STATEMENT OF

ANGELA BAILEY

Chief Human Capital Officer
U.S. Department of Homeland Security

and

RITA MOSS

Director of Human Resources
National Protection and Programs Directorate
U.S. Department of Homeland Security

FOR A HEARING ON

"Cybersecurity Workforce at the Department of Homeland Security"

BEFORE THE

House Committee on Homeland Security
Subcommittees on Cybersecurity, Infrastructure Protection,
and
Oversight and Management Efficiency
U.S. House of Representatives

March 7, 2018

Introduction

Chairman Ratcliffe, Chairman Perry, Ranking Member Richmond, Ranking Member Correa, and distinguished Members of the Subcommittees, thank you for the opportunity to appear before you today to address cybersecurity workforce issues at the Department of Homeland Security (DHS).

We are the Department's Chief Human Capital Officer and Director of Human Resources for the National Protection and Programs Directorate (NPPD). Together, we have over 50 years of experience in federal human resources.

We both support the Department's human capital program, which includes human resources policies and programs; strategic workforce planning and analysis; recruitment and hiring; pay and leave; performance management; employee development; executive resources; employee and labor relations; workforce health and safety; diversity and inclusion; and human resources information technology. We also oversee the human resources operational offices delivering all of the aforementioned services to Headquarters and NPPD employees.

As Secretary Nielsen stated during her November 2017 confirmation hearing, "…one of the most significant [aspects of the Department's mission] for our Nation's future is cybersecurity…The scope and pace of cyberattacks against our federal networks and the control systems that run our critical infrastructure are continually increasing, with attacks growing evermore complex and each more sophisticated than the last. Cyber criminals and nation states are continually looking for ways to exploit our hyper connectivity and reliance on IT systems."

The Department cannot strengthen the Nation's cybersecurity and successfully confront the threats Secretary Nielsen described without the creativity, intellect, and dedication of world-class cybersecurity experts. For that reason, supporting the human capital needs of the Department's cybersecurity workforce is a top priority for senior leadership, including the Secretary.

The Department faces intense competition for cybersecurity talent, and studies continue to make headlines by quantifying current shortages of specific cybersecurity skills and projecting future talent gaps. We recognize the difficulty of securing the right cybersecurity talent today and tomorrow, but we must proceed with urgency and ingenuity. We are committed to thoroughly understanding our workforce requirements and implementing the best possible human capital solutions to recruit, retain, and manage the cybersecurity talent our mission demands. Our teams work closely with human capital and cybersecurity technical leadership across the Department, including within NPPD, and with the Chief Information Officer (CIO), and our Component CIOs on three priorities:

1. *Analyze and Plan* for our complex set of cybersecurity talent needs;
2. *Recruit and Retain* highly qualified employees with capabilities vital to mission success; and
3. *Innovate* by implementing a new 21st century personnel system to revolutionize cybersecurity talent management.

Analyze and Plan

To effectively manage a workforce, one must begin with a comprehensive analysis of mission and talent requirements. We would like to thank Congress for your attention to cybersecurity workforce planning through the passage of several laws since 2014, and we would like to thank the Government Accountability Office (GAO) for their recent review of the Department's implementation of one of those laws, the *Homeland Security Cybersecurity Workforce Assessment Act of 2014*. Emphasizing the importance of these issues helps us focus all of DHS on a path forward.

Over the last decade, DHS has taken a variety of steps to better understand and document our cybersecurity workforce, but as GAO outlined in their February 6, 2018 report (*Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*), there is more work to be done—and done quickly.

As described in the Department's response letter, we concur with GAO's six recommendations, and we have taken a series of actions to address each of them. Each Component designated a lead cybersecurity workforce official, developed updated position coding guidance, and stepped up communications with Component stakeholders critical to ensuring positions are accurately identified, coded, and tracked. Additionally, we continue to engage Component senior leaders through the Cyber Workforce Coordinating Council, comprised of senior membership from both the Component CIO and human resources communities, and the Cybersecurity Technical Review Board, a working-level, cross-Component group to reinforce accountability and awareness. We also reach out quarterly to advise Components of their coding progress, validate coding data, and address problems in an effort to improve our progress and the accuracy of our data in this area.

