United States Government Accountability Office

Testimony

Before the Subcommittee on Information Technology, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Tuesday, April 4, 2017

CYBERSECURITY

Federal Efforts Are Under Way That May Address Workforce Challenges

Statement of Nick Marinos, Director, Cybersecurity and Information Management Issues

GAO-17-533T

April 4, 2017

CYBERSECURITY

Federal Efforts Are Under Way That May Address Workforce Challenges

Highlights of GAO-17-533T, a testimony before the Subcommittee on Information Technology, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

The federal government faces an ever-evolving array of cyber-based threats to its systems and information. Further, federal systems and networks are inherently at risk because of their complexity, technological diversity, and geographic dispersion, among other reasons. GAO has designated the protection of federal information systems as a government-wide high-risk area since 1997. In 2001, GAO introduced strategic government-wide human capital management as another area of high risk. A key component of the government's ability to mitigate and respond to cyber threats is having a qualified, well-trained cybersecurity workforce. However, shortages in qualified cybersecurity professionals have been identified, which can hinder the government's ability to ensure an effective workforce.

This statement discusses challenges agencies face in ensuring an effective cybersecurity workforce, recent initiatives aimed at improving the federal cyber workforce, and ongoing activities that could assist in recruiting and retaining cybersecurity professionals. In preparing this statement, GAO relied on published work related to federal cybersecurity workforce efforts, and information reported by other federal and non-federal entities focusing on cybersecurity workforce challenges.

What GAO Recommends

Over the past several years, GAO has made several recommendations to federal agencies to enhance their IT workforce efforts. Agencies are in various stages of implementing these recommendations.

View GAO-17-533T. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

GAO and others have identified a number of key challenges facing federal agencies in ensuring that they have an effective cybersecurity workforce:

- **Identifying skills gaps:** As GAO reported in 2011, 2015, and 2016, federal agencies have faced challenges in effectively implementing workforce planning processes for information technology (IT) and defining cybersecurity staffing needs. GAO also reported that the Office of Personnel Management (OPM) could improve its efforts to close government-wide skills gaps.
- **Recruiting and retaining qualified staff:** Federal agencies continue to be challenged in recruiting and retaining qualified cybersecurity staff. For example, in August 2016, GAO reported that federal chief information security officers faced significant challenges in recruiting and retaining personnel with high-demand skills.
- **Federal hiring activities:** The federal hiring process may cause agencies to lose out on qualified candidates. In August 2016 GAO reported that OPM and agencies needed to assess available federal hiring authorities to more effectively meet their workforce needs.

To address these and other challenges, several executive branch initiatives have been launched and federal laws enacted. For example, in July 2016, OPM and the Office of Management and Budget issued a strategy with goals, actions, and timelines for improving the cybersecurity workforce. In addition, laws such as the Federal Cybersecurity Workforce Assessment Act of 2015 require agencies to identify IT and cyber-related positions of greatest need.

Further, other ongoing activities have the potential to assist agencies in developing, recruiting, and retaining an effective cybersecurity workforce. For example:

- **Promoting cyber and science, technology, engineering and mathematics (STEM) education:** A center funded by the Department of Homeland Security (DHS) developed a kindergarten to 12th grade-level cyber-based curriculum that provides opportunities for students to become aware of cyber issues, engage in cyber education, and enter cyber career fields.
- **Cybersecurity scholarships:** Programs such as Scholarship for Service provide tuition assistance to undergraduate and graduate students studying cybersecurity in exchange for a commitment to federal service.
- **National Initiative for Cybersecurity Careers and Studies:** DHS, in partnership with several other agencies, launched the National Initiative for Cybersecurity Careers and Studies in 2013 as an online resource to connect government employees, students, educators, and industry with cybersecurity training providers across the nation.

If effectively implemented, these initiatives, laws, and activities could further agencies' efforts to establish the cybersecurity workforce needed to secure and protect federal IT systems.

Chairman Hurd, Ranking Member Kelly, and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the federal information technology (IT) and cybersecurity workforce. As recent cyberattacks have illustrated, the need for robust and effective cybersecurity has never been greater. Threats to federal IT infrastructure continue to grow in number and sophistication, posing a risk to the reliable functioning of our government. Compounding the risk, systems used by federal agencies often have security vulnerabilities.

