Chemical Facility Anti-Terrorism Standards program.[3] However, we found that DHS's new performance measure methodology did not measure reduction in vulnerability at a facility resulting from the implementation and verification of planned security measures during the compliance inspection process. We concluded that doing so would provide DHS an opportunity to begin assessing how vulnerability is reduced—and by extension, risk lowered—not only for individual high-risk facilities

[1] Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

[2] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014).

[3] GAO, *Critical Infrastructure Protection: DHS Should Take Actions to Measure Reduction in Chemical Facility Vulnerability and Share Information with First Responders*, GAO-18-538 (Washington, D.C.: Aug. 8, 2018).

but for the Chemical Facility Anti-Terrorism Standards program as a whole.

We also determined that, although DHS shares some Chemical Facility Anti-Terrorism Standards program information, first responders and emergency planners may not have all of the information they need to minimize the risk of injury or death when responding to incidents at high-risk facilities. This was due to first responders at the local level not having access or widely using a secure interface that DHS developed (known as the Infrastructure Protection Gateway) to obtain information about high-risk facilities and the specific chemicals they process.

To address the weaknesses we identified, we recommended that DHS take actions to (1) measure reduction in vulnerability of high-risk facilities and use that data to assess program performance, and (2) encourage access to and wider use of the Infrastructure Protection Gateway among first responders and emergency planners. DHS concurred with both recommendations and outlined efforts underway or planned to address them.

- **The federal government had identified major challenges to the adoption of the cybersecurity framework.** In February 2018, we reported that there were four different challenges to adopting the cybersecurity framework, including limited resources and competing priorities, reported by entities within their sectors.[4] We further reported that none of the 16 sector-specific agencies[5] were measuring the implementation by these entities, nor did they have qualitative or quantitative measures of framework adoption. While research had been done to determine the use of the framework in the sectors, these efforts had yielded no real results for sector wide adoption. We concluded that, until sector-specific agencies understand the use of the framework by the implementing entities, their ability to understand

[4] GAO, *Critical Infrastructure Protection: Additional Actions are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211 (Washington, D.C.: Feb. 15, 2018).

[5] Sector-specific agencies are federal departments or agencies with responsibility for providing institutional knowledge and specialized expertise. They accomplish this by leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the environment.

implementation efforts would be limited.[6] Accordingly, we made a total of nine recommendations to nine sector-specific agencies to address these issues. Five agencies agreed with the recommendations, while four others neither agreed nor disagreed; as of August 2018, all five recommendations had not been implemented.

- **Agencies had not addressed risks to their systems and the information they maintain.** In January 2018, we reported that the Department of Defense (DOD) and Federal Aviation Administration (FAA) identified a variety of operations and physical security risks related to Automatic Dependent Surveillance-Broadcast Out technology that could adversely affect DOD missions.[7] These risks came from information broadcast by the system itself,[8] as well as from potential vulnerabilities to electronic warfare- and cyber-attacks, and from the potential divestment of secondary-surveillance radars.[9] However, DOD and FAA had not approved any solutions to address the risks they identified to the system. Accordingly, we recommended that DOD and FAA, among other things, take action to approve one or more solutions to address Automatic Dependent Surveillance-Broadcast Out-related security risks. DOD and FAA generally agreed with our recommendations; however, as of August 2018, they had not been implemented.
- **Major challenges existed to securing the electricity grid against cyber threats.** In October 2015, we testified on the status of the electricity grid's cybersecurity, reporting that entities associated with the grid have encountered several challenges.[10] We noted that these

[6] The previous report, GAO-16-152, highlighted actions taken by agencies to develop and promote the framework. However, we identified deficiencies in agencies' ability to measure progress of their programs for promoting the adoption of the framework.

[7] GAO, *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft,* GAO-18-177 (Washington, D.C.: Jan. 18, 2018).

[8] In 2010, the FAA issued a final rule that requires all aircraft, including military aircraft, flying in specified airspace within the national airspace system as of January 1, 2020, to be equipped with technology that would transmit flight information to an enabled receiver. See 14 C.F.R §§ 91.225 and 91.227.

[9] DOD defines an electronic attack as a division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.

[10] GAO, *Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention*, GAO-16-174T (Washington, D.C.: Oct. 21, 2015).

challenges included implementation monitoring, built-in security features in smart grid systems, and establishing metrics for cybersecurity. We concluded that continued attention to these issues and cyber threats in general was required to help mitigate these risks to the electricity grid.

- **DHS and other agencies needed to enhance cybersecurity in the maritime environment.** In October 2015, we testified on the status of the cybersecurity of our nation's ports, concluding that steps needed to be taken to enhance their security.[11] Specifically, we noted that DHS needed to include cyber risks in its risk assessments that are already in place as well as addressing cyber risks in guidance for port security plans. We concluded that, until DHS and the other stakeholders take steps to address cybersecurity in the ports, risk of a cyber-attack with serious consequences are increased.
- **Sector-specific agencies were not properly addressing progress or metrics to measure their progress in cybersecurity.** In November 2015, we reported that sector-specific agencies were not comprehensively addressing the cyber risk to the infrastructure, as 11 of the 15 sectors had significant cyber risk.[12] Specifically, we noted that these entities had taken actions to mitigate their cyber risk; however, most had not identified incentives to promote cybersecurity in their sectors. We concluded that while the sector-specific agencies have successfully disseminated the information they possess, there was still work to be done to properly measure cybersecurity implementation progress. Accordingly, we made seven recommendations to six agencies to address these issues. Four of these agencies agreed with our recommendation, while two agencies did not comment on the recommendations. As of August 2018, all seven recommendations had not been implemented.

[11] GAO, *Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity*, GAO-16-116T (Washington, D.C.: Oct. 8, 2015).

[12] GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015). The government facilities sector was excluded from the scope of this review due to its uniquely governmental focus.

Appendix X: Action 9—Improve Federal Efforts to Protect Privacy and Sensitive Data

Advancements in technology, such as new search technology and data analytics software for searching and collecting information, have made it easier for individuals and organizations to correlate data and track it across large and numerous databases. In addition, lower data storage costs have made it less expensive to store vast amounts of data. Also, ubiquitous Internet and cellular connectivity make it easier to track individuals by allowing easy access to information pinpointing their locations.

Certain agencies, such as the Department of Education's Office of Federal Student Aid and the Department of Health and Human Services' (HHS) Centers for Medicare and Medicaid Services (CMS), hold millions of sensitive records for people all over the country. The focus on personally identifiable information (PII) is to protect this information as much as feasibly possible using federal standards and procedures to mitigate the risk that is always present with this type of information. We have issued several reports noting that agencies can take steps to improve their protection of privacy and sensitive data. For example:

- **CMS and external entities were at risk of compromising Medicare Beneficiary Data due to a lack of guidance and proper oversight.** In March 2018, we reported that CMS shares Medicare beneficiary data with three external entities—Medicare Administrative Contractors, researchers, and other qualified public and private entities.[1] However, we identified weakness in their oversight of these entities. Specifically, we found that researchers were not given guidance for how to implement proper security controls nor was there a program to oversee security implementation for these researchers or for qualified entities. As such, we made three recommendations to CMS to improve its oversight of the external entities it works with. The agency agreed with our recommendations, but had not implemented them as of August 2018.
- **The Department of Education's Office of Federal Student Aid did not properly oversee its school partners' records or information security programs.** In December 2017, we reported that the agency had established policies and procedures for managing and protecting the student information, but there were shortcomings that hindered

[1] GAO, *Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement*, GAO-18-210 (Washington, D.C.: March 6, 2018).

the effectiveness of these procedures.[2] Based on a survey of the schools, the majority of the schools had policies in place for records retention but the way these policies were implemented was highly varied for paper and electronic records. We also found that the oversight of the school's programs was lacking, as Federal Student Aid conducts reviews but does not consider information security as a factor for selecting schools.

Accordingly, we made seven recommendations to the Department of Education. The department agreed with five of the recommendations, partially agreed with one, and did not agree with one recommendation. However, we continued to believe that all the recommendations were warranted. As of August 2018, all of our recommendations had not been implemented.

- **HHS had not fully addressed key security elements in its guidance for protecting the security and privacy of electronic health information.** In August 2016, we reported that HHS's guidance for securing electronic health information issued by the department did not address all key controls called for by other federal cybersecurity guidance.[3] In addition, the department's oversight efforts did not always offer pertinent technical guidance and did not always follow up on corrective actions when investigative cases were closed. HHS generally concurred with the five recommendations we made to address these issues; however, as of August 2018, the five recommendations had not been implemented.
- **CMS had not fully protected the privacy of users' data on state-based marketplaces**. In March 2016, we reported on weaknesses in technical controls for the "data hub" that CMS uses to exchange information between its health insurance marketplace and external partners.[4] We also identified significant weaknesses in the controls in place at three selected state-based marketplaces established to carry

[2] GAO, *Federal Student Aid: Better Program Management and Oversight of Postsecondary Schools Needed to Protect Student Information,* GAO-18-121 (Washington, D.C.: Dec. 15, 2017).

[3] GAO, *Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight*, GAO-16-771 (Washington, D.C.: Sept. 26, 2016).

[4] GAO, *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls,* GAO-16-265 (Washington, D.C.: Mar. 23, 2016).

out provisions of the Patient Protection and Affordable Care Act.[5] We made three recommendations to CMS related to defining procedures for overseeing the security of state-based marketplaces and requiring continuous monitoring of state marketplace controls. HHS concurred with our recommendations. As of August 2018, two of the recommendations had not yet been implemented.

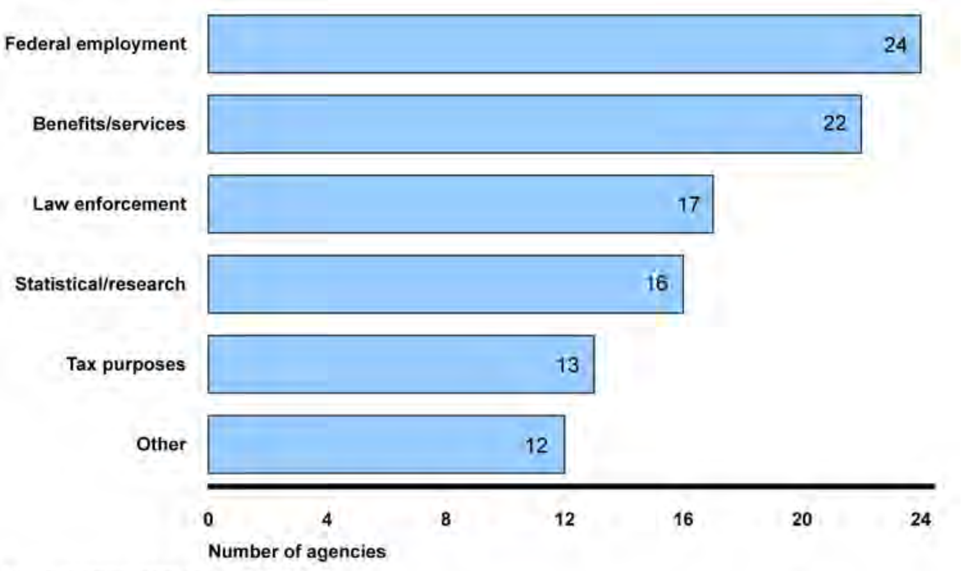
- **Poor planning and ineffective monitoring had resulted in the unsuccessful implementation of government initiatives designed to protect federal data**. In July 2017, we reported that government initiatives aimed at eliminating the unnecessary collection, use, and display of Social Security numbers (SSN) have had limited success.[6] Specifically, in agencies' response to our questionnaire on SSN reduction efforts, the 24 agencies covered by the Chief Financial Officers Act[7] reported successfully curtailing the collection, use, and display of SSNs. Nevertheless, all of the agencies continued to rely on SSNs for important government programs and systems, as seen in figure 10.

[5] Pub. L. No. 111-148, 124 Stat. 119 (Mar. 23, 2010), as amended by the *Health Care and Education Reconciliation Act of 2010*, Pub. L. No. 111-152,124 Stat.1029 (Mar. 30, 2010).

[6] GAO, *Social Security Numbers: OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risks by Reducing Collection, Use, and Display,* GAO-17-553 (Washington, D.C.: July 25, 2017).

[7] There are 24 agencies identified in the Chief Financial Officers Act: 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.

Figure 10: Agency Reported Use of Social Security Numbers



Source: Agency-reported data. | GAO-18-622

We also determined that poor planning by agencies and ineffective monitoring by the Office of Management and Budget (OMB) had also limited efforts to reduce SSN use. For example, lacking direction from OMB, many agencies' SSN reduction plans did not include key elements, such as time frames and performance indicators, calling into question their utility. Moreover, OMB had not required agencies to maintain up-to-date inventories of their SSN holdings or provided criteria for determining "unnecessary use and display," limiting agencies' ability to gauge progress. Finally, OMB had not ensured that agencies update their progress in annual reports or established performance metrics to monitor agency efforts. Accordingly, we made five recommendations to the Director of OMB to address these issues. As of August 2018, all five recommendations had not been implemented.

Appendix XI: Action 10—Appropriately Limit the Collection and Use of Personal Information and Ensure That It Is Obtained with Appropriate Knowledge or Consent

Given that access to data is so pervasive, personal privacy hinges on ensuring that databases of personally identifiable information (PII) maintained by government agencies or on their behalf are protected both from inappropriate access (i.e., data breaches) as well as inappropriate use (i.e., for purposes not originally specified when the information was collected). Likewise, the trend in the private sector of collecting extensive and detailed information about individuals needs appropriate limits. The vast number of individuals potentially affected by data breaches at federal agencies and private sector entities in recent years increases concerns that PII is not being properly protected.

- **The emergence of IoT devices can facilitate the collection of information about individuals without their knowledge or consent.**[1] In May 2017, we reported that the IoT has become increasingly used to communicate and process vast amounts of information using "smart" devices (such as a fitness tracker connected to a smartphone). However, we noted that this emerging technology also presents new issues in areas such as information security, privacy, and safety.
- **Smartphone tracking apps can present serious safety and privacy risks.** In April 2016, we reported on smartphone applications that facilitated the surreptitious tracking of a smartphone's location and other data.[2] Specifically, we noted that some applications could be used to intercept communications and text messages, essentially facilitating the stalking of others. While it is illegal to use these applications for these purposes, stakeholders differed over whether current federal laws needed to be strengthened to combat stalking. We also noted that stakeholders expressed concerns over what they perceived to be limited enforcement of laws related to tracking apps and stalking. In particular, domestic violence groups stated that additional education of law enforcement officials and consumers about how to protect against, detect, and remove tracking apps is needed.

[1] GAO-17-75.

[2] GAO, *Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps That Can Facilitate Stalking*, GAO-16-317 (Washington, D.C.: May 9, 2016).

- **The Federal Bureau of Investigation (FBI) has not ensured privacy and accuracy related to the use of face recognition technology.** In May 2016, we reported[3] that the Department of Justice had not been timely in publishing and updating privacy documentation for the FBI's use of face recognition technology.[4] Publishing such documents in a timely manner would better assure the public that the FBI is evaluating risks to privacy when implementing systems. Also, the FBI had taken limited steps to determine whether the face recognition system it was using was sufficiently accurate. We recommended that the department ensure required privacy-related documents are published and that the FBI test and review face recognition systems to ensure that they are sufficiently accurate. Of the six recommendations we made, the Department of Justice agreed with one, partially agreed with two, and disagreed with three. We continued to believe all the recommendations made were valid. As of August 2018, the six recommendations had not been implemented.

[3] GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016).

[4] Face recognition technology uses biometrics—the automated recognition of individuals based on their biological and behavioral characteristics—to identify the identity of individuals based on a comparison of a photograph of an unknown person against a database of photographs of known persons. Specifically, the technology extracts features from the faces and puts them into a format—often referred to as a faceprint—that can be used for verification, among other things. Once the faceprint has been created, the technology can use a face recognition algorithm to compare the faceprints against each other to produce a single score value that represents the degree of similarity between the two faces.

Appendix XII: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nick Marinos, (202) 512-9342 or marinosn@gao.gov
Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Jon Ticehurst, Assistant Director; Kush K. Malhotra, Analyst-In-Charge; Chris Businsky; Alan Daigle; Rebecca Eyler; Chaz Hubbard; David Plocher; Bradley Roach; Sukhjoot Singh; Di'Mond Spencer; and Umesh Thakkar made key contributions to this report.

