EXAMINING DHS'S EFFORTS TO STRENGTHEN ITS CYBERSECURITY WORKFORCE

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

AND THE

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

MARCH 7, 2018

Serial No. 115–52

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

30–788 PDF WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
CLAY HIGGINS, Louisiana
JOHN H. RUTHERFORD, Florida
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
DON BACON, Nebraska
BENNIE G. THOMPSON, Mississippi
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California

BRENDAN P. SHIELDS, *Staff Director*
STEVEN S. GIAIER, *Chief Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
HOPE GOINS, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

JOHN RATCLIFFE, Texas, *Chairman*

JOHN KATKO, New York
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
BRIAN K. FITZPATRICK, Pennsylvania
DON BACON, Nebraska
MICHAEL T. MCCAUL, Texas *(ex officio)*
CEDRIC L. RICHMOND, Louisiana
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
VAL BUTLER DEMINGS, Florida
BENNIE G. THOMPSON, Mississippi *(ex officio)*

KRISTEN M. DUNCAN, *Subcommittee Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND MANAGEMENT EFFICIENCY

SCOTT PERRY, Pennsylvania, *Chairman*

JOHN RATCLIFFE, Texas
CLAY HIGGINS, Louisiana
THOMAS A. GARRETT, JR., Virginia
RON ESTES, Kansas
MICHAEL T. MCCAUL, Texas *(ex officio)*
J. LUIS CORREA, California
KATHLEEN M. RICE, New York
NANETTE DIAZ BARRAGÁN, California
BENNIE G. THOMPSON, Mississippi *(ex officio)*

DIANA BERGWIN, *Subcommittee Staff Director*
ERICA D. WOODS, *Interim Subcommittee Minority Staff Director*

CONTENTS

Page

STATEMENTS

The Honorable John Ratcliffe, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Cybersecurity and Infrastructure Protection:
Oral Statement 1
Prepared Statement 2
The Honorable Scott Perry, a Representative in Congress From the State of Pennsylvania, and Chairman, Subcommittee on Oversight and Management Efficiency:
Oral Statement 4
Prepared Statement 6
The Honorable J. Luis Correa, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Oversight and Management Efficiency:
Oral Statement 3
Prepared Statement 4
The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Chairman, Committee on Homeland Security:
Oral Statement 7
Prepared Statement 8
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Prepared Statement 8
The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas:
Prepared Statement 9
The Honorable Cedric L. Richmond, a Representative in Congress From the State of Louisiana, and Ranking Member, Subcommittee on Cybersecurity and Infrastructure Protection:
Prepared Statement 12

WITNESSES

Mr. Gregory Wilshusen, Director of Information Security Issues, Government Accountability Office:
Oral Statement 14
Prepared Statement 15
Ms. Angela Bailey, Chief Human Capital Officer, Management Directorate, U.S. Department of Homeland Security:
Oral Statement 22
Joint Prepared Statement 23
Ms. Rita Moss, Director, Office of Human Capital, National Protection and Programs Directorate, U.S. Department of Homeland Security:
Oral Statement 28
Joint Prepared Statement 23

APPENDIX

Questions From Chairman John Ratcliffe for Gregory C. Wilshusen 47
Questions From Honorable Ron Estes for Gregory C. Wilshusen 48

Page

Questions From Chairman John Ratcliffe for the Department of Homeland Security 48
Questions From Honorable Ron Estes for the Department of Homeland Security 51

EXAMINING DHS'S EFFORTS TO STRENGTHEN ITS CYBERSECURITY WORKFORCE

Wednesday, March 7, 2018

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY AND
INFRASTRUCTURE PROTECTION, AND
SUBCOMMITTEE ON OVERSIGHT AND
MANAGEMENT EFFICIENCY,
Washington, DC.

The subcommittees met, pursuant to notice, at 2:05 p.m., in room HVC–210, Capitol Visitor Center, Hon. John Ratcliffe [Chairman of the Cybersecurity and Infrastructure Protection subcommittee] presiding.