Notably, the Department's cybersecurity workforce planning efforts and GAO's report focus heavily on the National Initiative for Cybersecurity Education (NICE) Workforce Framework (NICE Framework). NICE, led by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, is a partnership between government, academia, and the private sector working to energize and promote cybersecurity education, training, and workforce development. The NICE Framework is a reference structure that describes the interdisciplinary nature of cybersecurity, and it uses a common, consistent lexicon to categorize and describe cybersecurity work, including information key knowledge, skills, and abilities. In 2013, the Office of Personnel Management (OPM) and NICE began collaborating to ensure agencies could code their federal positions according to the NICE Framework in the human resources information technology (HRIT) systems of shared service providers.

Currently, the Department is focused on transitioning from two-digit position codes based on the original version of the Framework to the new three-digit, role-based position codes aligned to the latest version of the Framework. In doing so, DHS is revising personnel records with our shared service provider (the National Finance Center) that made system updates to accommodate three-digit codes at the end of 2017.

We acknowledge GAO's focus on the importance of coding vacant positions associated with cybersecurity work, and we have charted a path to do so. Fortunately, the Department has

broader efforts underway to ensure accurate documentation of all DHS position requirements, including vacant positions. While DHS does not have an enterprise-wide, automated solution to support such work, we continue to set and refine data standards with Components, patch together multiple datasets, and lay the groundwork for a future solution as part of our Strategic Improvement Opportunities (SIOs) process for the DHS HRIT program. We believe that linking cybersecurity position identification, coding, and tracking with our ambitious position management project will help to accelerate both initiatives.

In the coming months, we have a series of actions planned with Components to ensure they enter, validate, and then analyze their data to determine critical gaps. Ongoing workforce planning efforts have demonstrated that the DHS cybersecurity workforce is complex and varied. We have identified a total population of over 7,400 federal civilian positions, as well as over 2,800 United States Coast Guard military positions and 4,800 contractor positions. The federal civilian population includes 18 Components and organizations and covers over 40 federal occupational series, and all 33 specialty areas of the NICE Cybersecurity Workforce Framework. When we apply the NICE Framework, the most populous category and specialty area codes at DHS—each associated with more than 250 positions/employees—are Investigation, Information Assurance/Compliance, Digital Forensics, Securely Provision, and Operate and Maintain.

Past data calls have identified a great deal of information about Component recruitment and retention challenges and staffing gaps. For the population of 7,400 civilian positions, we are averaging a vacancy rate of 10 percent and an attrition rate of five percent, but in some Components, both rates are regularly above 20 percent. In addition, Components have cited all portions of the NICE Cybersecurity Workforce Framework to describe their current and projected shortages of positions/employees.

DHS must now dig deeper to isolate and monitor priority skills and mission roles, including those where shortages exist or are anticipated. The Framework is a helpful tool for describing critical roles and shortages, but we cannot stop there. Some DHS cybersecurity work is highly specialized, requiring industry, sector, or mission specific skills and knowledge not captured by the Framework's general structures and definitions. In cases where DHS work is unique or specificity is critical to describing the talent needed to meet the Department's mission objectives, DHS will document such detail, and, as appropriate, report it to Congress along with the data elements outlined in statute.

Recruit and Retain

Our understanding of both our current and future workforce needs informs our recruitment and retention strategy. The Department must ensure we are attracting, hiring, and keeping the best cybersecurity talent, and given the competitive cybersecurity labor market, DHS must leverage all available tools to ensure we keep attrition and vacancy rates at acceptable levels. OCHCO has a team dedicated to attracting talent to the Department by improving our employment brand and developing and implementing Department-wide recruitment strategies, to include the use of available hiring flexibilities such as the DHS Schedule A cybersecurity hiring authority and the government-wide IT (information security) direct hire authority.

OCHCO works closely with recruiters and human capital leadership from across Components,

and holds regular meetings of our Corporate Recruiting Council. This Council oversees the creation and monitoring of targeted recruitment plans for specific DHS mission critical occupations, including cybersecurity. As part of a long-term effort to improve cybersecurity recruiting, our staffs manage cybersecurity pipeline development and outreach activities focused on two- and four-year academic institutions, including the National Centers of Academic Excellence in Cyber Defense and Cyber Operations, national and local community organizations, and professional associations. In fiscal year (FY) 2017 and FY 2018 to date, we have engaged with over 1,300 students from 122 academic institutions, including 40 National Centers of Academic Excellence.

In addition, OCHCO operates the Secretary's Honors Program Cyber Student Volunteer Initiative, which offers students temporary assignments in DHS cybersecurity-focused field offices. Approximately 6,500 students from over 400 academic institutions have applied to the program since its inception in 2013, and 258 have completed assignments alongside our cybersecurity professionals. While this is a great starter program, we are enhancing and expanding Component-specific and government-wide programs, such as the Intelligence & Analysis Internship Program and the CyberCorps®: Scholarship for Service program. Now, thanks to Congressional support, all are paid internships that lead to full-time federal/DHS cyber-specific jobs.