(102624)

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

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

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

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

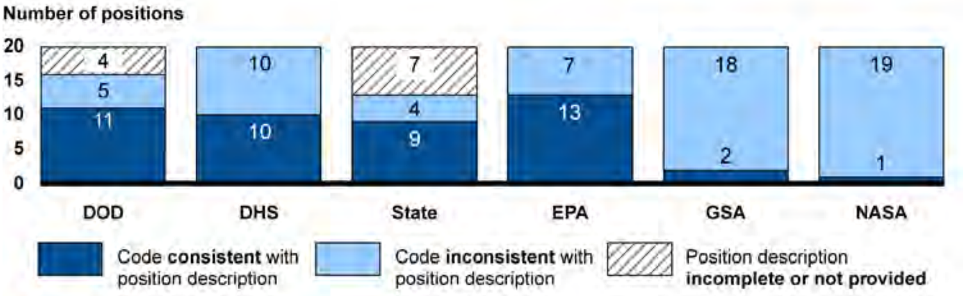
GAO is making 28 recommendations to 22 agencies to review and assign the appropriate codes to their IT, cybersecurity, and cyber-related positions. Of the 22 agencies to which GAO made recommendations, 20 agreed with the recommendations, one partially agreed, and one did not agree with one of two recommendations.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

Tables

Figures

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

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, 201*6, 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

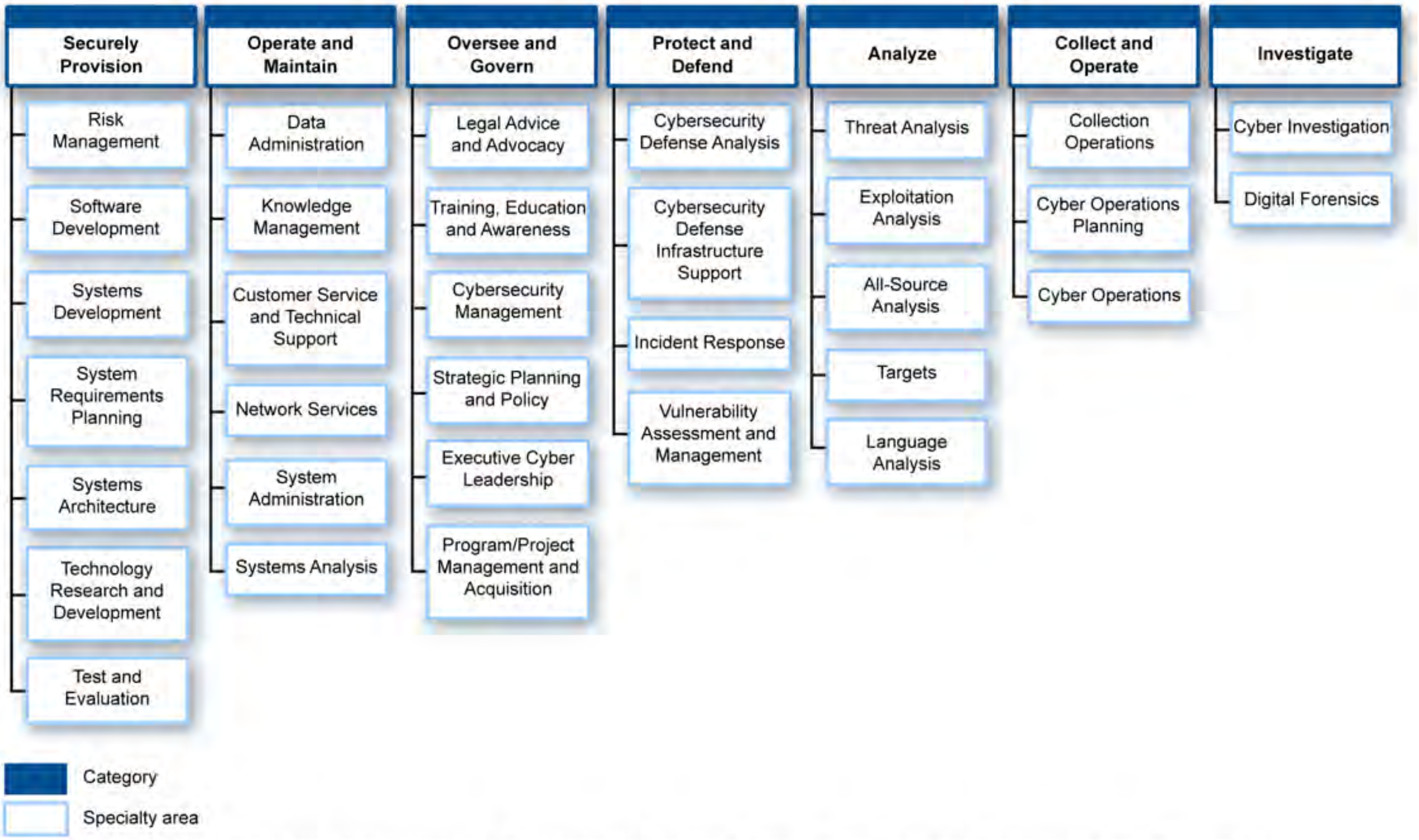
NIST coordinates the National Initiative for Cybersecurity Education (NICE) partnership among government, academia, and the private sector. The initiative's goal is to improve cybersecurity education, awareness, training, and workforce development in an effort to increase the number of skilled cybersecurity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

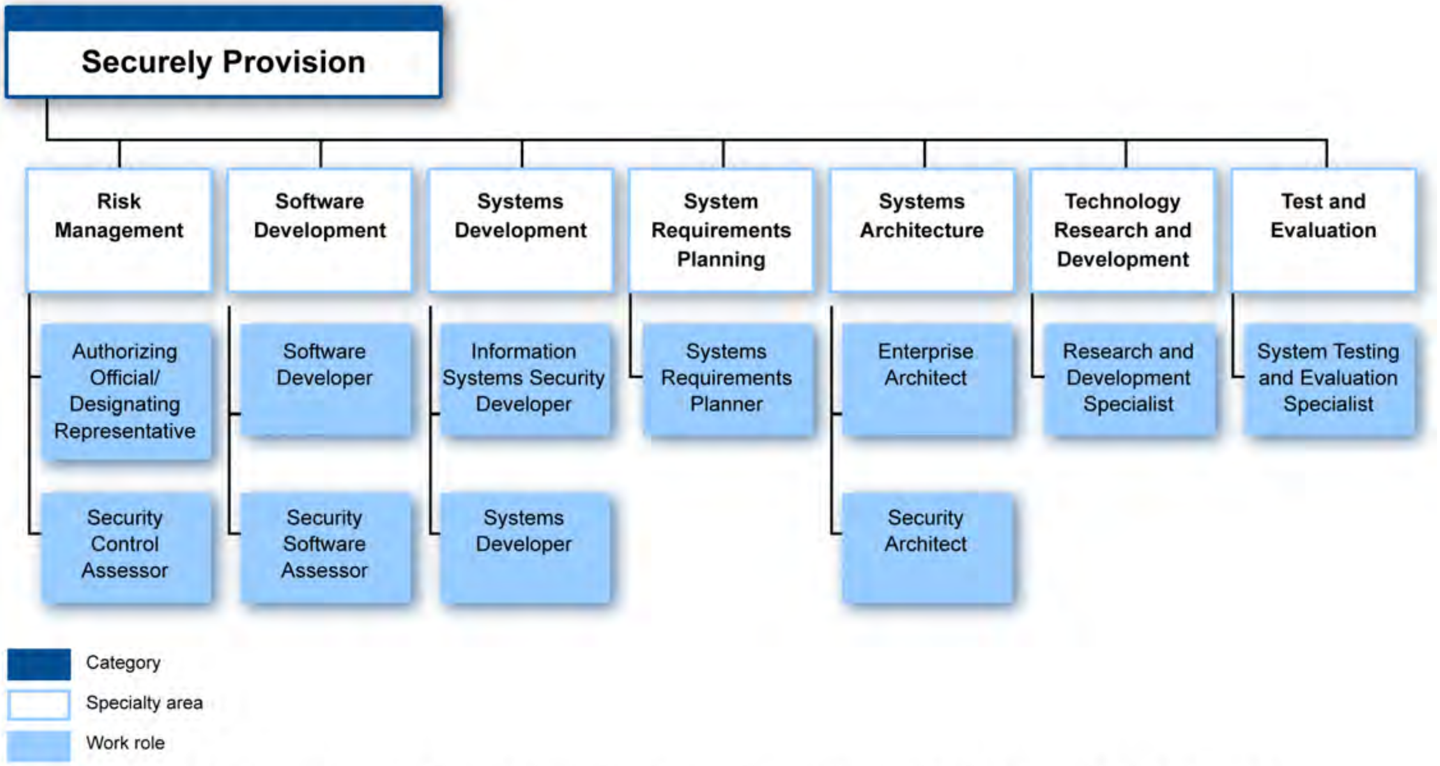


Source: GAO analysis of National Institute of Standards and Technology, *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*, SP-800-181. | GAO-19-144

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
Software Development
Systems Development
System Requirements Planning
Systems Architecture
Technology Research and Development
Test and Evaluation
Authorizing Official/ Designating Representative
Security Control Assessor
Software Developer
Security Software Assessor
Information Systems Security Developer
Systems Developer
Systems Requirements Planner
Enterprise Architect
Security Architect
Research and Development Specialist
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

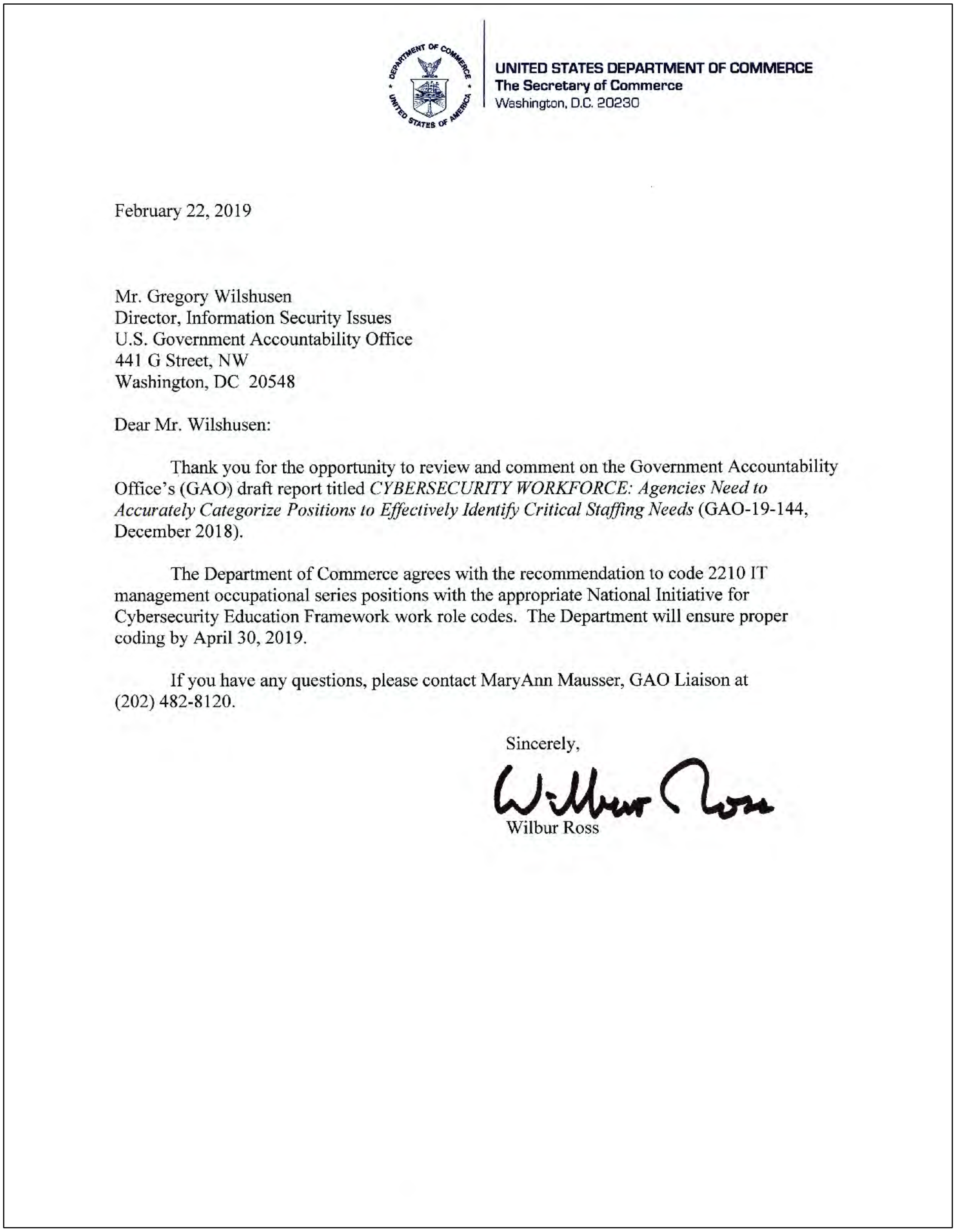
Table 9: Top 12 Preliminary Work Roles of Critical Need Reported by the 24 CFO Act Agencies as of November 2018

	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.

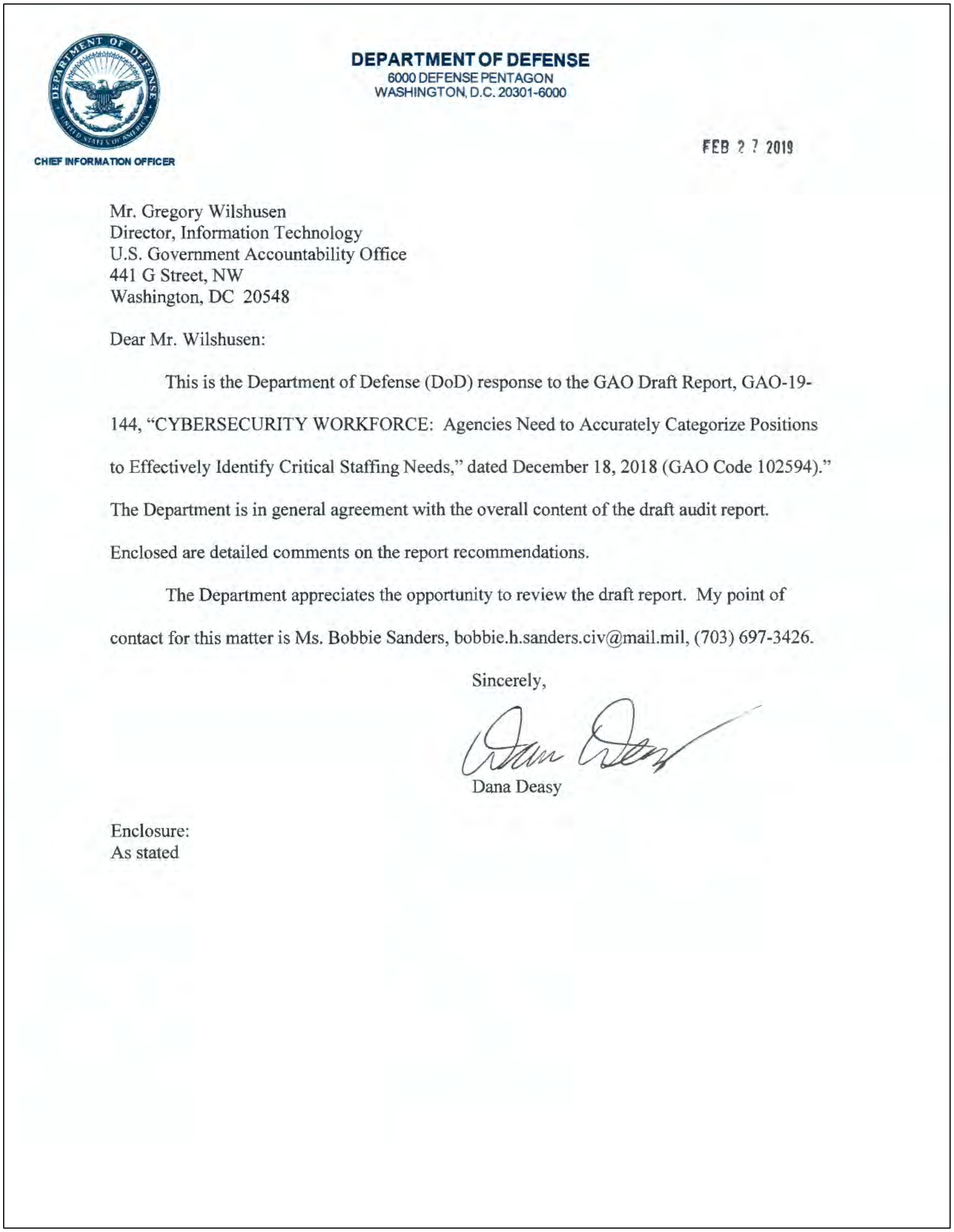
If you have any questions, please contact MaryAnn Mausser, GAO Liaison at (202) 482-8120.