Present: Representatives Ratcliffe, Perry, Katko, Higgins, Donovan, Garrett, Estes, Fitzpatrick, Correa, Jackson Lee, Langevin, Barragán, and Demings.

Also present: Representative McCaul.

Mr. RATCLIFFE. Good afternoon. The Committee on Homeland Security, Subcommittees on Cybersecurity and Infrastructure Protection and Oversight Management Efficiency will come to order.

The subcommittees are meeting today to examine how the Department of Homeland Security is working to address its cybersecurity work force needs. I now recognize myself for an opening statement.

I would like to begin by thanking our panel for taking the time to be here to testify today. Your thoughts and opinions certainly are important as we oversee the implementation of work force authorities at the Department of Homeland Security.

We have seen cyber attacks affect almost every facet of our daily lives, with sometimes devastating impact. They remind us how vulnerable governments and economies are to the very real threat that our cyber adversaries pose.

As the lead civilian agency for our Federal cybersecurity posture, the Department of Homeland Security is a key piece of this equation, especially the National Protection Programs Directorate. A knowledgeable and skilled cybersecurity work force at DHS is on the front lines of securing our Federal networks and protecting our critical infrastructure.

It is against this backdrop that DHS must compete with the private sector to recruit and to retain the best talent possible, in order to carry out its cybersecurity mission and protect our critical infrastructure. In 2014 Congress passed several pieces of legislation in order to augment the cybersecurity work force at DHS, including

the Homeland Security, Cybersecurity Workforce Assessment Act and the Border Patrol Agent Pay Reform Act.

Among other effects, these laws expanded DHS's hiring authorities and allowed the Department to better recruit and hire qualified cyber professionals. Unfortunately, these new authorities have not yet been fully implemented.

Last month, the Government Accountability Office released a report entitled, "Urgent need for DHS to take actions to identify its position and critical skill requirements." The findings are pretty troubling. While DHS has taken actions to idetify, categorize, and assign employment codes to its cybersecurity positions, its efforts have been neither timely, nor complete.

Identifying DHS work force capability gaps and recruiting to fill them, is a problem that this committee has long examined. However, GAO found that DHS has not identified its Department-wide security or cybersecurity critical needs. Ensuring that DHS collects complete and accurate data on all filled and vacant cybersecurity positions for identification and coding efforts is a task that DHS must not ignore, nor fail to complete. A scatter-shot approach to fulfilling work force needs without comprehensive data to back up those needs is not an effective use of Federal resources.

In fact, there may even be the potential of delaying assistance to critical infrastructure sectors and State and local governments if DHS does not have an adequate amount of cyber workers with the correct skills. At the same time, I am pleased to hear that DHS acknowledged and agreed with all of the recommendations presented by GAO in this report.

DHS will create a periodic review process for cyber roles by the end of next month, and, most importantly, DHS promised to develop Department-wide guidance for identifying areas and positions of critical need by this summer.

While DHS must work to overcome slow hiring processes and work force pipeline issues in order to build the essential work force required to meet its cyber mission, at the end of the day DHS cannot bring people into the hiring pipeline if it does not have accurate accounting of what its current and future needs really are.

NPPD is our Government's premier civilian cybersecurity agency, a distinction that I hope will soon be bolstered by its elevation to the Cybersecurity and Infrastructure Security Agency, with pending legislation over in the Senate.

So let us look at some of the challenges we will be discussing today as collective opportunities to lead together. We must get this right, and I believe that we will.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

MARCH 7, 2018

I would like begin by thanking our panel for taking the time today to testify. Your thoughts and opinions are very important as we oversee the implementation of workforce authorities at the Department of Homeland Security.