Accordingly, having cybersecurity professionals in the federal workforce to help to prevent or mitigate vulnerabilities in federal IT systems that can be exploited by the increasing number of threats from a variety of sources is essential. However, achieving a resilient, well-trained, and dedicated cybersecurity workforce to help protect our information and infrastructure has been a long-standing challenge for the federal government. Since 1997 we have identified the protection of federal information systems as a government-wide high-risk area. In addition, in 2001, we introduced strategic government-wide human capital management as another area of high risk.[1]

My statement today discusses a number of the key challenges federal agencies face in ensuring that they have an effective cybersecurity workforce with the right knowledge, skills, and abilities to secure federal systems and critical cyber infrastructure. I will also discuss executive branch initiatives and federal laws aimed at improving the federal cybersecurity workforce, as well as other ongoing activities that could assist agencies in recruiting and retaining cybersecurity professionals.

In preparing this statement, we relied on our previously published work related to cybersecurity and government-wide workforce efforts and challenges faced by the federal government in establishing an effective cybersecurity workforce. Based on this work, we examined recently enacted legislation, executive-branch initiatives, and other activities intended to address these challenges. Further, we reviewed information reported by other federal and non-federal entities focusing on cybersecurity workforce challenges. Our reports cited in this statement

[1]GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

include detailed discussions of the objectives, scope, and methodology for the work that we conducted.

The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

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

The security of federal information systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. However, systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. For example, the national vulnerability database maintained by the National Institute of Standards and Technology (NIST) identified 82,384 publicly known cybersecurity vulnerabilities and exposures as of February 9, 2017, with more being added each day.

Federal systems and networks are also often interconnected with other internal and external systems and networks, including the Internet, thereby increasing the number of avenues of attack and expanding their attack surface. In addition, cyber threats to systems supporting the federal government and critical infrastructure are evolving and becoming more sophisticated. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, foreign nations—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks.

Cybersecurity professionals can help to prevent or mitigate the vulnerabilities that could allow malicious individuals and groups access to federal IT systems. The ability to secure federal systems depends on the knowledge, skills, and abilities of the federal and contractor workforce that uses, implements, secures, and maintains these systems. This includes federal and contractor employees who use the IT systems in the course of their work as well as the designers, developers, programmers, and administrators of the programs and systems.

However, the Office of Management and Budget (OMB) has noted that the federal government and private industry face a persistent shortage of cybersecurity and IT talent to implement and oversee information security protections to combat cyber threats. In addition, the RAND Corporation[2] and the Partnership for Public Service[3] have reported that there is a nationwide shortage of cybersecurity experts, in particular in the federal government. According to these reports, this shortage of cybersecurity professionals makes securing the nation's networks more challenging and may leave federal IT systems vulnerable to malicious attacks.

Agencies Face Key Challenges in Ensuring an Effective Cybersecurity Workforce

We and others have identified a number of key challenges federal agencies are facing to ensure that they have a sufficient cybersecurity workforce with the skills necessary to protect their information and networks from cyber threats. These challenges pertain to identifying and closing skill gaps as part of a comprehensive workforce planning process, recruiting and retaining qualified staff, and navigating the federal hiring process.

Identifying and closing skill gaps

A high-performance organization needs a workforce with talent, multidisciplinary knowledge, and up-to-date skills in order to achieve its

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

[3]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).

mission. To ensure such a workforce for cybersecurity, we have identified key practices for strategic IT workforce planning that focus especially on the need for organizations to identify and address gaps in critical skills. These practices include (1) setting the strategic direction for IT workforce planning, (2) analyzing the workforce to identify skill gaps, (3) developing strategies and implementing activities to address these gaps, and (4) monitoring and reporting progress in addressing gaps.[4]

However, over the last several years, we and others have reported on federal agencies' challenges to define their cybersecurity workforces and address their IT skills gaps. For example:

- In November 2011, we reported that eight federal agencies had identified challenges in their workforce planning efforts.[5] For example, they were not able to determine the size of their cybersecurity workforce because of variations in how the cyber-related work was defined and the lack of a cybersecurity specific occupational series. In addition, we noted that the eight agencies had taken varied steps to implement workforce planning practices for cybersecurity personnel. For example, five of the eight agencies had established cybersecurity workforce plans or other agency-wide activities addressing cybersecurity workforce planning. However, these plans did not always include strategies for addressing gaps in critical skills or competencies, among other things. To address these shortcomings, we made six recommendations to enhance individual agency workforce planning activities. Of the six agencies to which we made individual recommendations, five agreed and one neither agreed nor disagreed with our recommendations. Since our report was issued, the agencies have implemented most of these recommendations.

- In January 2015, we reported that the Office of Personnel Management (OPM) and a Chief Human Capital Officers Council working group had identified skills gaps in government-wide, mission-

[4]See GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination,* GAO-12-8 (Washington, D.C.: Nov. 29, 2011) and *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).

[5]GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination,* GAO-12-8 (Washington, D.C.: Nov. 29, 2011).

critical occupations, including cybersecurity.[6] We noted that, although these initial efforts had created an infrastructure for addressing skills gaps, overall progress was mixed. At times, goals had targets that were difficult to measure. Likewise, agency officials chose to track metrics that often did not allow for an accurate assessment of progress made toward these goals for closing skills gaps. In addition, OPM had not established time frames or a process for collecting government-wide staffing and competency data to help agencies determine the competencies that are critical to successfully achieving their mission. We pointed out that OPM and selected agencies could improve efforts to address skills gaps by strengthening their use of quarterly data-driven reviews (known as HRstats). Based on these findings, we recommended that OPM (1) strengthen its methodology for identifying and addressing skills gaps, (2) establish a schedule and process for collecting government-wide staffing and competency data, and (3) develop a set of metrics for agency HRstat reviews. OPM generally concurred with the first and third recommendations, but did not concur with the second recommendation, citing funding constraints. These recommendations have not yet been implemented.

- In an April 2015 report, the Partnership for Public Service noted a continuing need for the government to develop an understanding of the size and skills of the current cybersecurity workforce; project the government's future cybersecurity human capital needs; assess qualitative and quantitative gaps between the current workforce and the workforce needed to address future challenges; and develop strategies, as well as program and policy goals, designed to close those gaps. The Partnership attributed these challenges to the lack of a government-wide master cybersecurity workforce strategy, leaving agencies to operate largely on their own under a haphazard system.[7]

- In November 2016, we reported that five selected agencies had made mixed progress in assessing their IT skill gaps.[8] These agencies had started focusing on identifying cybersecurity staffing gaps, but more work remained in assessing competency gaps and in broadening the

[6]GAO, *Federal Workforce: OPM and Agencies Need to Strengthen Efforts to Identify and Close Mission-Critical Skills Gaps,* GAO-15-223 (Washington, D.C.: Jan. 30, 2015).

[7]Partnership for Public Service, *Cyber In-Security II*.

[8]GAO-17-8.

focus to include the entire IT community. For example, four of the five agencies had not demonstrated an established IT workforce planning process, which would assist them in identifying and addressing skill gaps. In several cases, these shortcomings were due to a lack of comprehensive policies and procedures for assessing workforce needs. We recommended that the agencies take steps to fully implement IT workforce planning practices. The agencies agreed or partially agreed with our recommendations; however, the recommendations have not yet been implemented.

Recruiting and retaining qualified staff

An effective hiring process meets the needs of agencies and managers by filling positions with quality employees through the use of a timely, efficient, and transparent process. To recruit and retain personnel with the critical skills needed to accomplish their missions, federal agencies can offer incentives, such as recruitment, relocation, and retention incentive payments; student loan repayments; annual leave enhancements; and scholarships. Agencies can also use training and development opportunities as an incentive to help recruit and retain employees.