Sincerely,

Wilbur Ross

Wilbur Ross

Appendix VI: Comments from the Department of Defense



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

CHIEF INFORMATION OFFICER

FEB 2 7 2019

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

Dear Mr. Wilshusen:

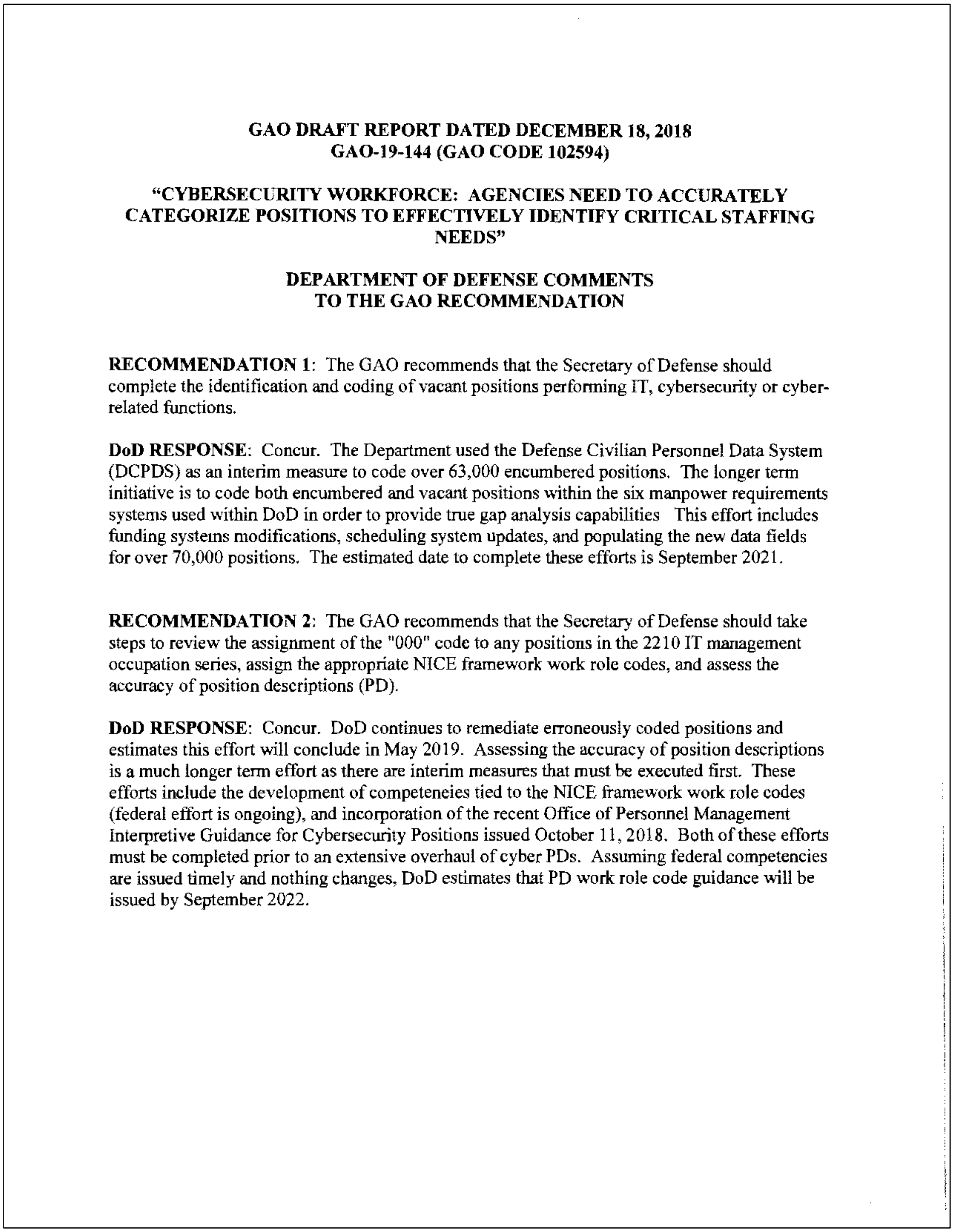
This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-19-144, "CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs," dated December 18, 2018 (GAO Code 102594)." The Department is in general agreement with the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

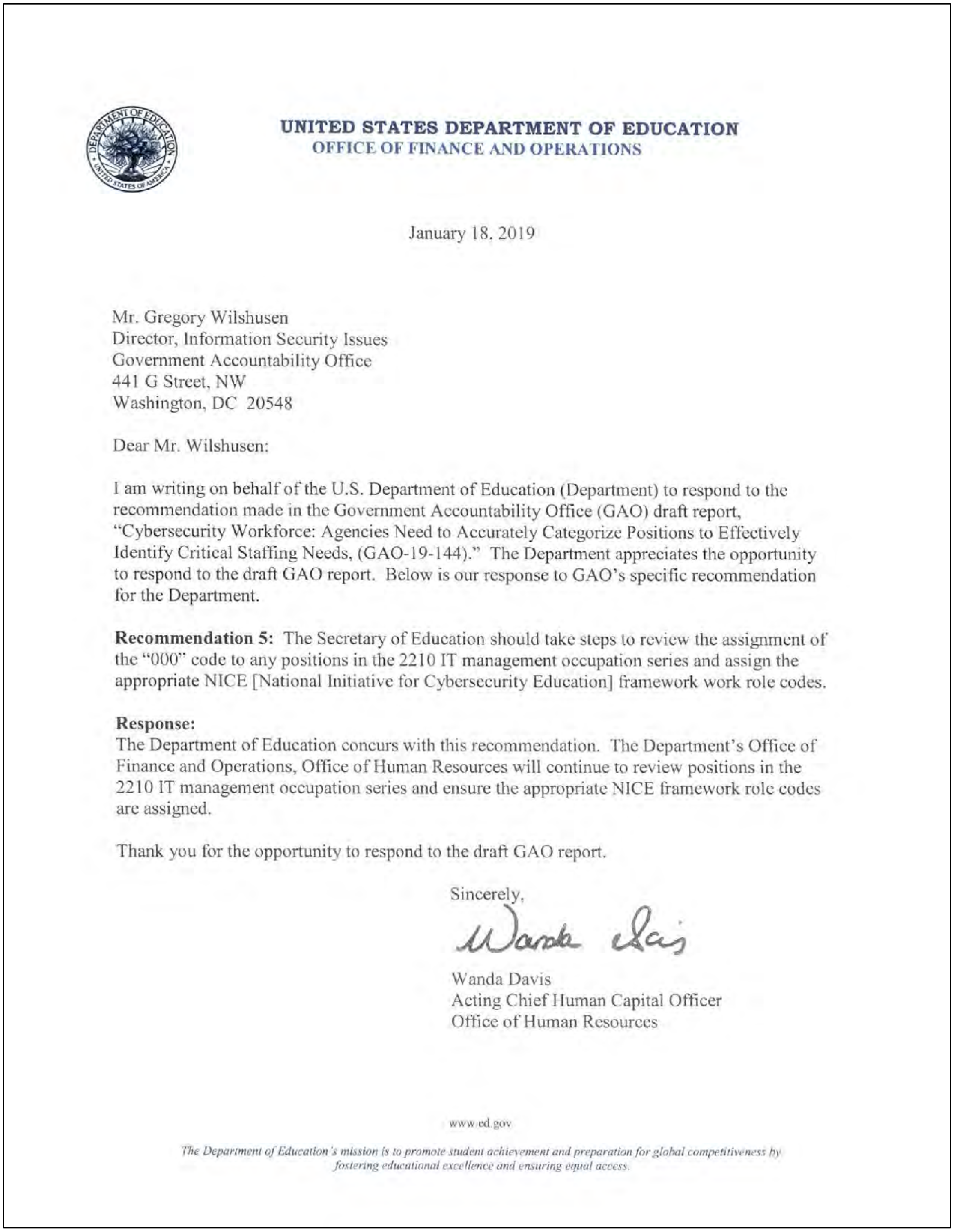
RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should complete the identification and coding of vacant positions performing IT, cybersecurity or cyber-related functions.

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,

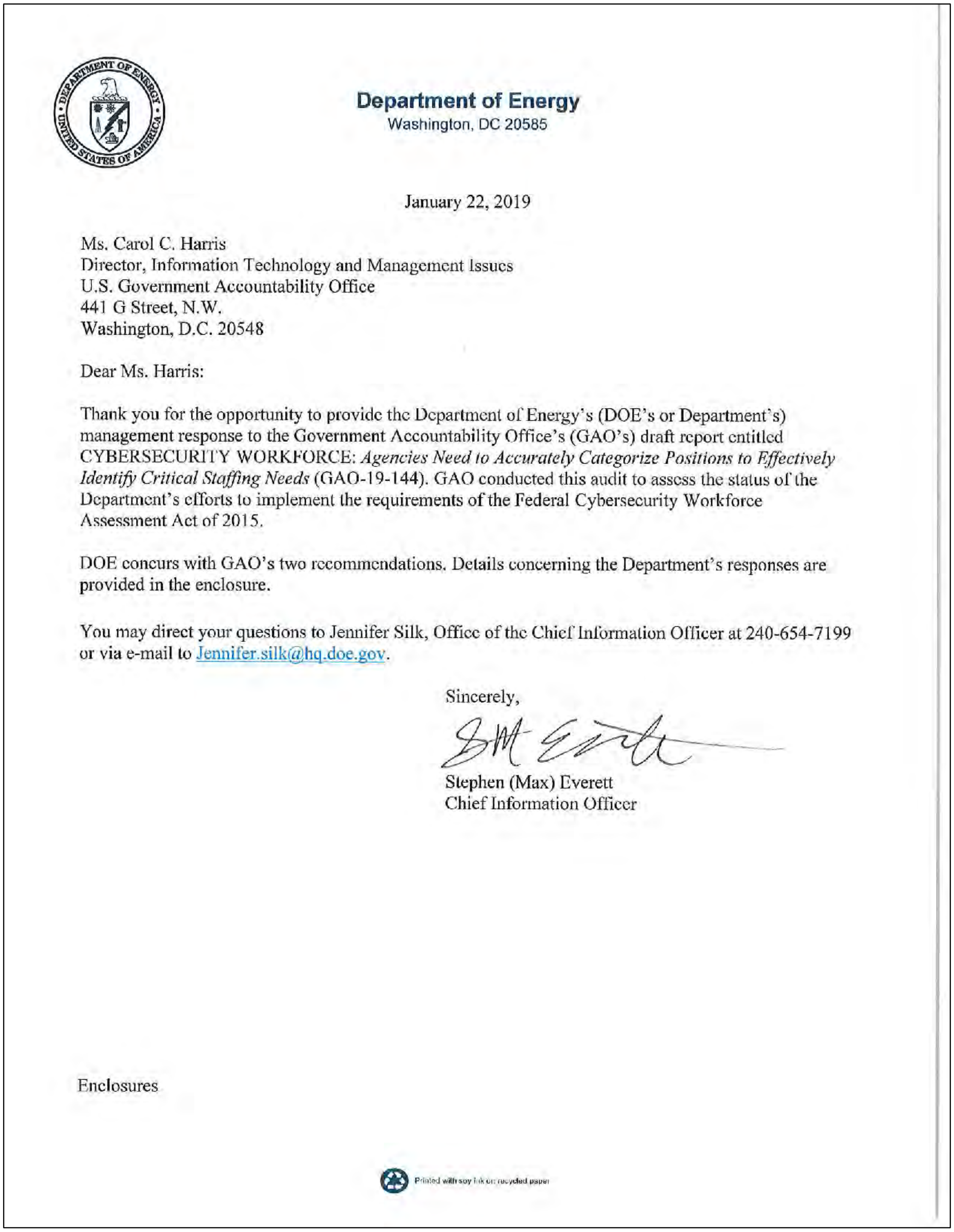
Wanda Davis

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.

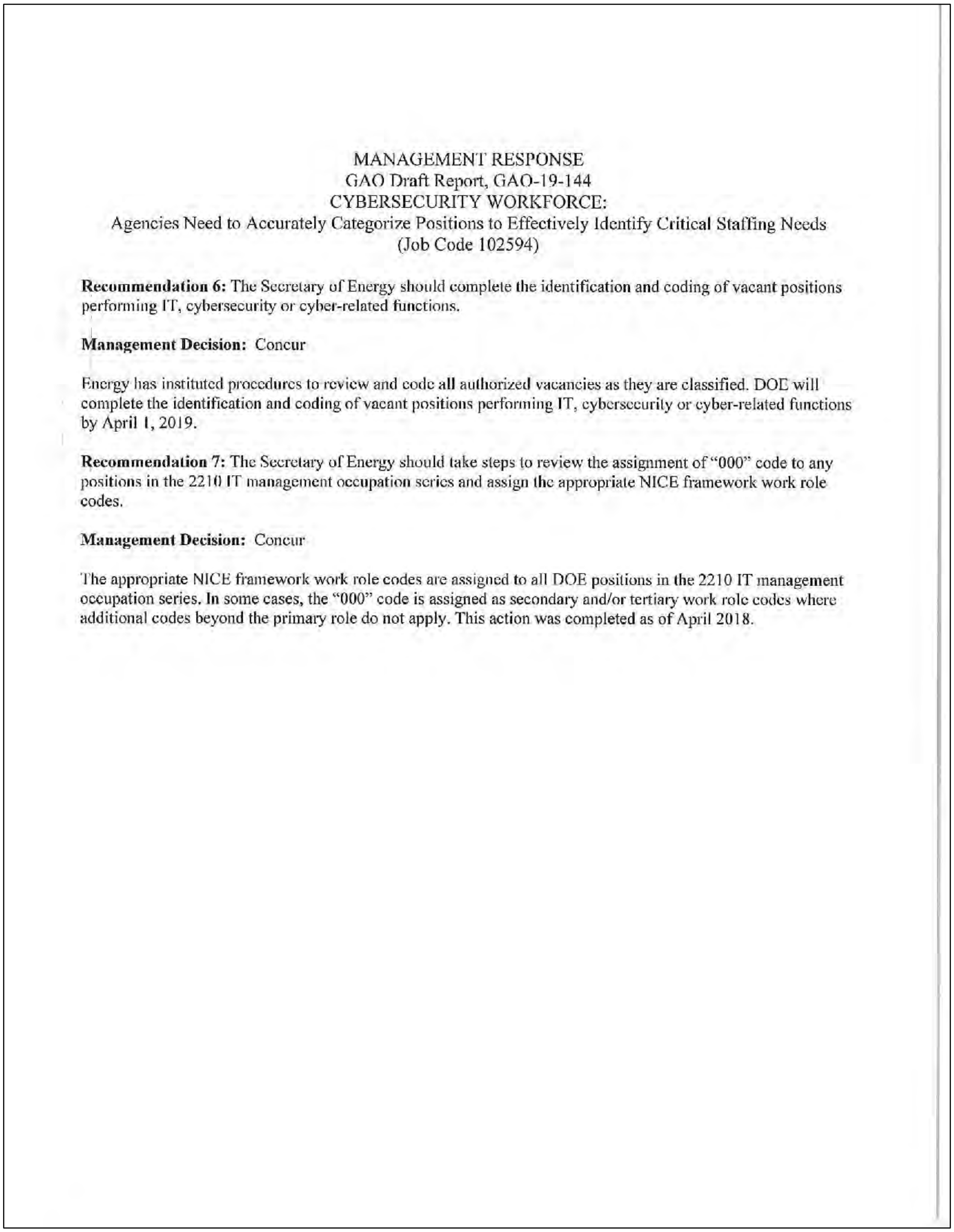
You may direct your questions to Jennifer Silk, Office of the Chief Information Officer at 240-654-7199 or via e-mail to Jennifer.silk@hq.doe.gov.

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

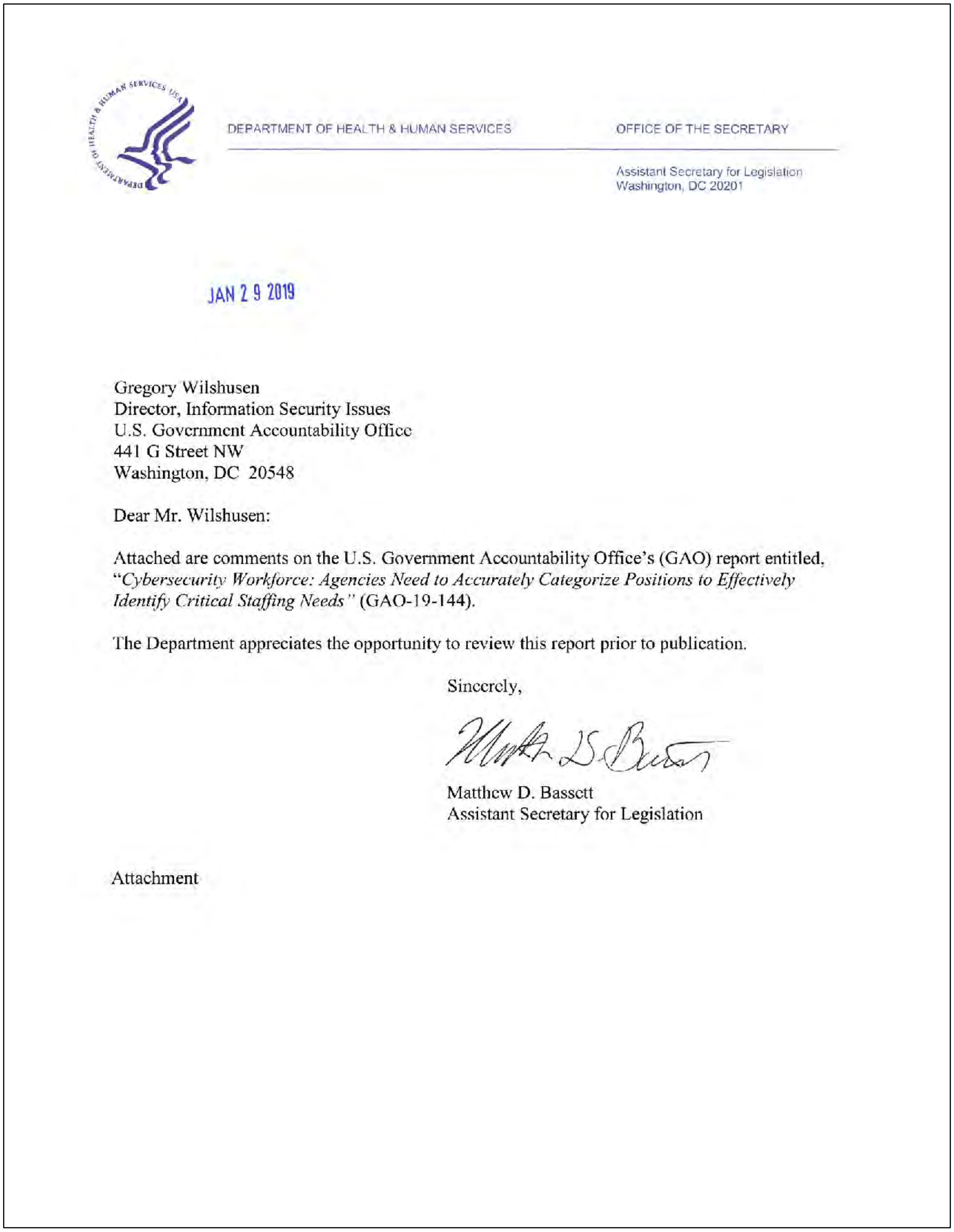
Energy has instituted procedures to review and code all authorized vacancies as they are classified. DOE will complete the identification and coding of vacant positions performing IT, cybersecurity or cyber-related functions by April 1, 2019.