Creating interest in DHS cybersecurity work and attracting top applicants is only part of the recruitment equation. Reducing the burden and length of the hiring process for candidates is equally critical. DHS is focusing on hiring process improvement for all occupations, including those related to cybersecurity and information technology. Our teams have worked to gather all available hiring process data to assist Components in identifying barriers, reengineering steps, setting better operational targets, and identifying opportunities for additional automation. We are also focusing on forging smart partnerships across DHS Components, lines of business, and federal agencies to ensure that DHS human resources personnel are aware of leading practices and can collaborate to achieve economies of scale.

One of the key hiring improvement strategies we have deployed is joint recruiting and special hiring events. The Department has held successful joint cybersecurity, veterans, intern and recent graduate events that brought together multiple Components to a single location enabling onsite interviews and on-the-spot tentative job offers in the same day. As a direct result of these events, the Department was able to hire nearly 700 new employees with a reduced time-to-hire. With the cybersecurity event alone, we were able to bring onboard approximately 300 employees, cutting the time-to-hire by up to six weeks in most cases. The Department has also ramped up participation in similar hiring events with federal partners, including the CyberCorps®: Scholarship for Service Job Fair and Federal CIO Council's Federal Tech/Cyber Hiring and Recruitment Event. Based on previous success, the Department will hold another DHS cybersecurity hiring event later this year in Washington, D.C.

Innovative interventions to speed hiring and reduce vacancies are just the first part of a larger Departmental strategy to do cybersecurity human capital better and smarter. Human capital flexibilities are most useful when human resources practitioners understand them and deploy them appropriately to target the Department's most critical job candidates and personnel. We remain committed to ensuring that the DHS human resources community receives additional

cybersecurity-focused training and guidance.

Since 2016, OCHCO has released over 15 simplified guidance documents to help human capital and cybersecurity personnel across the Department understand existing human capital tools, such as direct hire authority and recruitment incentives; dispel myths; and identify how these human capital tools can best support cybersecurity talent. Furthermore, we are working closely with OPM and other DHS Component human resources directors to ensure human resources specialists across DHS stay on the forefront of any new developments and understand the full set of recruitment and retention tools at their disposal. For example, we are building a DHS HR Academy with both formal and informal training as well as rotational and internship opportunities. The Department rolled out the first Academy course in data analytics in the fall of 2017, and we anticipate delivering career path guides by the summer of 2018.

In addition to increased training on all available retention flexibilities, we are working with human capital leadership across Components on specific retention interventions. In 2017, OCHCO built upon successful NPPD practices and released a Department-wide retention incentive plan for cybersecurity employees, which should help Components retain highly skilled talent by financially recognizing the significant training and certification accomplishments of employees. We are also exploring ways to increase the use of student loan repayment and tuition assistance, and with OPM and the rest of the federal human resources community, we are considering possible compensation flexibilities.

Despite current and past efforts, we find that attrition rates for cybersecurity professionals in some DHS organizations remain much higher than the rates for other occupations. Our analysis indicates that work in the field of cybersecurity is increasingly project-based, and we recognize that the prospect of a decades-long federal civil service career may not appeal to cybersecurity professionals. We are passionate about continuing to explore these retention challenges with experts in both human capital and cybersecurity across Components.

Innovate

While we are committed to developing some immediate fixes with DHS human capital and cybersecurity leadership, our primary cybersecurity human capital focus is accelerating the implementation of a new cybersecurity-focused personnel system, which will change the methods, policies and process used to recruit, hire, retain, and develop cybersecurity employees. We believe this will revolutionize how DHS hires, manages, and retains our best cybersecurity talent.

The Department appreciates that Congress passed the *Border Patrol Agent Pay Reform Act of 2014*. Section 3 amended the *Homeland Security Act of 2002* to grant the Secretary the authority to create a cybersecurity focused personnel system exempt from many of the restrictions governing the conventional civil service. This authority allows for a variety of human capital management changes, including alternative methods for defining jobs, conducting hiring, and compensating employees.

Department leadership is aware of the time that has elapsed since the law's passage. We also recognize that implementing such an authority represents new territory and is a significant

personnel transformation for the Department. Successful design, implementation, and maintenance of a new federal personnel system is extremely complex, and requires highly specialized federal human capital expertise. The design and subsequent implementation and execution of such a system all present unique challenges that require technical knowledge related to pay setting and administration, labor market analysis, psychometric research, regulation drafting, change management, etc. Despite these challenges, we are making progress in implementing such a system.