However, we and others have found that agencies have faced persistent challenges in recruiting and retaining well-qualified cybersecurity talent:

- In November 2011, we reported that the quality of cybersecurity training and development programs varied significantly across the eight agencies in our review. Additionally, most of the eight agencies in our review said they used some incentives to support their cybersecurity workforce; however, they either had not evaluated or had difficulty evaluating whether incentives effectively support hiring and retaining highly skilled personnel in hard-to-fill positions.[9] We also found that, although OPM had planned to develop guidance and tools to assist agencies in the administration and oversight of their incentive programs, it had not yet done so. To address this shortcoming, we recommended that OPM finalize and issue guidance to agencies on how to track the use and effectiveness of incentives for hard-to-fill positions, including cybersecurity positions; OPM has since implemented this recommendation.

[9]GAO-12-8.

- In August 2016, we reported the results of our review of the current authorities of agency chief information security officers (CISO).[10] Among other things, CISOs identified key challenges they faced in fulfilling their responsibilities. Several of these challenges 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 said that some security personnel lacked security skills or were not sufficiently trained.

- Others have also noted the challenge of hiring and retaining qualified cybersecurity professionals. For example, the April 2015 Partnership for Public Service report highlighted obstacles to federal recruitment of cybersecurity talent, including the inability of the government to offer salaries competitive with those in the private sector.[11] In addition, according to a January 2017 report from the federal CIO Council, chief information officers (CIO) reported that it is difficult for agencies to offer well-qualified candidates a salary that is competitive with the private sector.[12] This salary issue in turn can create problems in retaining talented government employees. OMB has also identified additional potential issues, such as job candidates' concern that a private sector position may give them more autonomy and a more flexible work culture than a federal information security position.

Navigating the federal hiring process

We have previously reported that the federal hiring process all too often does not meet the needs of (1) agencies in achieving their missions; (2) managers in filling positions with the right talent; and (3) applicants for a timely, efficient, transparent, and merit-based process. In short, we noted that the federal hiring process is often an impediment to the very customers it is designed to serve in that it makes it difficult for agencies and managers to obtain the right people with the right skills, and

[10]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).

[11]Partnership for Public Service, *Cyber-Insecurity II.*

[12]CIO Council, *State of Federal Information Technology* (January 2017).

applicants can be dissuaded from public service because of the complex and lengthy procedures.[13]

As we and others have reported, the federal hiring process can pose obstacles to the efficient and effective hiring of cybersecurity talent:

- The Partnership for Public Service reported in 2015 that the government loses top candidates to a slow and ineffective hiring process characterized by "self-inflicted" process delays and outdated assessment methods.[14] The CIO Council also reported in January 2017 that CIOs were often frustrated with the federal hiring process. Its report noted that the hiring process for federal agencies often takes significantly longer than in the private sector and that selection officials with limited cybersecurity expertise may misevaluate candidates' capabilities, leading to under-qualified candidates advancing ahead of well-qualified ones.[15]

- In August 2016, we issued a report on the extent to which federal hiring authorities were meeting agency needs.[16] Although competitive hiring[17] 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

[13]GAO, *Human Capital: Transforming Federal Recruiting and Hiring Efforts*, GAO-08-762T (Washington, D.C.: May 8, 2008).

[14]Partnership for Public Service, *Cyber In-Security II*.

[15]CIO Council, *State of Federal Information Technology*.

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

[17]Federal employees can be hired under several different hiring authorities, including competitive service (the standard hiring authority), excepted service, and direct hire authority. Each authority has different rules and regulations governing the selection of candidates, with the rules for excepted service and direct hire intended to make it easier or faster for agencies to hire personnel under certain circumstances.

authorities to more effectively meet their hiring needs. We recommended that OPM work with agencies to determine the extent to which hiring authorities were meeting agency needs and use this information to refine, eliminate, or expand authorities as needed. OPM generally concurred with these recommendations but has not yet implemented them.

As noted previously, we have identified both information security and strategic human capital management as government-wide high-risk areas. To address these high-risk areas, agencies need to take focused, concerted action, including implementing our outstanding recommendations, which can help mitigate the challenges associated with developing an effective cybersecurity workforce. This will help ensure that the federal government has a capable cybersecurity workforce with the necessary knowledge, skills, and competencies for carrying out its mission.