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:

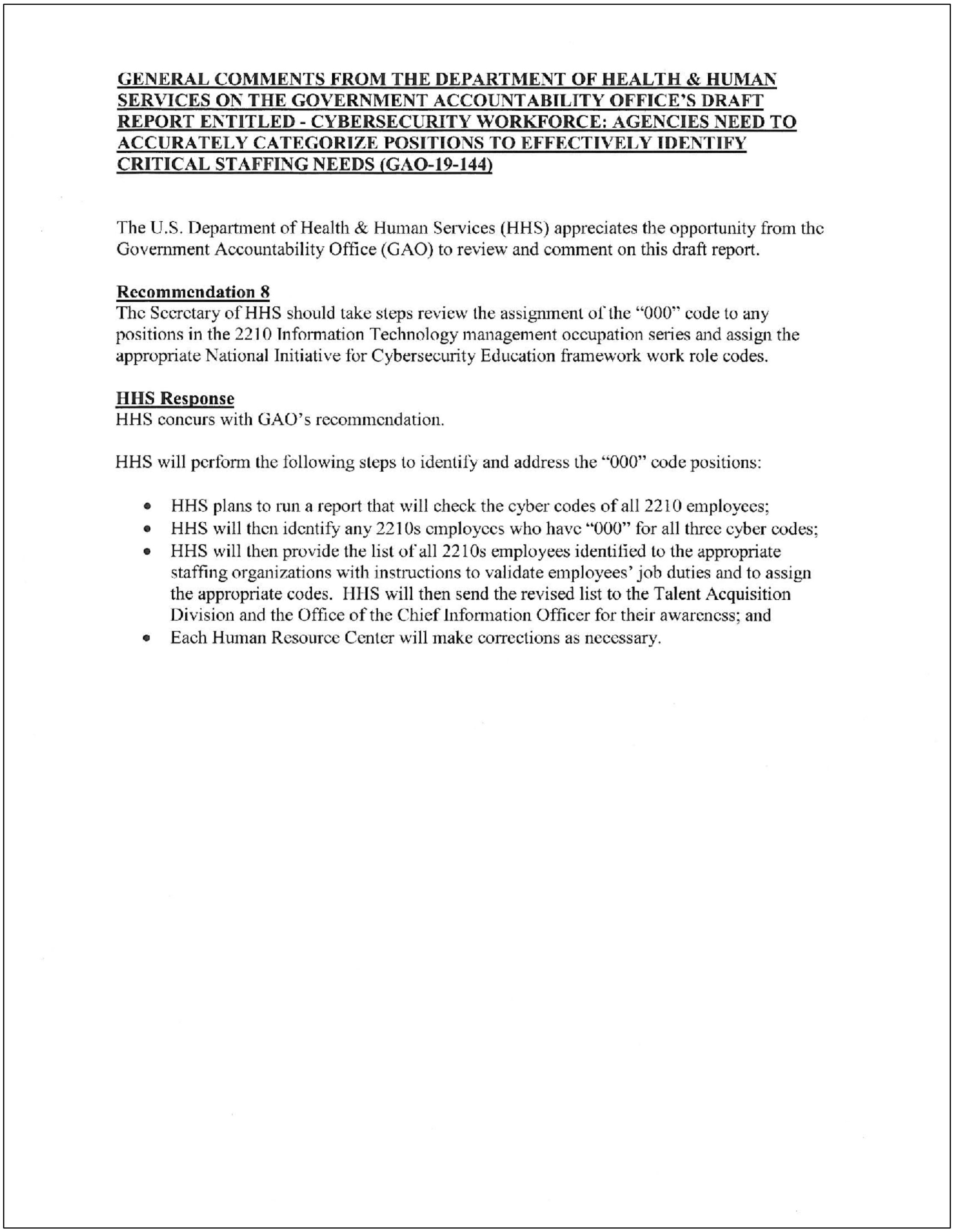
Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*" (GAO-19-144).

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.

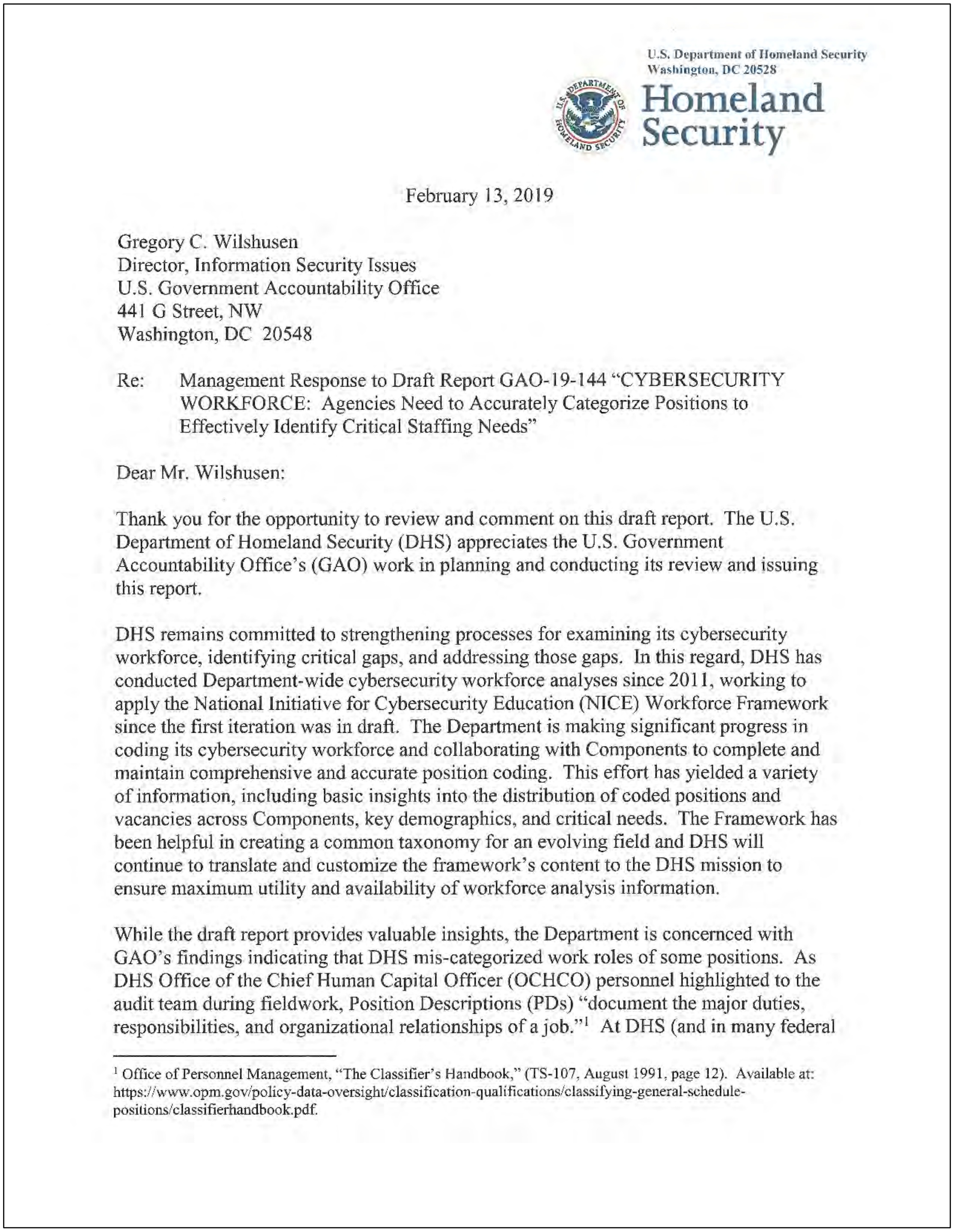
Recommendation 8
The Secretary of HHS should take steps review the assignment of the "000" code to any positions in the 2210 Information Technology management occupation series and assign the appropriate National Initiative for Cybersecurity Education framework work role codes.

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"

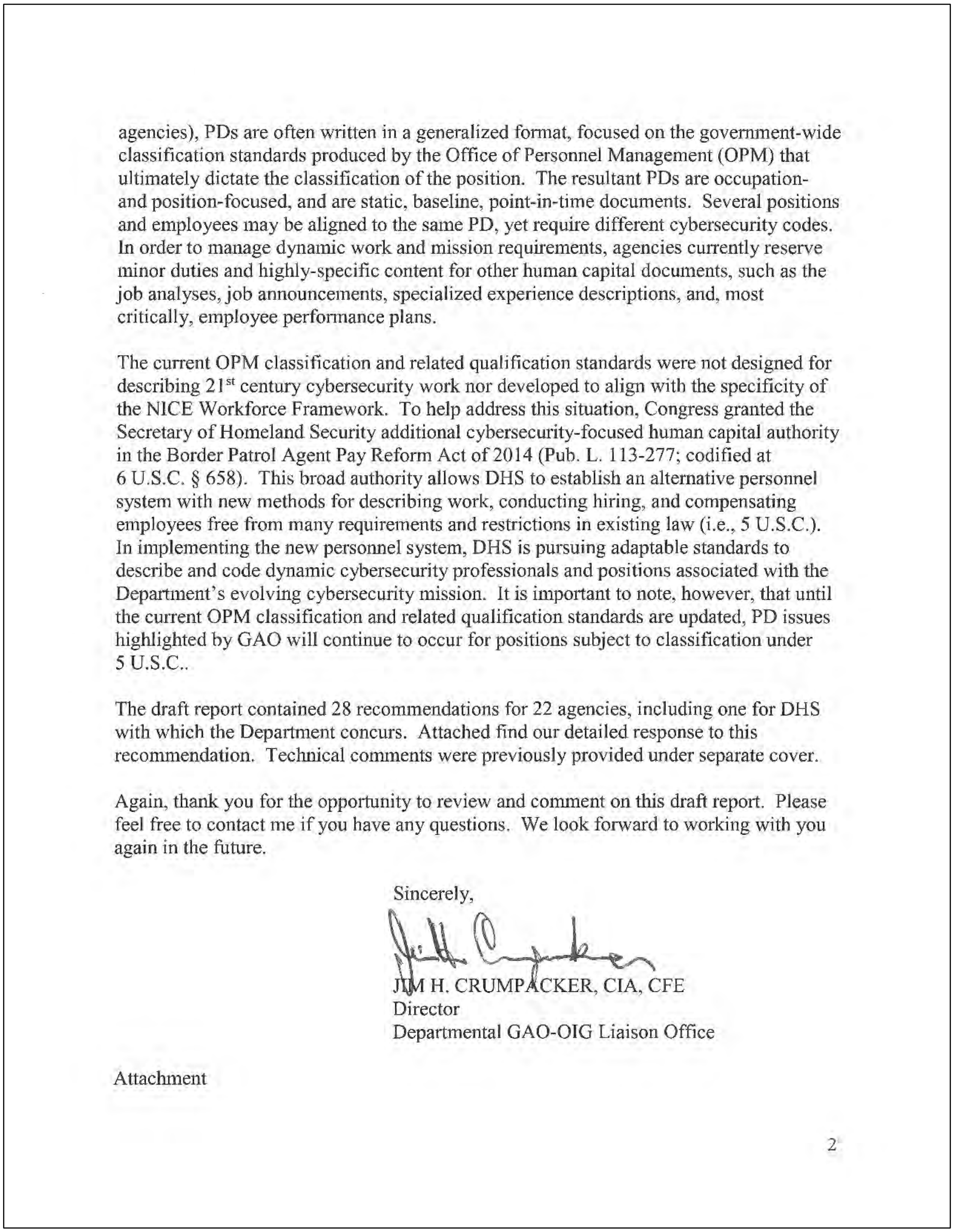
Dear Mr. Wilshusen:

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.

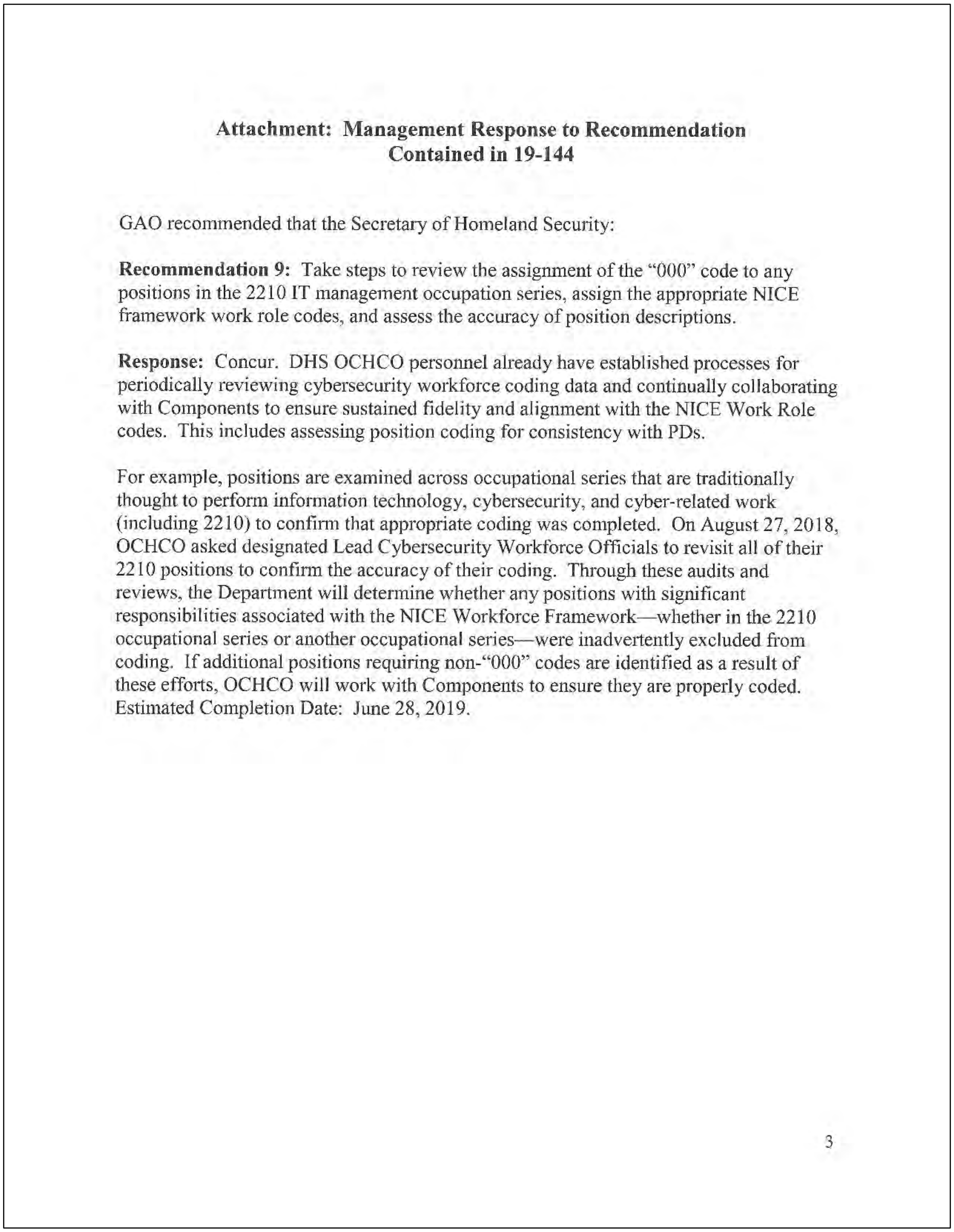
Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

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

Attachment

2



Attachment: Management Response to Recommendation Contained in 19-144

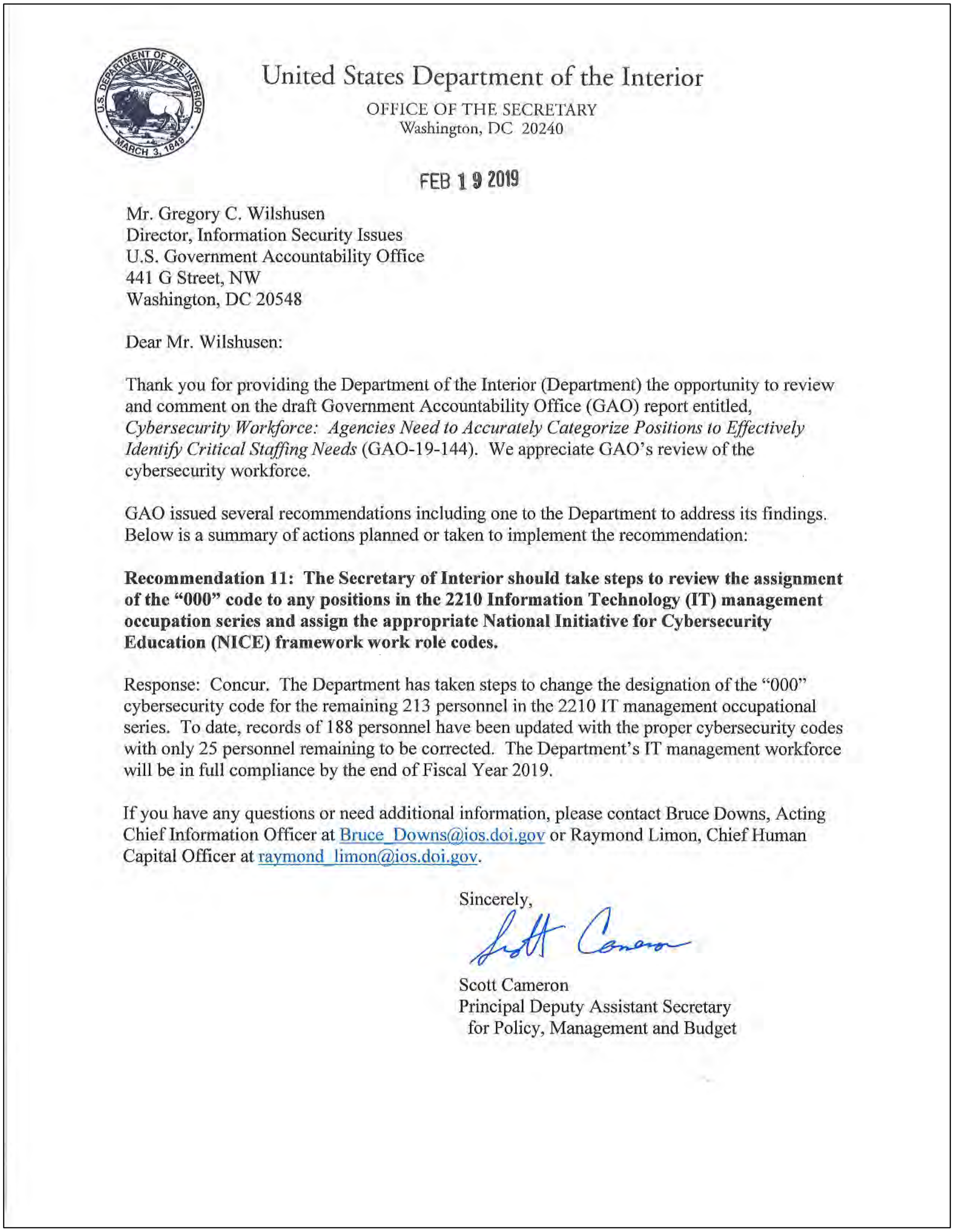
GAO recommended that the Secretary of Homeland Security:

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.