After Congress granted the Secretary this additional authority, the Department began an initial research and analysis process that included benchmarking with other federal agencies, fact finding with the Department of Defense and OPM, and the development of a slate of possible human capital changes. Since both of us arrived at DHS in 2016, we have redoubled the effort to source specialized talent for the project, and OCHCO established a dedicated human capital policy team, which includes a well experienced, senior advisory cadre. We have strengthened the Department's collaboration with OPM, and established regular working meetings between OCHCO, OPM, and the DHS Office of the General Counsel. In addition, the Deputy Under Secretary for Management reinitiated the Cyber Workforce Coordinating Council, which as previously mentioned, includes membership from both the Component CIO and human resources communities.

Our teams have completed research on all the major alternative personnel systems since the 1970s, and by combining leading practices and many new ideas, have designed a flexible, twenty-first century personnel system tailored to the evolving, project-based field of cybersecurity. Our conclusion is that the current civil service system cannot adequately address the cybersecurity talent challenges the Department faces, and making simple modifications or cosmetic changes to the current Title 5, will not suffice.

The General Schedule (GS) was created by the *Classification Act of 1949*, during the Truman Administration, but in reality, many of its foundational principles date back to the *Classification Act of 1923*. The federal workforce is no longer primarily composed of narrowly defined, clerical jobs, and we are not using long tables of clerks or a secretarial pool to combat cybersecurity threats. If we are to attract, hire, compensate, and retain top cybersecurity talent, we need to recognize a variety of truths, including:

- Jobs are becoming increasingly non-standard and complex;
- Employee expectations no longer map to the 30-year federal career; and
- A highly competitive labor market exists for cybersecurity talent—of which the Federal Government is only one employer.

To modernize the civil service for cybersecurity work, we need to revisit some of the foundational theories and structures that underlie how we have managed federal human capital for decades, and we need to update them for the 21st century. Some key shifts include:

- Streamlined, Proactive Hiring
    - 20th Century: Recruitment is focused on posting a position-specific announcement, praying the right candidates apply, allowing candidates to self-rate their skills, and comparing applicants to rigid—often outdated—occupation-based standards
    - 21st Century: Strategically recruit from a variety of sources on an ongoing basis,

and use up-to-date, cybersecurity-focused standards and validated tools to screen, assess, and select talent

- Market-Sensitive Pay
  - 20th Century: GS pay rules are based on tenure, and apply regardless of the field of work
  - 21st Century: Increase the focus on an individual's knowledge, skills, and capabilities and use a pay structure and compensation procedures that are designed with the cybersecurity labor market in mind
- Flexible, Dynamic Career Paths
  - 20th Century: Temporary assignments and details are exceptions to the norm, and static career paths limit advancement to a single occupational series or vertical, tenure-based career ladder
  - 21st Century: Accommodate dynamic careers with streamlined movement between the government and private sector, across Components, and through a variety of permanent/non-permanent assignments
- Development-Focused Performance Management
  - 20th Century: The annual performance assessment is the main opportunity for award and pay progression, and the process has become complex and burdened with paperwork
  - 21st Century: Simplify annual performance ratings, and focus more on continuous, development-focused feedback about employee contributions and skills increases to inform adjustments to pay, assignments, etc.

We are working with the Deputy Under Secretary for Management, the Assistant Secretary for Cybersecurity and Communications, the CIO, and the Cyber Workforce Coordinating Council to finalize the personnel system. The new system will ultimately serve front-line cybersecurity professionals, so it is critical that all interested parties at the Department provide input and have a stake in our shared solution. The Secretary, in coordination with the Acting Director of OPM, is also working to prescribe regulations for the administration of the new system. While we engage in the regulatory process, we are dedicated to a host of technical human capital analysis, policy development, and change management activities to ensure that we launch a system that will be legally defensible, better reflect the needs of high-caliber cybersecurity talent, and enhance the Department's ability to execute its mission.

The implementation effort has momentum, but we are seeking to increase our pace. The cybersecurity threats facing our Nation will not pause while we evolve the Department's approach to cybersecurity human capital. We are committed to making our new cybersecurity service personnel system operational and we would like to increase our collaboration with Congress, including these Subcommittees, to keep you informed of the progress we make and the obstacles we encounter.

Thank you again for your interest in our Nation's cybersecurity and your continued support of the Department's cybersecurity responsibilities and the employees charged with executing them.