Recent Federal Initiatives, Legislation, and Ongoing Activities Are Intended to Improve the Federal Cybersecurity Workforce

Based on a review of our previous work, we identified a number of ongoing efforts to improve the cybersecurity workforce. The executive branch, Congress, and federal agencies have recognized the need for, and taken actions aimed at achieving, an effective federal cybersecurity workforce. Specifically, executive branch organizations have initiatives under way to help government agencies address workforce-related challenges; Congress passed legislation intended to improve workforce planning and hiring; and federal agencies have instituted other ongoing activities that may assist the federal government in enhancing its cybersecurity workforce.

Multiple Executive Branch Initiatives Are Under Way to Address Workforce Challenges

A number of executive branch initiatives have been undertaken over the last several years intended to improve the federal cybersecurity workforce. They include the following, among others:

- **The National Initiative for Cybersecurity Education (NICE):** This initiative, which began in March 2010, is a partnership between government, academia, and the private sector that is coordinated by NIST to help improve cybersecurity education, including efforts directed at training, public awareness, and the federal cybersecurity workforce. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and

workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure.

- **National Cybersecurity Workforce Framework:** In April 2013, NICE published a national cybersecurity workforce framework, which was intended to provide a consistent way to define and describe cybersecurity work at any public or private organization, including federal agencies. The framework defined 31 cybersecurity-related specialty areas that were organized into seven categories: (1) securely provision, (2) operate and maintain, (3) protect and defend, (4) investigate, (5) collect and operate, (6) analyze, and (7) oversight and development.

  In November 2016, NIST issued a draft revision to the framework.[18] Among other things, the revised framework defines work roles[19] within each specialty area and also describes cybersecurity tasks for each work role and the knowledge, skills, and abilities demonstrated by a person whose cybersecurity position includes each work role. The revised framework is intended to enable agencies to examine specific IT, cybersecurity, and cyber-related work roles, and identify personnel skills gaps, rather than merely examining the number of vacancies by job series.

- **OMB Cybersecurity Strategy and Implementation Plan**: In October 2015, OMB issued its *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* to present the results of a comprehensive review of the federal government's cybersecurity (known as the "Cybersecurity Sprint").[20] According to the CSIP, the

[18]NIST, *NICE Cybersecurity Workforce Framework (NCWF), National Initiative for Cybersecurity Education (NICE)*, Draft Special Publication 800-181 (Gaithersburg, Md.: November 2016).

[19]According to NIST, work roles are the most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific knowledge, skills, and abilities required to perform a set of tasks. Some examples or work roles could include an authorizing official, a software developer, or a system administrator.

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

Cybersecurity Sprint identified two key observations related to the federal cybersecurity workforce: (1) the vast majority of federal agencies cited a lack of cyber and IT talent as a major resource constraint that impacts their ability to protect information and assets; and (2) there were a number of existing federal initiatives to address this challenge, but implementation and awareness of these programs was inconsistent. To address these challenges, among other things, the CSIP tasked OPM to provide agencies with information on a number of hiring, pay, and leave flexibilities to help recruit and retain individuals in cybersecurity positions, and called for OMB and OPM to publish a cybersecurity human resources strategy and identify possible actions to help the federal government recruit, develop, and maintain a pipeline of cybersecurity talent.

- **Cybersecurity National Action Plan:** Announced by the White House in February 2016, the *Cybersecurity National Action Plan* was intended to build on the CSIP activities while calling for innovation and investments in cybersecurity education and training to strengthen the talent pipeline. As part of this plan, the fiscal year 2017 President's Budget proposed investing $62 million to, among other things, expand the CyberCorps® Scholarship for Service program to include a CyberCorps Reserve program offering scholarships for Americans who wish to gain cybersecurity education and serve their country in the civilian federal government; develop a cybersecurity core curriculum for academic institutions; and strengthen the National Centers for Academic Excellence in Cybersecurity Program to increase the number of participating academic institutions and expand cybersecurity education across the nation. These initiatives were intended to help the federal government recruit and retain cybersecurity talent with the technical skills, policy expertise, and leadership abilities necessary to secure federal assets and networks well into the future.