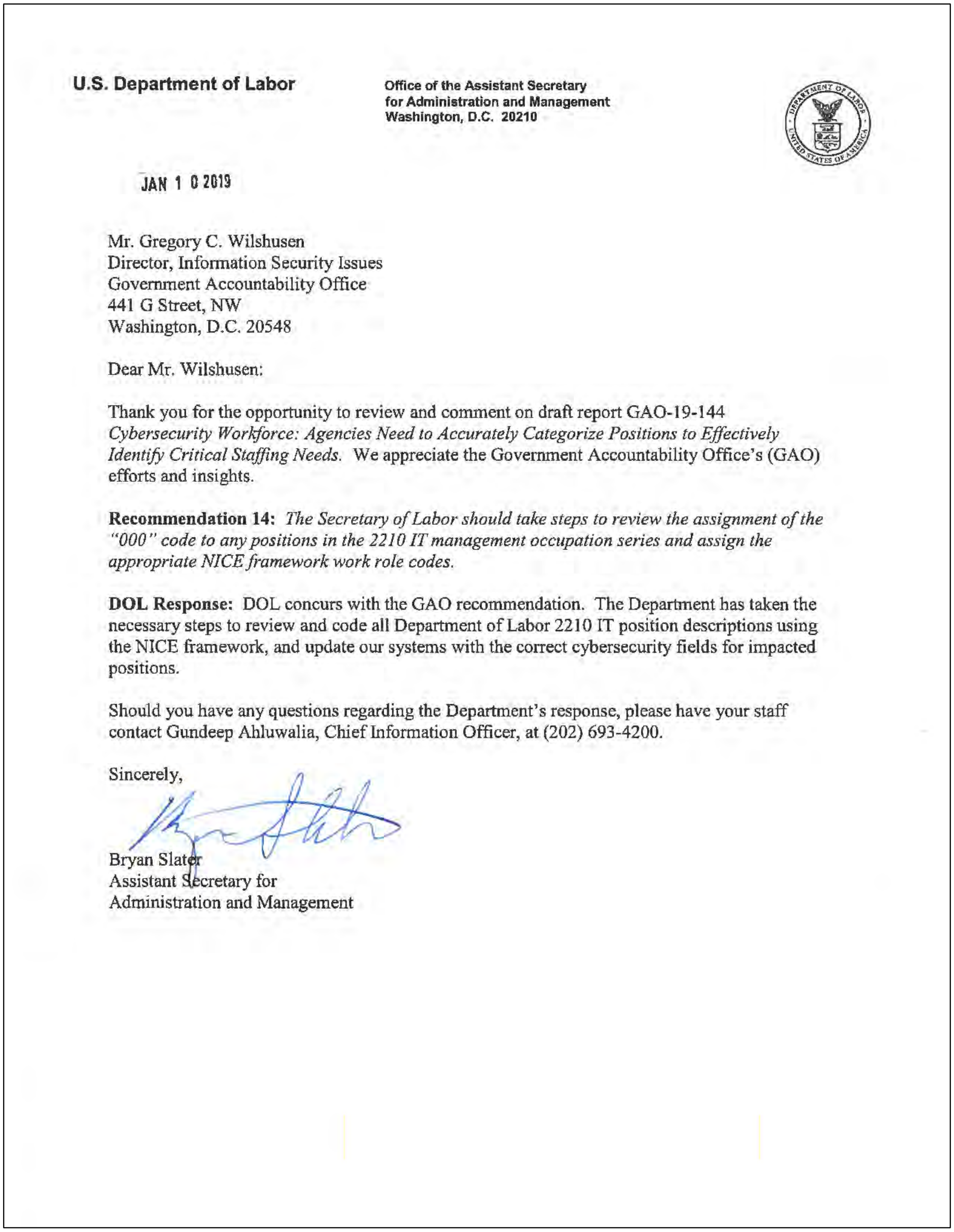
If you have any questions or need additional information, please contact Bruce Downs, Acting Chief Information Officer at Bruce_Downs@ios.doi.gov or Raymond Limon, Chief Human Capital Officer at raymond_limon@ios.doi.gov.

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.*

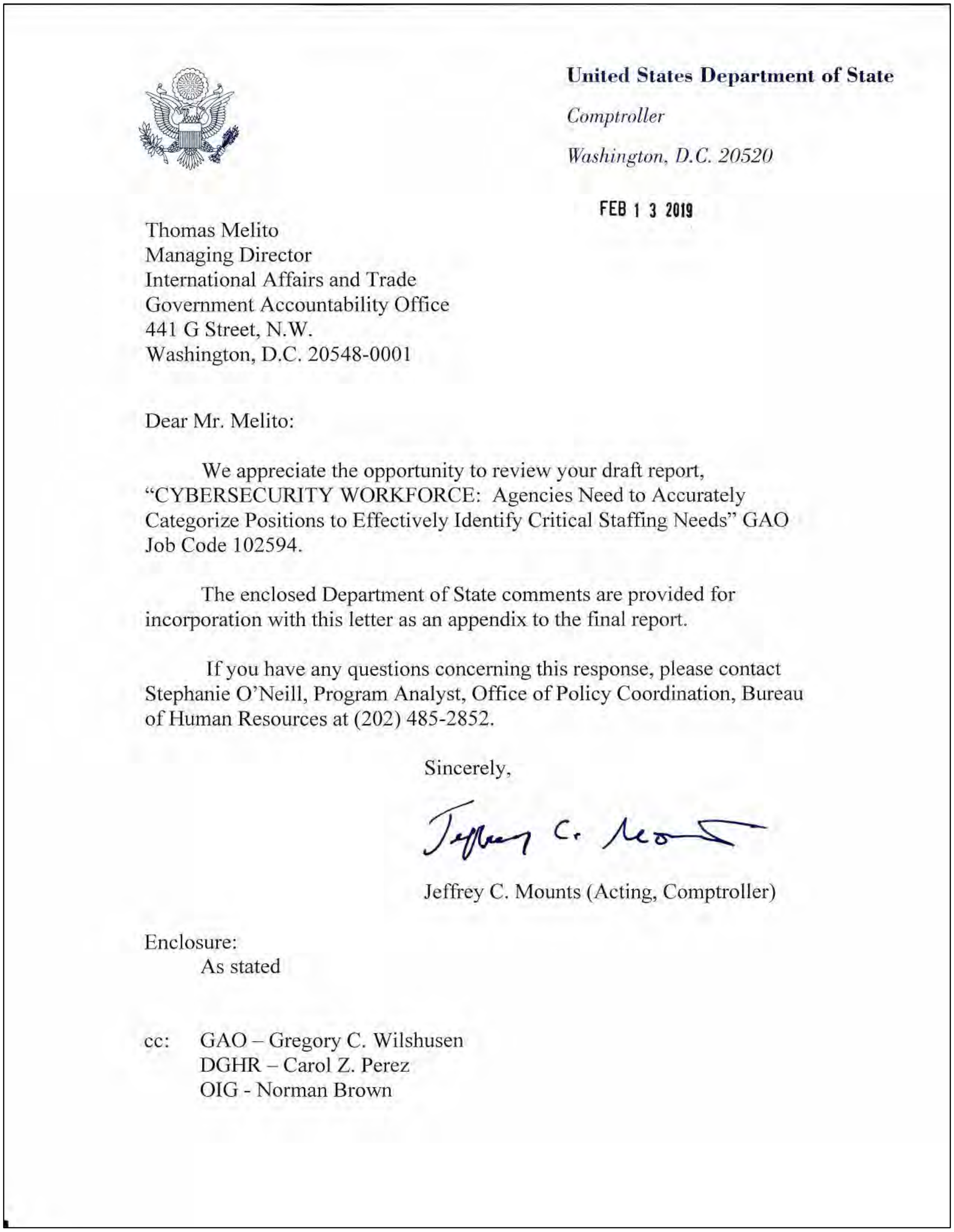
DOL Response: DOL concurs with the GAO recommendation. The Department has taken the necessary steps to review and code all Department of Labor 2210 IT position descriptions using the NICE framework, and update our systems with the correct cybersecurity fields for impacted positions.

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.

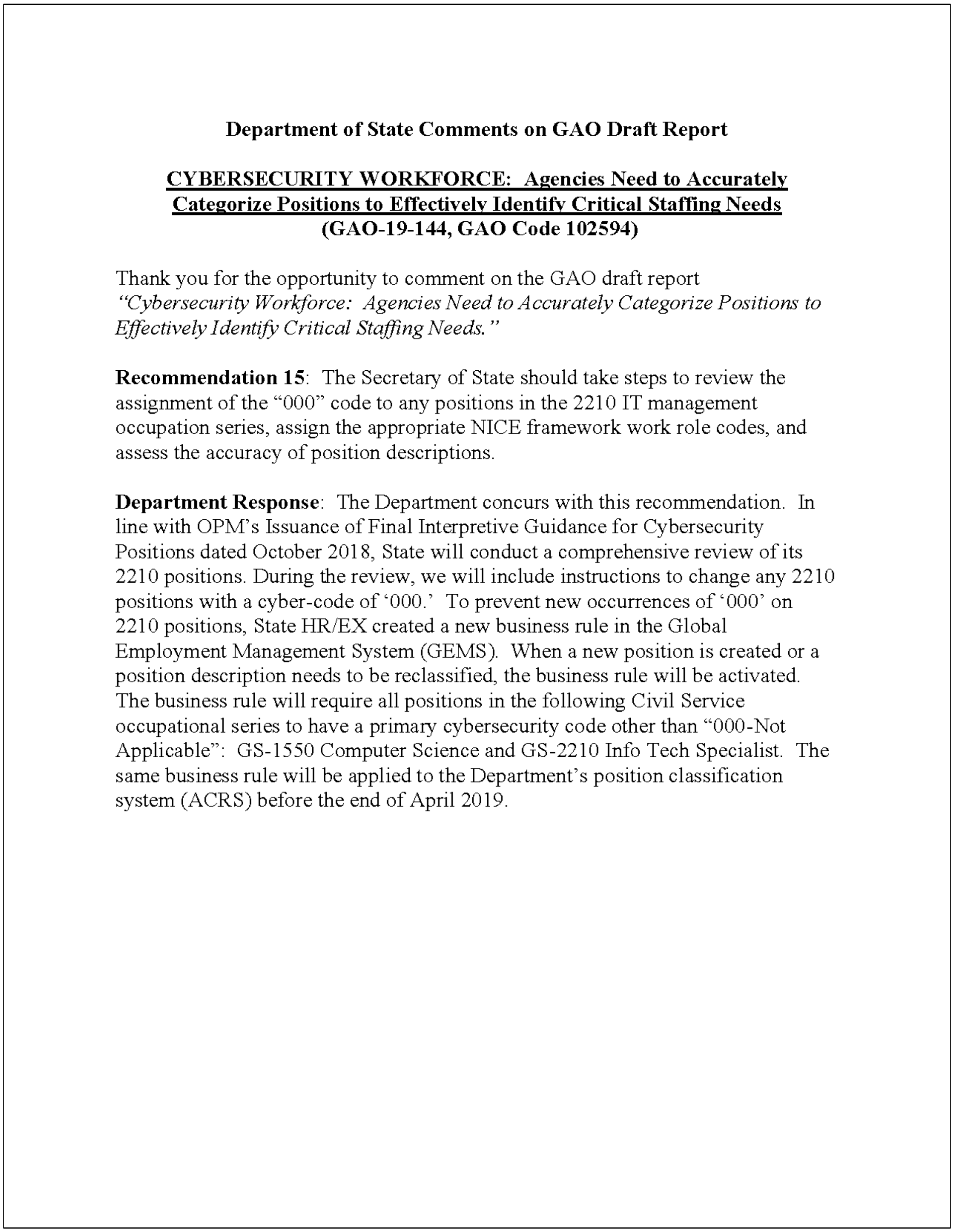
Sincerely,

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

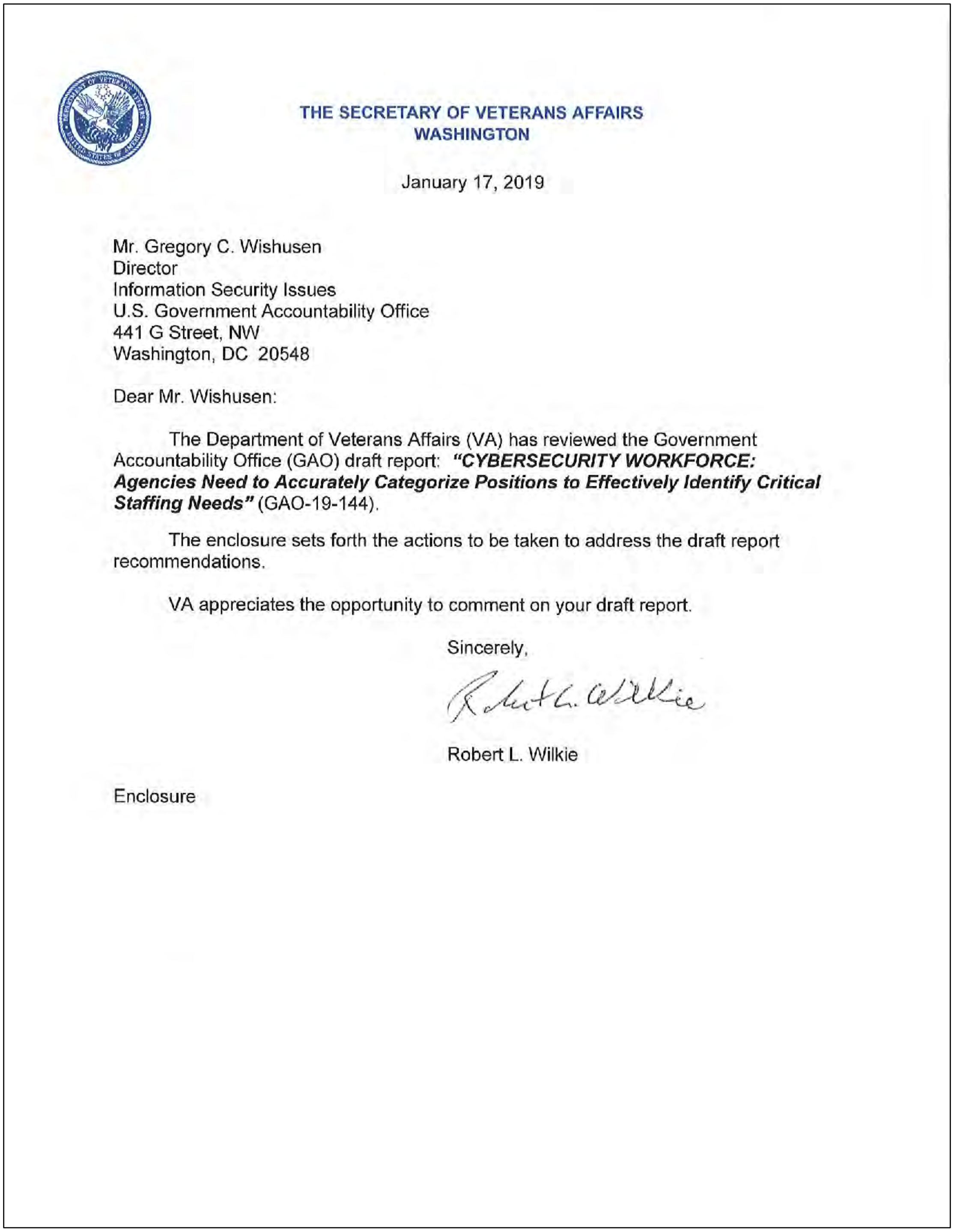
CYBERSECURITY WORKFORCE: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs
(GAO-19-144, GAO Code 102594)

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).