- **Federal Cybersecurity Workforce Strategy**: As called for by the CSIP, OMB and OPM issued the *Federal Cybersecurity Workforce Strategy* in July 2016, detailing government-wide actions to identify, expand, recruit, develop, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats.[21] The strategy identified a number of key

[21]OMB and OPM, *Federal Cybersecurity Workforce Strategy*, M-16-15 (Washington, D.C.: July 12, 2016).

actions within four broad goals to address cybersecurity workforce challenges. Table 1 describes the goals of the strategy and associated activities.

Table 1: National Cybersecurity Workforce Strategy Goals, Activities, and Responsible Entities

Goal	Examples of required activities	Responsible entities
1. Identify Cybersecurity Workforce Needs	• educate federal human resources and CIO staff about the revised National Cybersecurity Workforce Framework • expand cybersecurity position coding to capture work roles outlined in the framework, and align those roles with cybersecurity vacancies • conduct strategic workforce planning • work with the private sector to explore trends and anticipate future workforce needs	Office of Personnel Management (OPM), National Initiative for Cybersecurity Education (NICE) partner agencies, other federal agencies
2. Expand the Cybersecurity Workforce through Education and Training	• collaborate with academic institutions to address skill gaps by identifying or promoting existing foundational curriculum that institutions can consult and adopt • provide resources to academic institutions to accelerate and expand cybersecurity education across the nation	Office of Management and Budget, National Security Agency, Department of Homeland Security (DHS), and NICE partner agencies
3. Recruit and Hire Highly-Skilled Cybersecurity Talent	• establish programs to assist federal agencies in their use of existing flexibilities for compensation and explore opportunities for new or revised pay programs for cybersecurity positions • establish a cybersecurity HR Cadre (an expert group of HR professionals from across the government) to execute a model cybersecurity end-to-end hiring process at agencies that is tailored, timely, and a high-quality experience for both applicants and hiring managers	OPM, DHS
4. Retain and Develop Highly Skilled Talent	• develop a common training program for specific categories of cybersecurity professionals • develop career paths that leverage existing programs and responsibilities to deliver on best practices of performance management, talent development, and compensation flexibility, among other things	OPM, DHS

Source: OMB and OPM Federal Cybersecurity Workforce Strategy, M-16-15 (Washington, D.C.: July 12, 2016). | GAO-17-533T

According to OMB's 2016 report on agency implementation of the Federal Information Security Modernization Act of 2014 (FISMA), agencies had made progress in implementing this strategy to address

workforce shortages.[22] Specifically, OMB reported that agencies hired over 7,500 cybersecurity and IT employees in 2016; by comparison, federal agencies hired 5,100 cybersecurity and IT employees in 2015.

These executive branch initiatives include many actions that could help address the challenges of identifying and closing skill gaps, recruiting and retaining staff, and navigating the federal hiring process. While responsible agencies have begun to take action on many of these items, it will be important to continue this momentum if these efforts are to be effectively implemented and foster a significant improvement in the federal cybersecurity workforce.

Recent Laws Address Cybersecurity Workforce Issues

In addition to the aforementioned executive-level initiatives, several recently enacted federal laws include provisions aimed at improving the federal cybersecurity workforce.[23] For example:

- **The Cybersecurity Enhancement Act of 2014** includes provisions intended to address challenges related to recruiting and hiring. Specifically, the law requires the Department of Commerce, National Science Foundation (NSF), and the Department of Homeland Security (DHS), in consultation with OPM, to support competitions and challenges to identify, develop, and recruit talented individuals to perform duties relating to the security of information technology in federal, state, local, and tribal government agencies, and the private sector.[24] The law also calls for NSF, in coordination with OPM and DHS, to continue a federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for federal, state, local, and tribal governments.

- **The Border Patrol Agent Pay Reform Act of 2014** includes provisions intended to improve recruiting and hiring of cybersecurity staff at DHS. Specifically, the law authorizes the Secretary of Homeland Security to establish, as positions in the excepted service,

[22]OMB, *Federal Information Security Modernization Act of 2014 Annual Report to Congress, Fiscal Year 2016* (Washington, D.C.: Mar. 10, 2017).

[23]We have not evaluated whether these actions have been implemented.

[24]Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, (Dec. 18, 2014).

such positions in DHS as the Secretary determines to be necessary to carry out certain responsibilities relating to cybersecurity.[25]

- **The Homeland Security Cybersecurity Workforce Assessment Act (2014)** requires DHS to take certain actions related to cybersecurity workforce planning. Specifically, the Secretary of Homeland Security is to identify all positions in DHS that perform cybersecurity functions and identify cybersecurity work categories and specialty areas of critical need.[26]

- **The Federal Cybersecurity Workforce Assessment Act of 2015** assigns specific workforce planning-related actions to federal agencies.[27] These actions include
  - developing a coding structure to capture the work roles outlined in the revised national cybersecurity workforce framework (OPM, in coordination with NIST); [28]
  - establishing procedures for implementing the coding structure to identify all civilian cybersecurity positions (OPM, in coordination with DHS, NIST, and the Office of the Director of National Intelligence);
  - identifying all IT or cyber positions at agencies, and assigning the appropriate codes to each (federal agencies); and

[25]DHS cybersecurity workforce recruitment and retention provisions were enacted as section 3 of the Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277 § 3,128 Stat. 2995, 3005-3008 (Dec. 18, 2014), 6 U.S.C. § 147.

[26]The Homeland Security Cybersecurity Workforce Assessment Act was enacted as part of the Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277 § 4,128 Stat. 2995, 3008-3010, (Dec. 18, 2014), 6 U.S.C. § 146 note. The act also requires GAO to assess DHS's efforts implementing the cybersecurity workforce initiative and to report on our assessment by December 18, 2017.

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

[28]In October 2012, OPM, in coordination with NIST, published a coding structure for federal cybersecurity positions based on the NCWF. The structure assigns unique numeric codes to each of the seven categories identified in the framework, as well as three new categories. The codes were intended to allow OPM and agencies to identify and categorize all federal cybersecurity positions, laying the groundwork for a consistent government-wide count of the federal cybersecurity workforce. The coding structure that was developed under the Federal Cybersecurity Workforce Assessment Act of 2015 was based on the November 2016 revision of the NCWF.

- identifying IT and cyber-related work roles of critical need, and report these needs to OPM (each federal agency, in consultation with OPM, NIST, and DHS).[29]

The act also requires GAO to analyze and monitor the implementation of the act's requirements and report on this assessment to Congress.[30] We plan to report on the results of our review by no later than December 18, 2018.

Similar to the executive branch initiatives discussed above, these laws call for actions that, if effectively implemented, can address challenges related to skill gaps and recruiting, hiring, and retaining skilled cybersecurity professionals. Further, these laws are an important mechanism to hold agencies accountable for taking action and demonstrating results in building an effective cybersecurity workforce.

Other Ongoing Activities Could Assist Agencies in Recruiting and Retaining Cybersecurity Professionals

Beyond the government-wide initiatives and recently enacted legislation discussed previously, federal agencies have instituted other ongoing activities that may assist the federal government in enhancing its cybersecurity workforce. These include the following, among others:

- **Promoting cyber and science, technology, engineering and mathematics (STEM) education:** A recent presidential commission on cybersecurity highlighted the need for federal programs that support education at all levels to incorporate cybersecurity awareness for students as they are introduced to and provided with Internet-based devices.[31] As an example of such a program, the National Integrated Cyber Education Research Center (NICERC), an academic division of the Cyber Innovation Center funded by DHS, was created to design, develop, and advance both cyber and STEM academic outreach and workforce development programs across the nation.

[29]The act also includes various reporting and other requirements, including that OPM was to submit a progress report on the implementation of the law's requirements related to the coding structure and applying the revised codes by June 2016. OPM submitted this report in July 2016.

[30]Federal Cybersecurity Workforce Assessment Act of 2015, Pub. L. No. 114-113, Div. N, Title III, § 305 (Dec. 18, 2015).

[31]Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (Dec. 1, 2016).