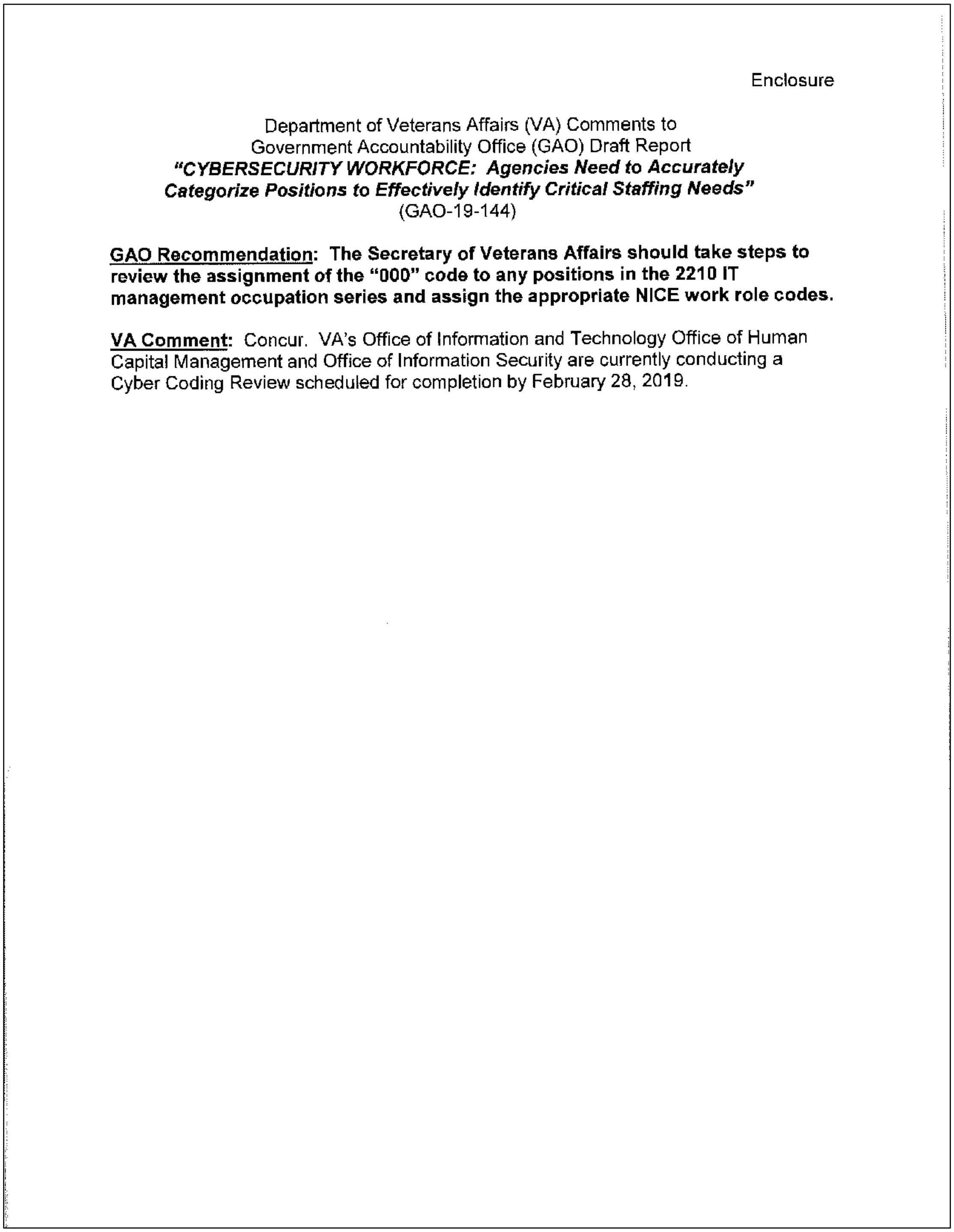
The enclosure sets forth the actions to be taken to address the draft report recommendations.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Robert L. Wilkie

Enclosure



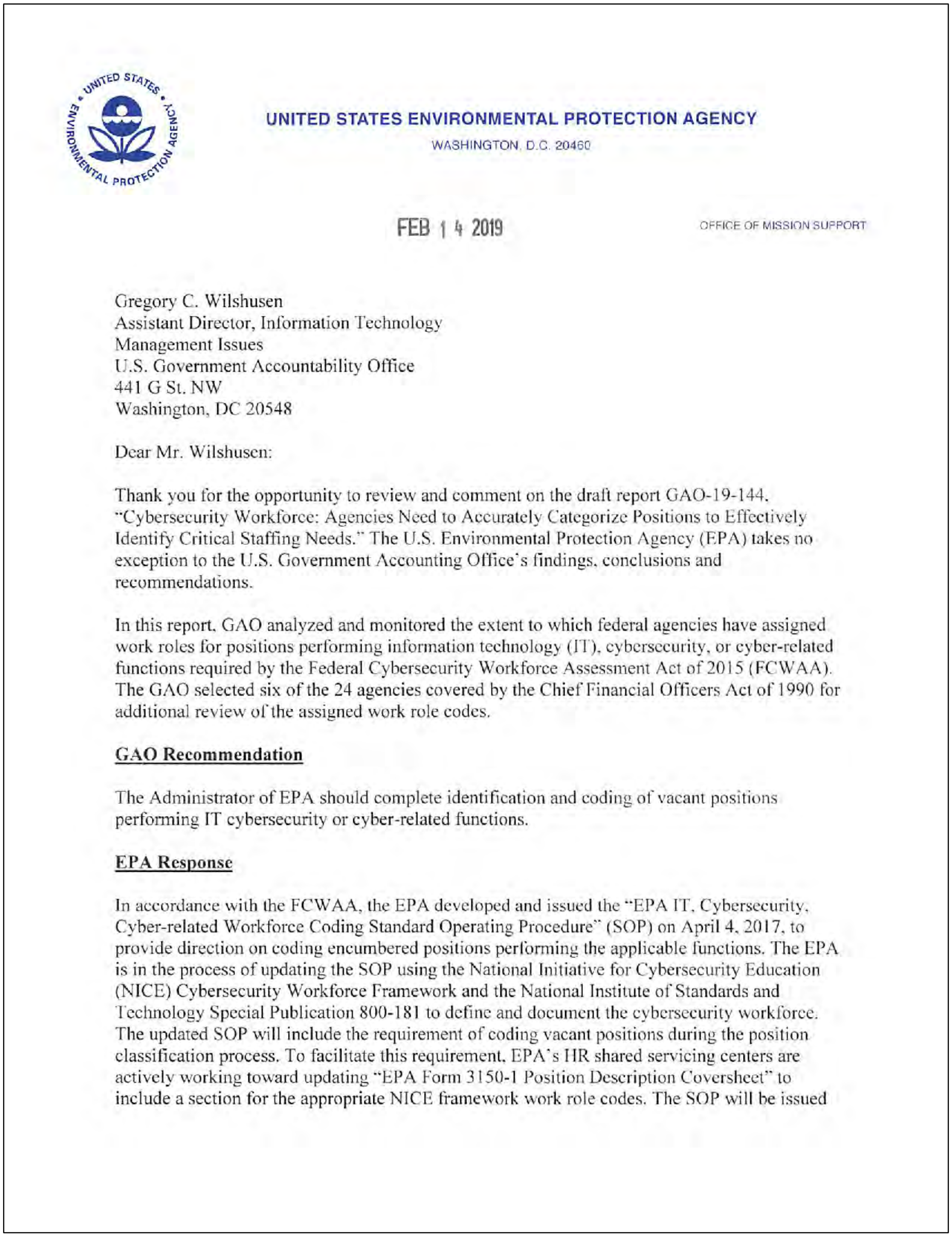
Enclosure

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)

<u>GAO Recommendation</u>: 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.

<u>VA Comment</u>: 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.

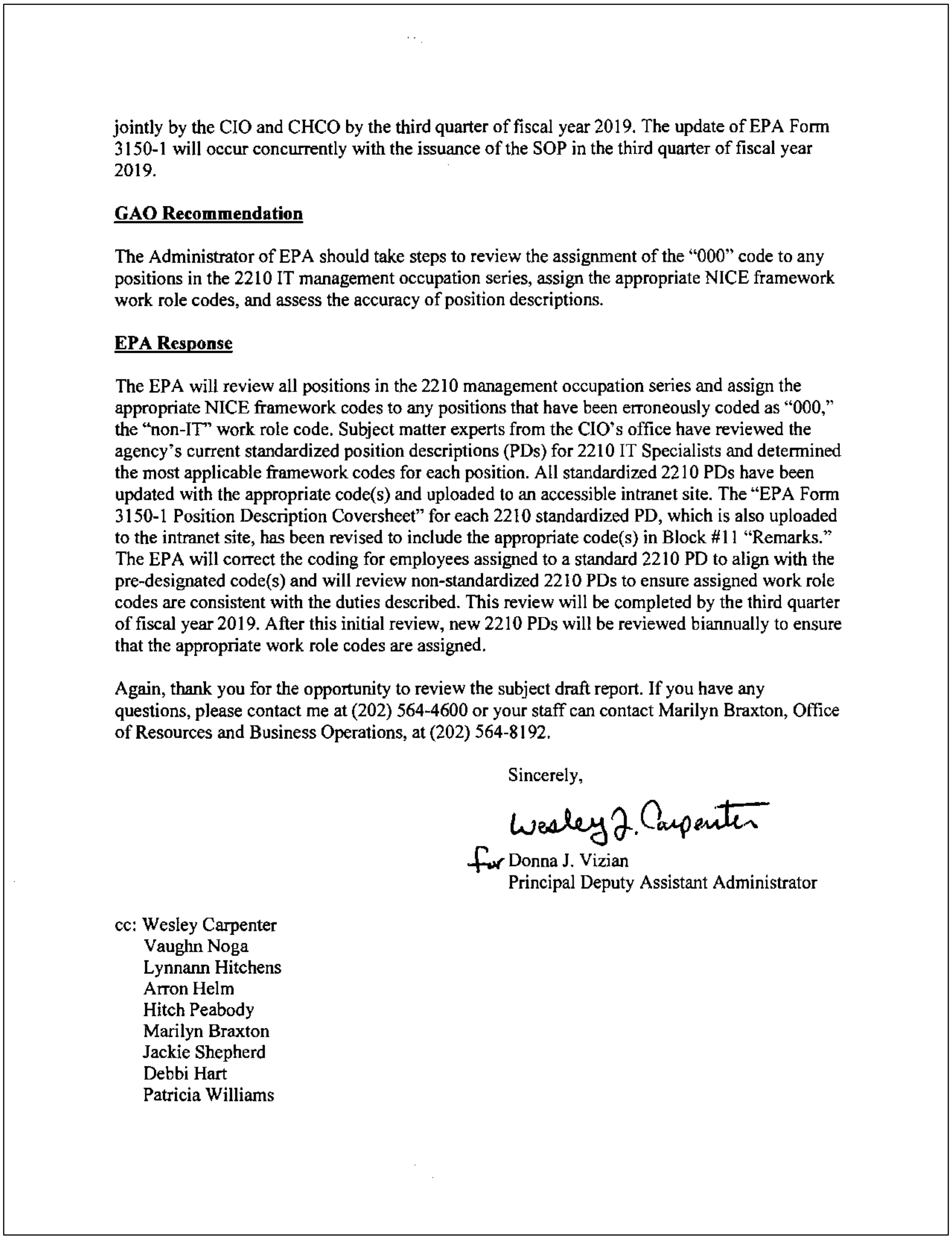
In this report, GAO analyzed and monitored the extent to which federal agencies have assigned work roles for positions performing information technology (IT), cybersecurity, or cyber-related functions required by the Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA). The GAO selected six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

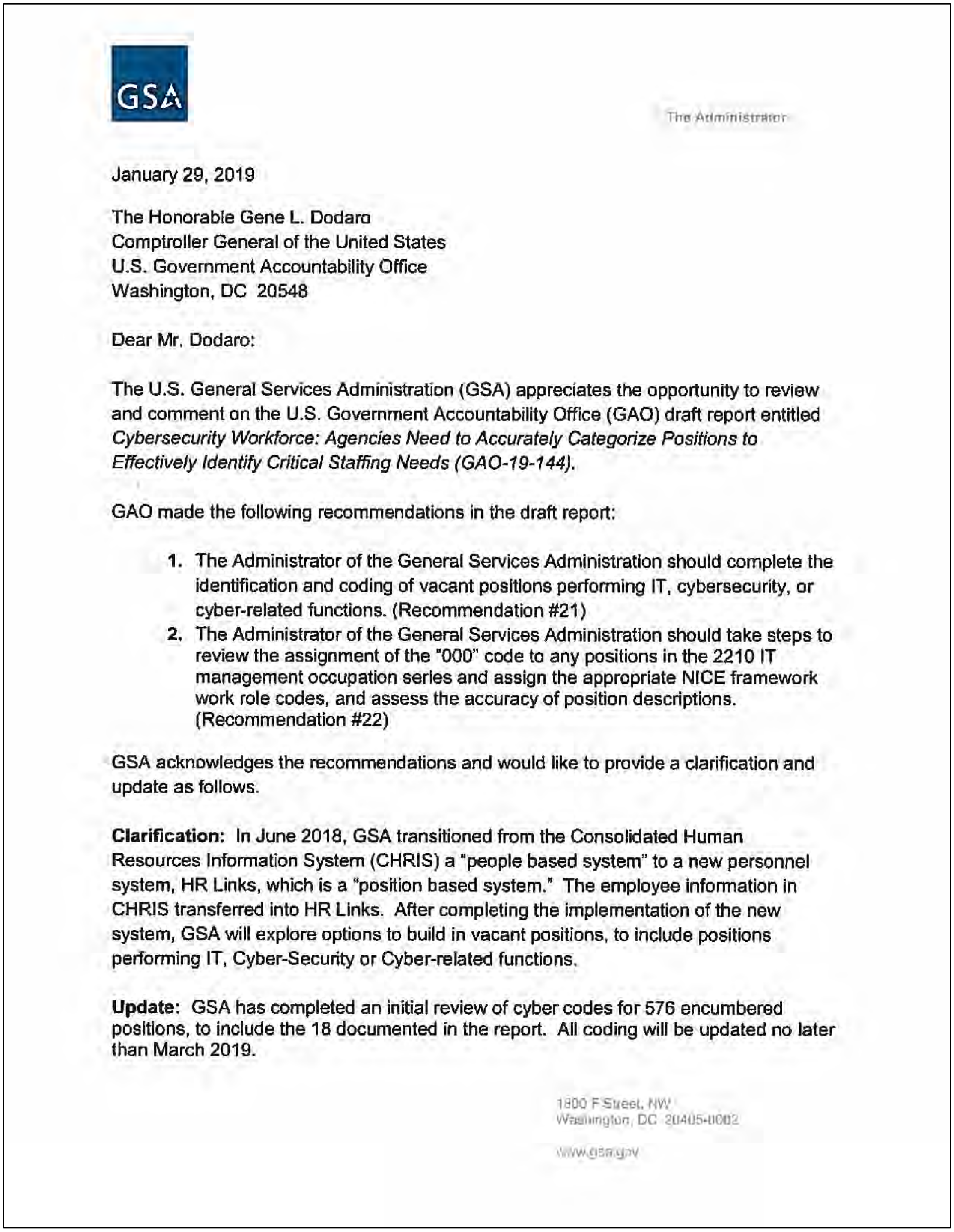
Sincerely,

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)

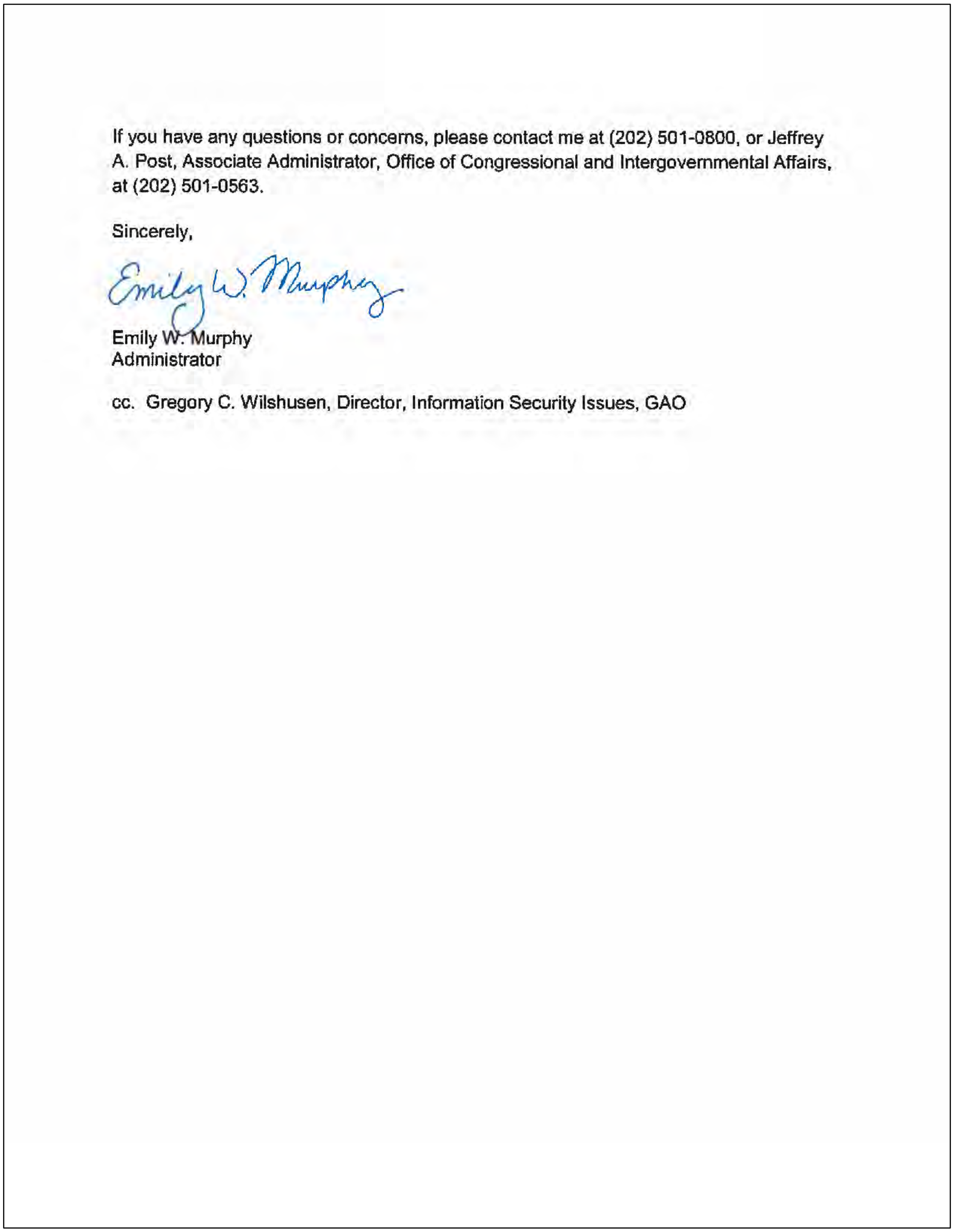
GSA acknowledges the recommendations and would like to provide a clarification and update as follows.