NICERC develops cyber-based curricula for use by K-12 teachers across the country. The curricula developed by NICERC is free to any K-12 educator within the United States and comprises a library of cyber-based curricula that provides opportunities for students to become aware of cyber issues, engage in cyber education, and enter cyber career fields.

- **CyberCorps scholarship:** According to the Partnership for Public Service, one way agencies can increase the supply of cyber talent is through the use of undergraduate and graduate scholarships to promising cybersecurity and STEM students. One such program—the Scholarship for Service program operated by DHS and NSF—provides scholarships and stipends to undergraduate and graduate students who are pursuing information security-related degrees, in exchange for 2 years of federal service after graduation. According to a November 2015 memo from the federal Chief Human Capital Officer Council, since 2000 these scholarships have been awarded to more than 1,650 students. There are also nearly 400 graduating students in related academic programs to meet agencies' cybersecurity needs each year.

- **National Centers of Academic Excellence:** Sponsored by DHS and the National Security Agency, this program designates specific 2- and 4-year colleges and universities as "centers of academic excellence" (CAE) based on their robust degree programs and close alignment to specific cybersecurity-related knowledge units, validated by subject matter experts. Currently, over 200 colleges and universities across 44 states, the District of Columbia, and the Commonwealth of Puerto Rico are designated CAEs for cyber-related degree programs. This program is intended to help institutions of higher education produce skilled and capable cybersecurity professionals and equip students with the necessary knowledge, skills, and abilities needed to protect and defend our nation's infrastructures.

- **National Initiative for Cybersecurity Careers and Studies:** DHS, in partnership with several other agencies, launched the National Initiative for Cybersecurity Careers and Studies (NICCS) in February 2013 as an online resource to connect government employees, students, educators, and industry with cybersecurity training providers across the nation. NICCS provides a catalog of cybersecurity-focused training courses that are delivered by accredited universities, National Centers of Academic Excellence, federal agencies, and other training providers. Each course is mapped to the National Cybersecurity Workforce Framework.

In coordination with a strategic, government-wide approach to improving the workforce, these programs and activities are intended to provide valuable resources for agencies as they attempt to mitigate the shortage of cybersecurity professionals.

In summary, recruiting, developing, and retaining a qualified and competent cybersecurity workforce remains a critical challenge for the federal government. This is highlighted by the ever-evolving nature of the cyber threat and the vulnerabilities that we have identified over the years in agencies' information security programs. The federal government continues to be challenged in key areas—such as identifying skills gaps, recruiting and retaining qualified staff, and navigating the federal hiring process—that are essential to ensuring the adequacy of its cybersecurity workforce. To better equip agencies to adequately protect federal information and information systems from increasingly sophisticated and ever-changing cyber threats, it is critical that a number of our open recommendations be addressed.

Recent federal initiatives and legislation are intended to address the challenges associated with the cybersecurity workforce, and agencies may also be able to draw on other ongoing activities to help assist in mitigating cybersecurity workforce gaps.

If effectively implemented, these initiatives, laws, and activities could help establish the cybersecurity workforce needed to secure and protect federal IT systems.

Chairman Hurd, Ranking Member Kelly, and Members of the Subcommittee, this concludes my statement. I would be pleased to address any questions that you have.

Contact and Staff Acknowledgments

If you have any questions about this statement, please contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov. Other contributors to this statement include Tammi Kalugdan, assistant director; William Cook, analyst-in-charge; Chris Businsky; David Hong; Franklin Jackson; Lee McCracken; Luis Rodriguez; Adam Vodraska; Daniel Wexler; and Merry Woo.

Nick Marinos, U.S. Government Accountability Office

Nick Marinos joined the U.S. Government Accountability Office (GAO) in 2002 and serves as Director of Cybersecurity & Information Management issues within its Information Technology team. As part of his responsibilities in this role, Mr. Marinos manages audit teams that perform government wide and agency-specific cybersecurity, privacy, and information management reviews across all major federal agencies. Mr. Marinos is a certified information privacy professional and holds a Master's in Business Administration and a Bachelor's of Science from Virginia Tech.