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.

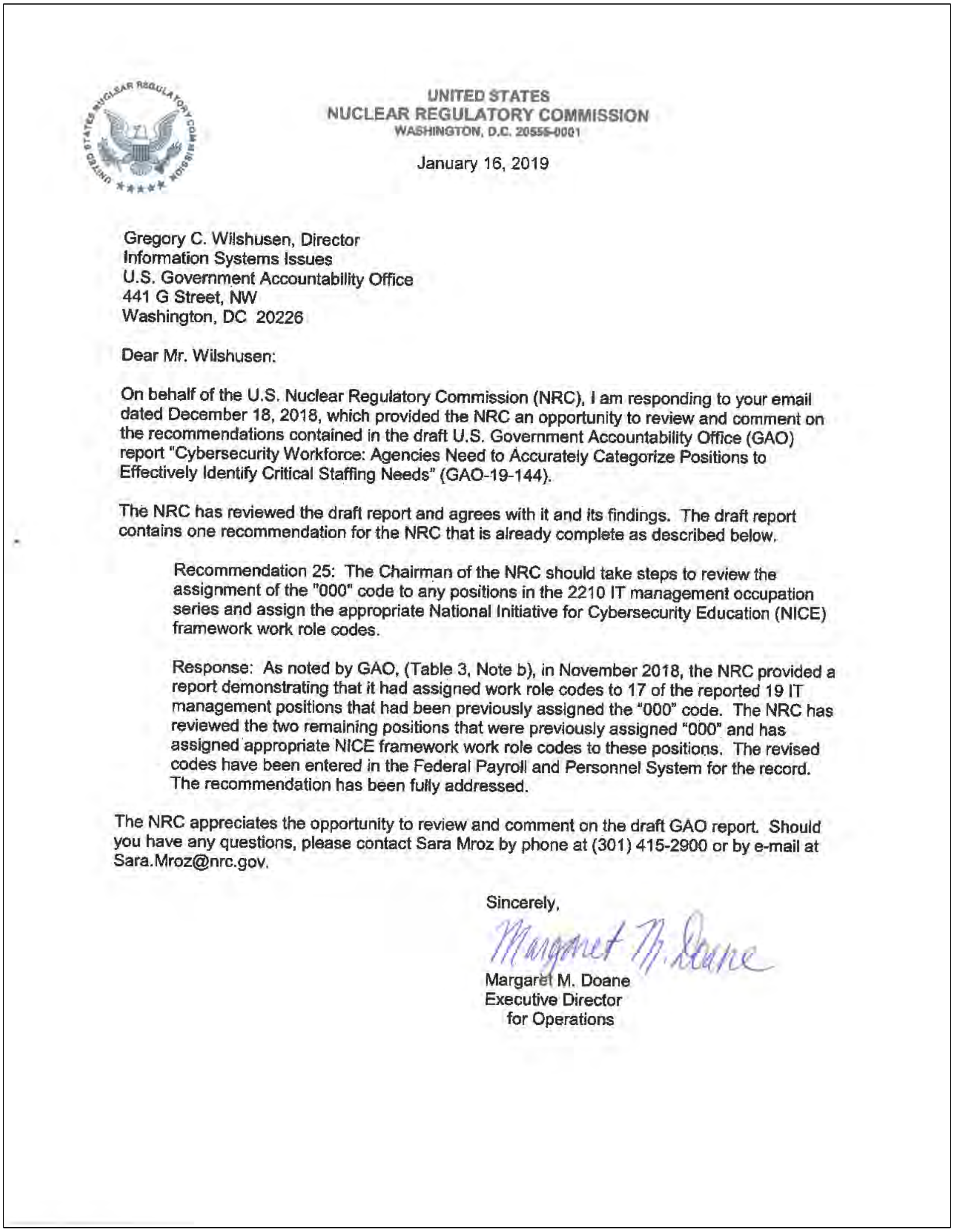
Sincerely,

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.

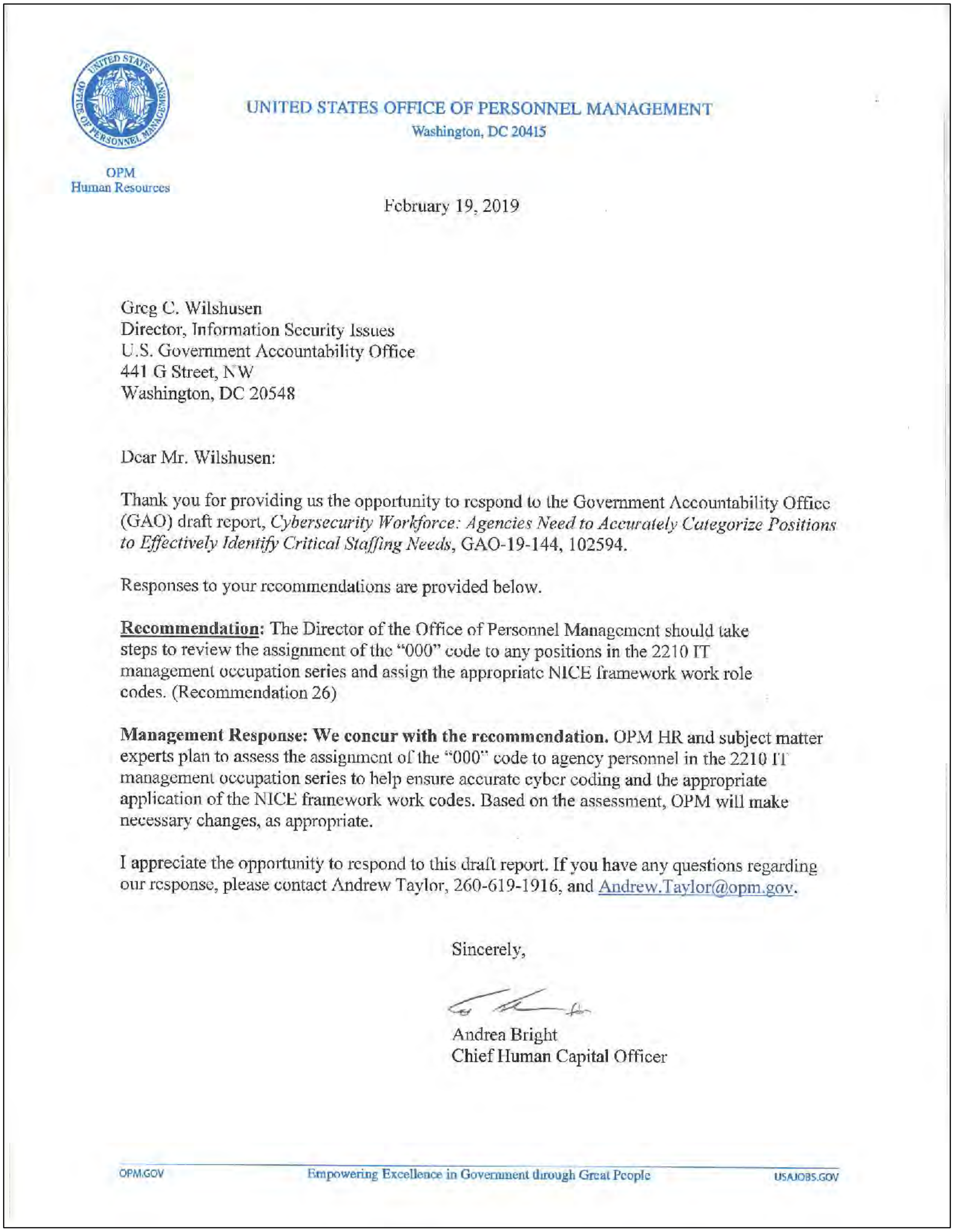
The NRC appreciates the opportunity to review and comment on the draft GAO report. Should you have any questions, please contact Sara Mroz by phone at (301) 415-2900 or by e-mail at Sara.Mroz@nrc.gov.

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.

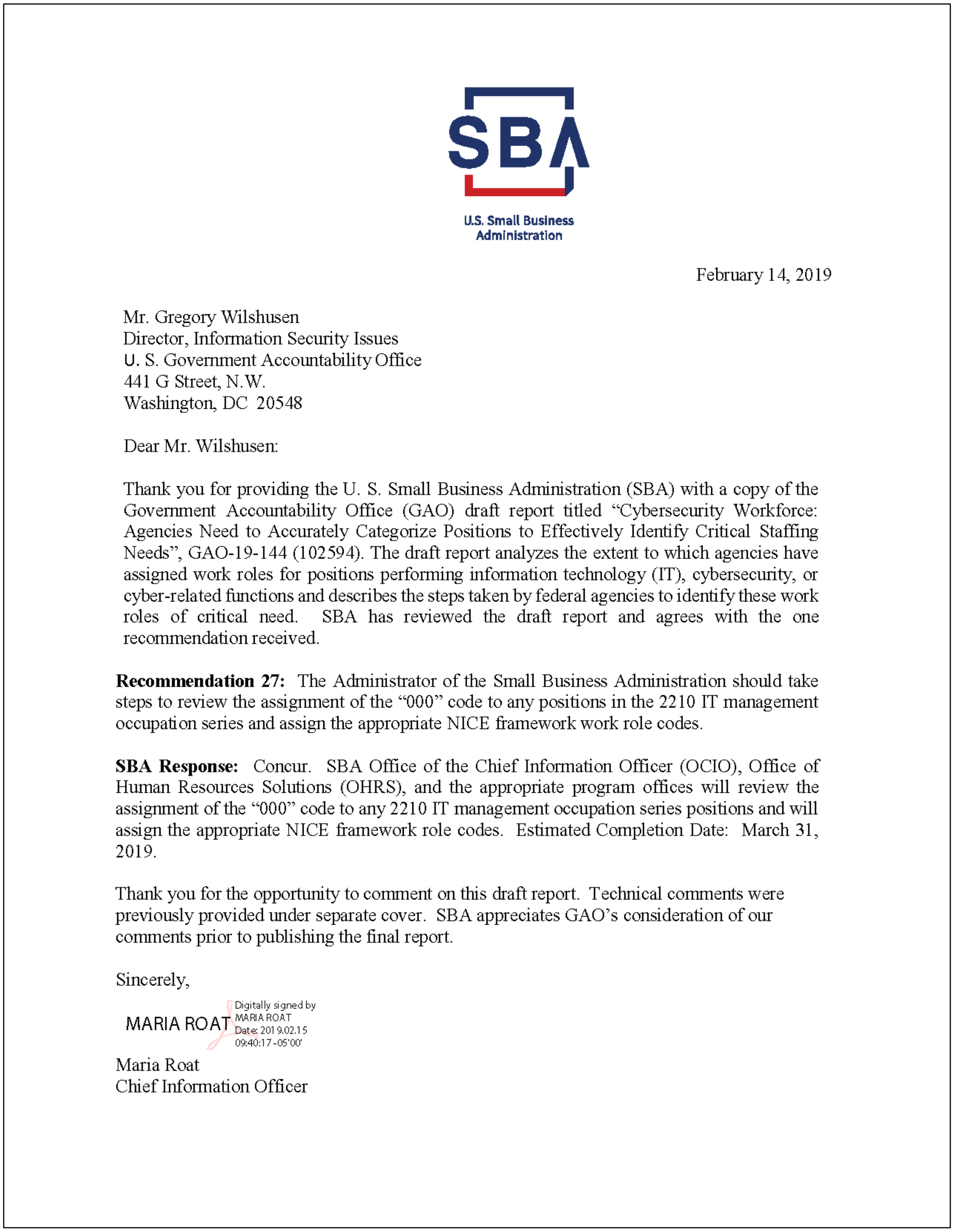
I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Andrew Taylor, 260-619-1916, and Andrew.Taylor@opm.gov.

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



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.

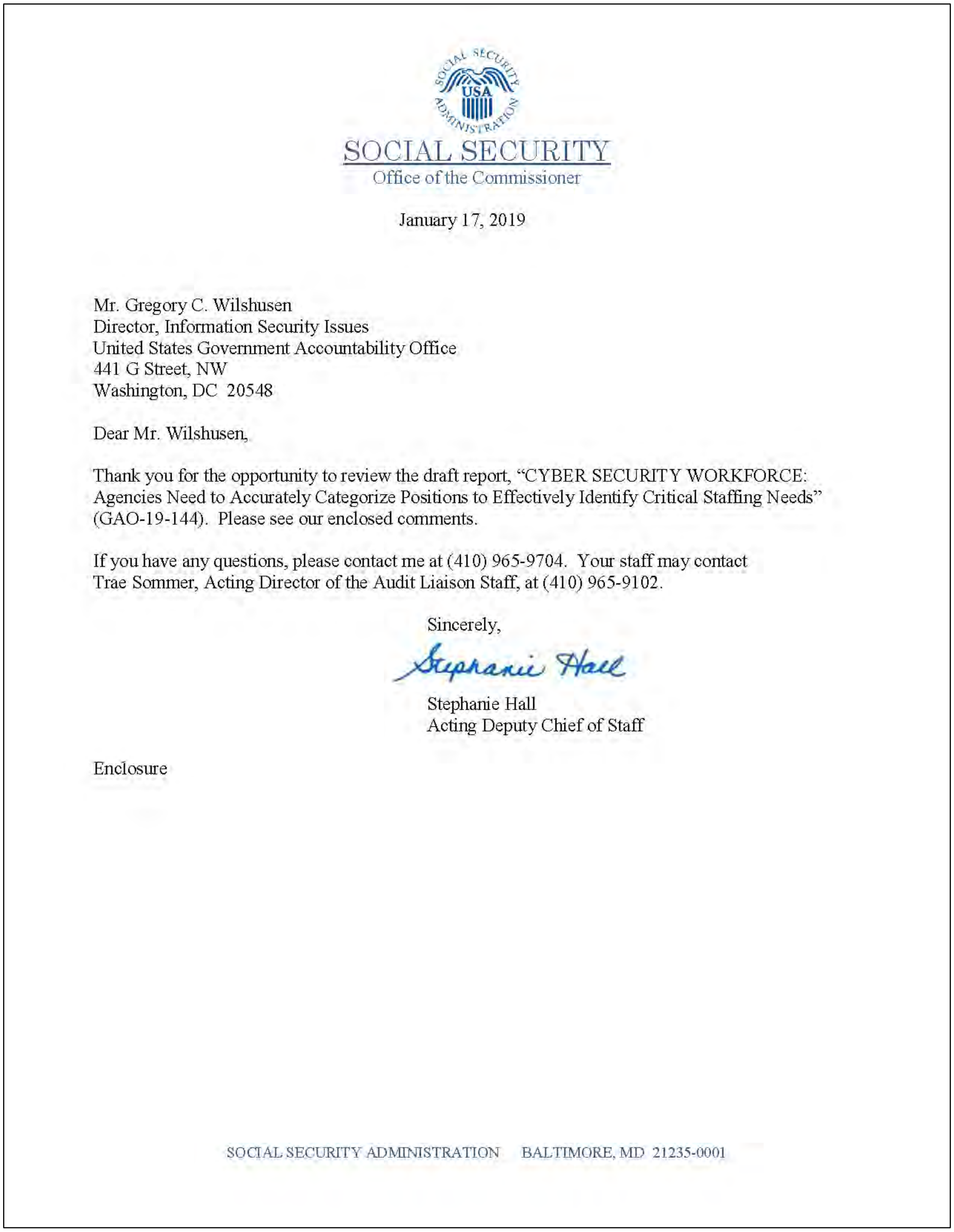
Thank you for the opportunity to comment on this draft report. Technical comments were previously provided under separate cover. SBA appreciates GAO's consideration of our comments prior to publishing the final report.

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.

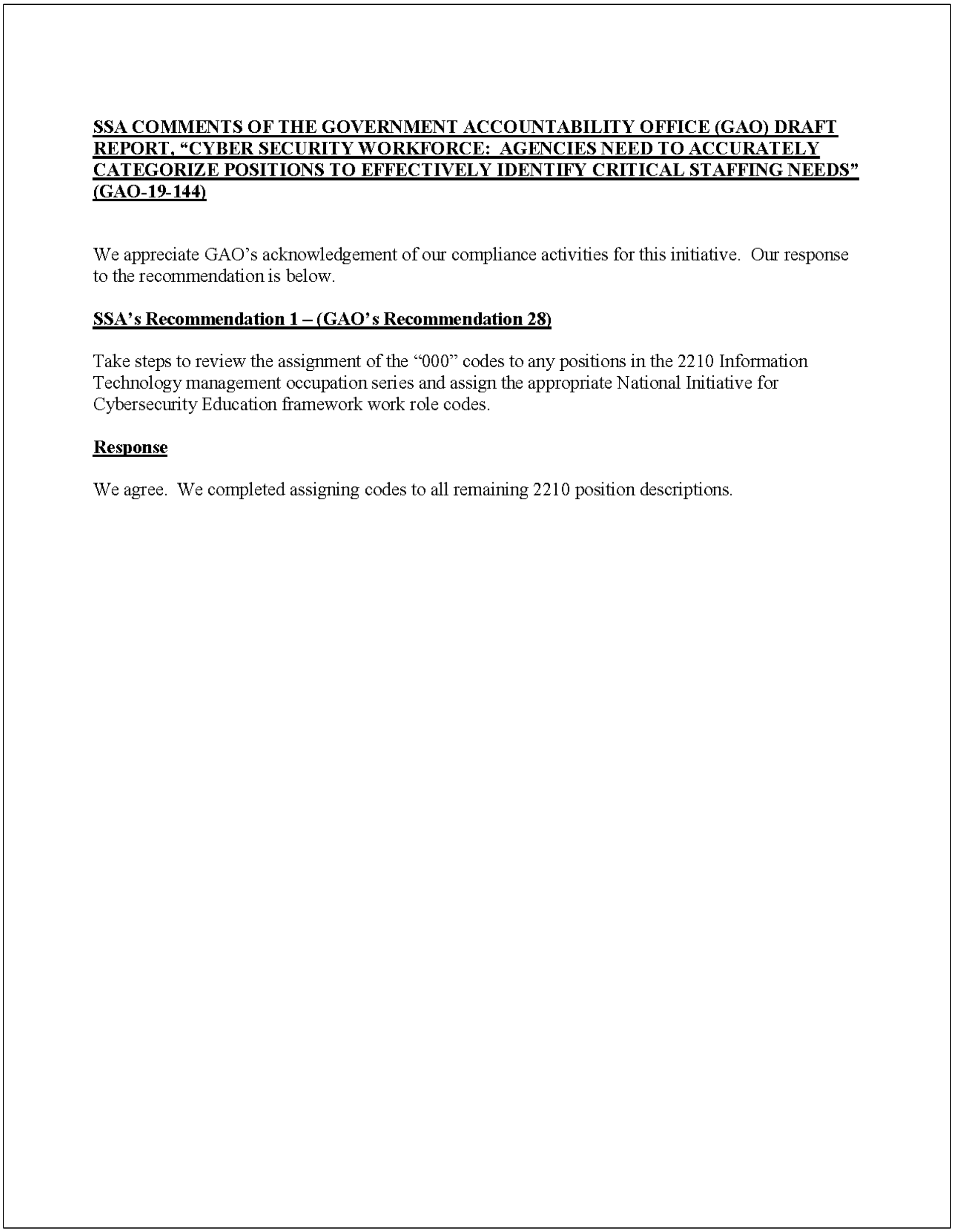
Sincerely,

Stephanie Hall

Stephanie Hall
Acting Deputy Chief of Staff

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001



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.

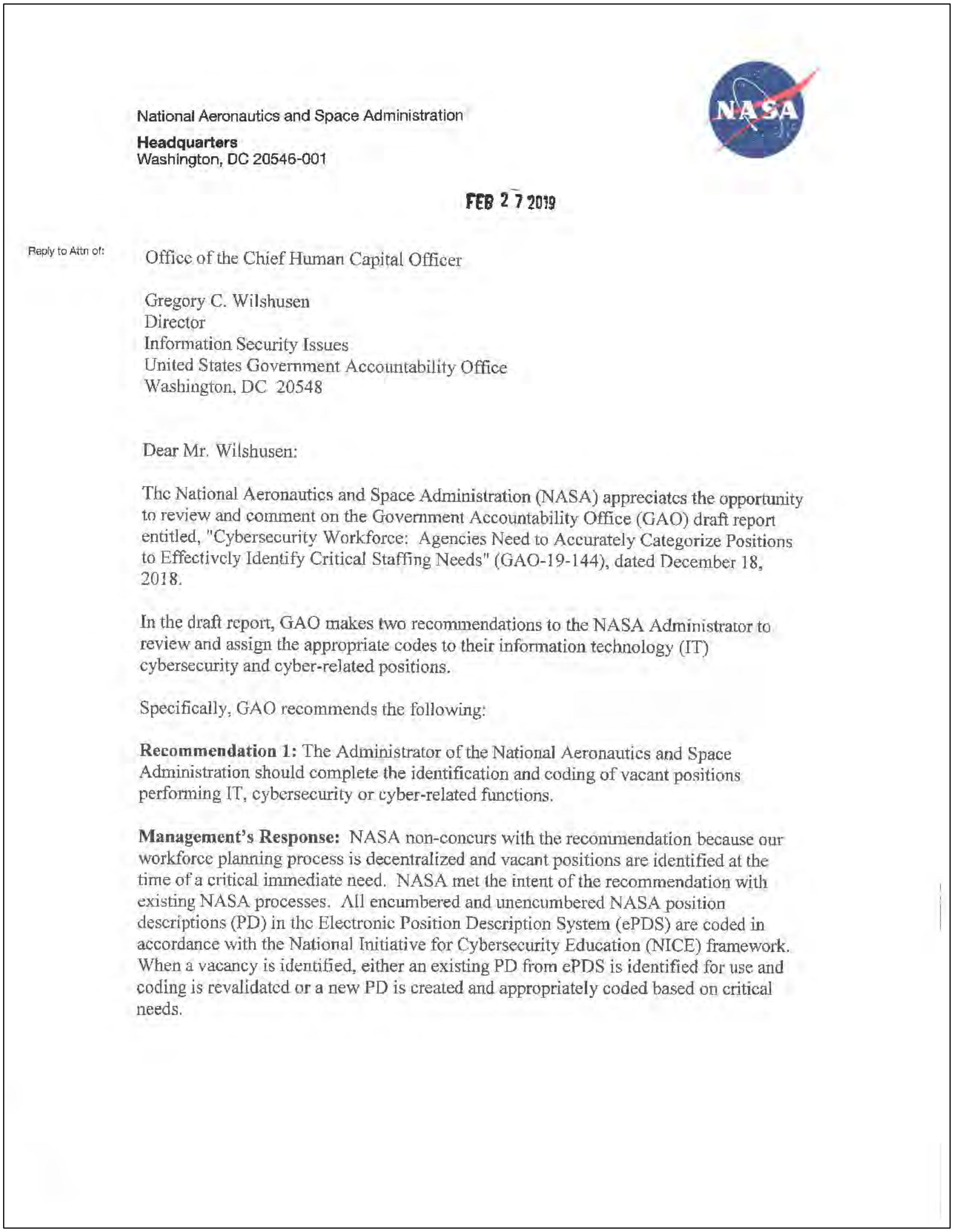
SSA's Recommendation 1 – (GAO's Recommendation 28)

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 27 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:

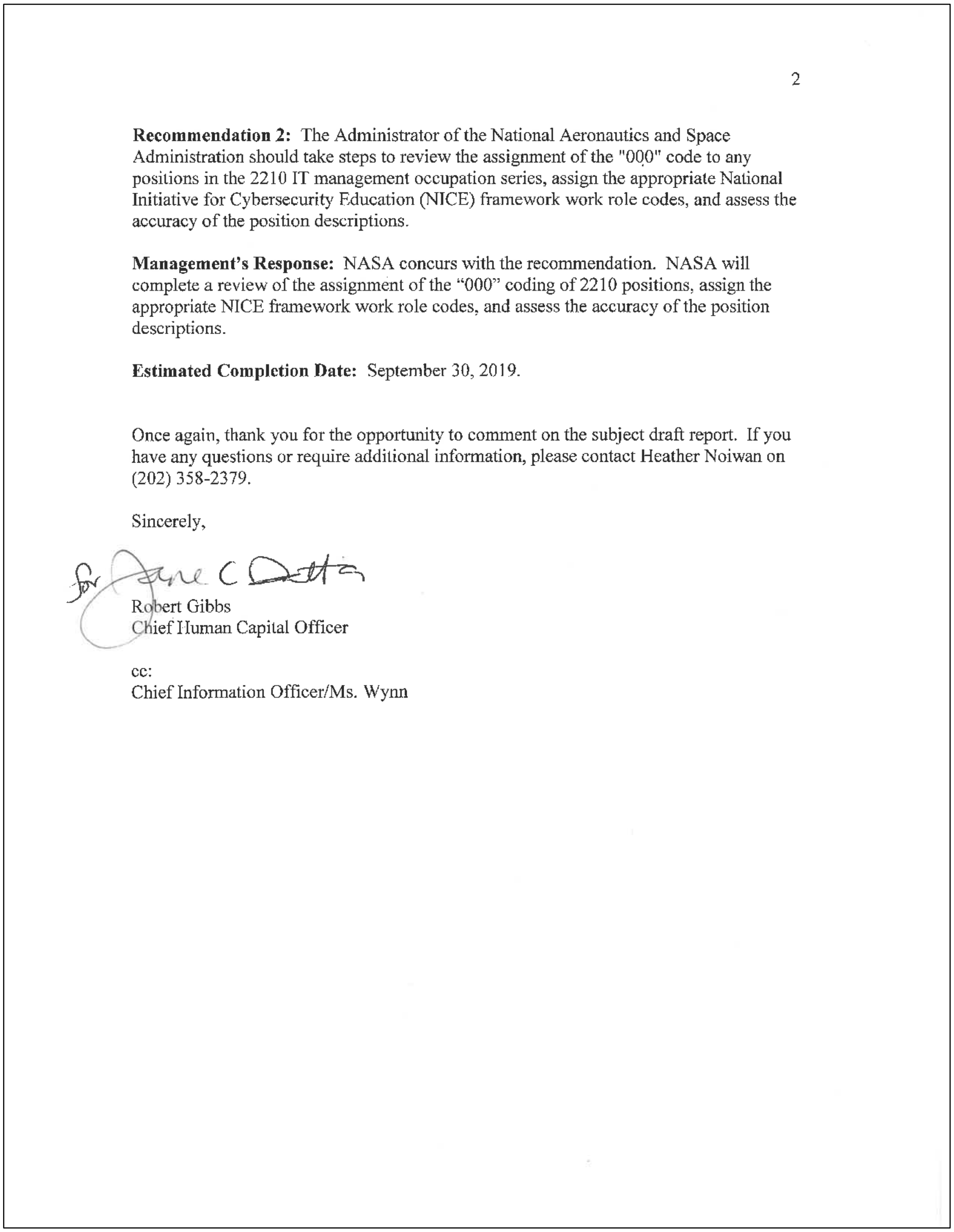
The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs" (GAO-19-144),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

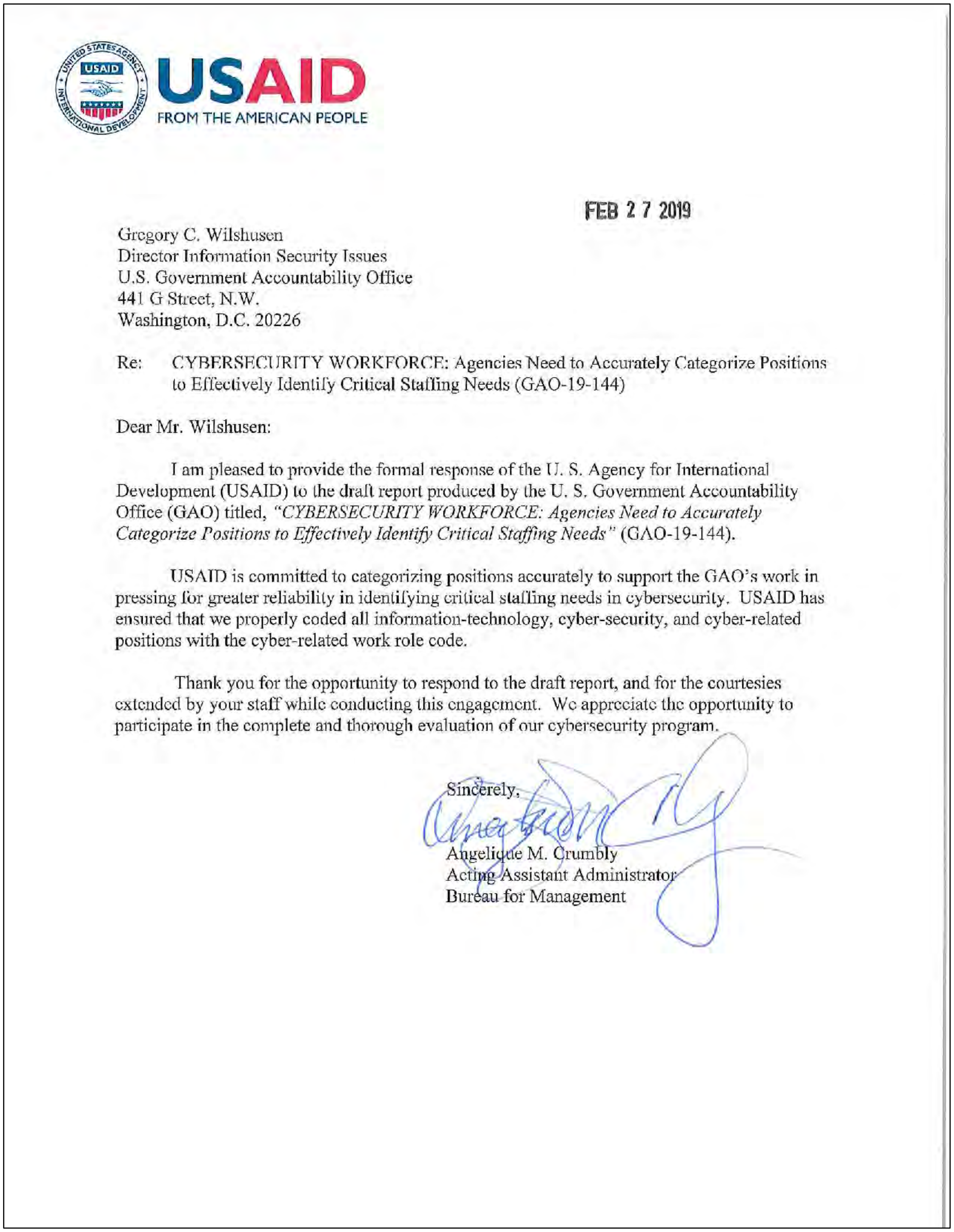
Sincerely,

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 2 7 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)

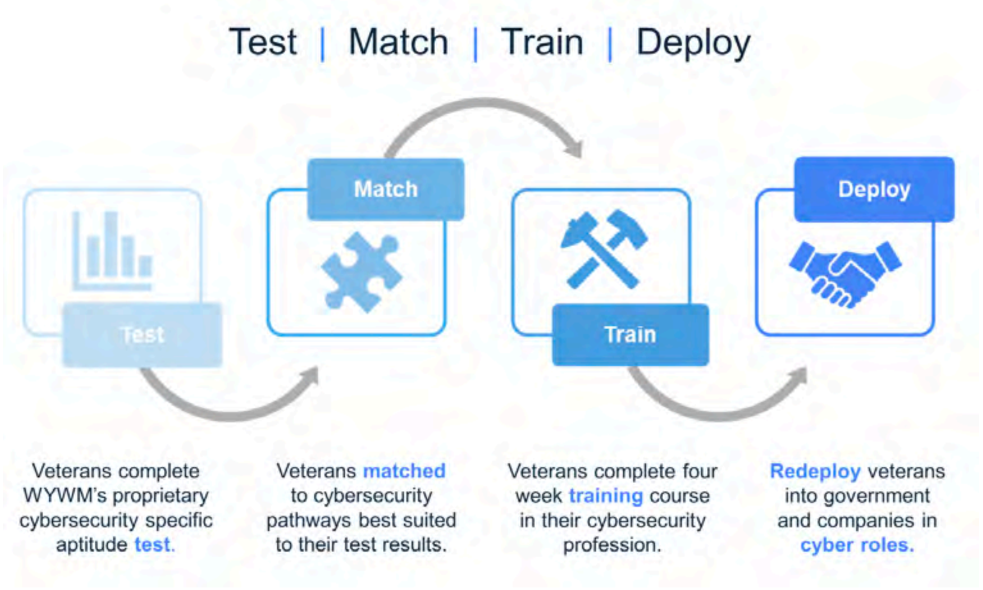
WITH
YOU
WITH
ME

Who are we?

WithYouWithMe (WYWM) is an online veteran run and owned company helping to solve veteran underemployment by developing and up-skilling talented military veterans in their transition to a new career in Cyber Security. We work closely with veterans to put them on a career pathway and an individual up-skill program to develop job-ready "hard skills" that fill the gaps in technology jobs in the labor market making them highly sought-after talent.

The program can also be used to upskill current serving members to provide skill uplift and greater capacity to build cyber capability.

We are Australia's premier veteran organization and fastest growing tech company, and we’ve now relocated to the U.S. and headquartered in DC. We use a skills-based competency training methodology, tailored to the individual and their matched career pathway.



Veterans complete WYWM’s proprietary cybersecurity specific aptitude **test.**

Veterans **matched** to cybersecurity pathways best suited to their test results.

Veterans complete four week **training** course in their cybersecurity profession.

Redeploy veterans into government and companies in **cyber roles.**

How do we do it?

WYWM’s infrastructure is set up to train anyone, from any background, without the requirement of previous cyber-security experience and qualifications. We are currently recruiting professionals for over 160 companies including SAP, Deloitte, Raytheon, Accenture, Amazon and the US Federal Government. Our success is due to our complex methodology and the use of data driven decisions. We call this our Predict, Develop, Match and Employ approach.

How can we help?

Our methodology helps in two ways:

1. We can drastically increase veteran and spouse employment rates by training them in high-demand skills and placing them in high paid jobs, free of charge and at scale.

2. Build the labor force for local businesses to deliver their services and thrive. This will improve the local and regional economy and empower it to prosper in an increasingly high-tech world.

Can we train at scale?

Through our online platform, we can train thousands of people, simultaneously, with industry respected certifications on completion of training.

Who do we work with?

We work with major American companies such as Raytheon, Lockheed, Booz Allen, Amazon, Bank of America, Splunk, ViaSat, General Dynamics, Deloitte, Accenture, SAP, multiple Federal and State Government Departments, etc. We add more employers to our ecosystem across the nation every week.

What high tech skills?

Cybersecurity, Data Analyst, Robotic Process Automation, and System Administration. We currently have open jobs based in District of Columbia, Virginia, Maryland, Georgia and Texas.

Sincerely,

Michelle Mosey
CEO North America
WithYouWithMe Inc.
830 D St SE
Washington, D.C. 20003
michelle@withyouwithme.com

WITH YOU WITH ME