We have seen cyber attacks affect almost every facet of our daily lives with devastating impacts, and they remind us of how vulnerable governments and economies are to the very real threat that our cyber adversaries pose. As the lead civilian agency for our Federal cybersecurity posture, the Department of Homeland Security is a key piece of this equation, especially the National Protection and Programs Di-

rectorate. A knowledgeable and skilled cybersecurity workforce at DHS is on the front lines of securing our Federal networks and protecting critical infrastructure.

Against this backdrop, DHS must compete with the private sector to recruit and retain the best talent possible in order to carry out its cybersecurity mission and protect our critical infrastructure. In 2014, Congress passed several pieces of legislation in order to augment the cybersecurity workforce at DHS, including the Homeland Security Cybersecurity Workforce Assessment Act and the Border Patrol Agent Pay Reform Act. Among other effects, these laws expanded DHS's hiring authorities and allowed the Department to better recruit and hire qualified cyber professionals. Unfortunately, these new authorities have not yet been fully implemented.

Last month, the Government Accountability Office released a report entitled "Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements"—and the findings are troubling. While DHS has taken actions to identify, categorize, and assign employment codes to its cybersecurity positions, its efforts have been neither timely nor complete. Identifying DHS workforce capability gaps and recruiting to fill them is a problem this committee has long examined; however, GAO found that DHS has not identified its Department-wide cybersecurity critical needs. Ensuring that DHS collects complete and accurate data on all filled and vacant cybersecurity positions for identification and coding efforts is a task that DHS must not ignore or fail to complete. A scattershot approach to fulfilling workforce needs without comprehensive data to back those needs up is not an effective use of Federal resources. In fact, there may even be the potential of delaying assistance to critical infrastructure sectors and State and local governments if DHS does not have an adequate amount of cyber workers with the correct skills.

At the same time, I am pleased to hear that DHS acknowledged and agreed with all of the recommendations presented by GAO in this report. DHS will create a periodic review process for cyber roles by the end of next month, and, most significantly, DHS promised to develop Department-wide guidance for identifying areas and positions of critical need by this summer. While DHS must work to overcome slow hiring processes and workforce pipeline issues in order to build the essential workforce required to meet its cyber mission, at the end of the day, DHS cannot bring people into the hiring pipeline if it does not have accurate accounting of what its current and future needs are.

NPPD is our Government's premier civilian cybersecurity agency—a distinction that I hope will soon be bolstered by its elevation to the Cybersecurity and Infrastructure Security Agency with pending legislation in the Senate. So let us look at some of the challenges we will be discussing today as collective opportunities to lead together. We must get this right, and I believe that we will.

Mr. RATCLIFFE. The Chair now recognizes the gentleman from California, Mr. Correa, for any statement that he may have.

Mr. CORREA. Thank you, Mr. Chairman. Want to thank you and Chairman Perry for holding this most important hearing today. Of course, I want to thank also our witnesses for being here today. All of you know, watching TV, watching news very frequently. You hear stories about China, Russia, and others targeting our cyber system, including our election system and, of course, our critical infrastructures.

Our National security, our economy, in many ways our daily lives, depend on a stable, safe, and resilient cyber system. The Department of Homeland Security plays a critical role in protecting the Nation's cyber space, which includes not only our own DHS computers but also those belonging to other civilian agencies in our critical infrastructure and, of course, including our collection system.

To fulfill this role, DHS must have cybersecurity work force that is knowledgeable, well-trained, and dedicated to our mission. Sadly and unfortunately, according to the GAO, DHS has not taken the proper and necessary steps to staff the Department with cyber professionals. Specifically, DHS has not identified or reported to Congress on its own Department-wide cybersecurity critical work force

needs. Additionally, according to the GAO, DHS has overstated the number of filled positions.

Without appropriate tracking DHS is not in the position to effectively examine its cybersecurity work force, identify its critical skills gaps or improve its work force planning. DHS has been given a number of tools to help bolster its work force, including special hiring authority, allowing DHS to expedite the hiring process and providing monetary incentives and also a flexible approach to recruiting and retention of cyber experts.

I look forward to speaking with the witnesses today about the specifics of the GAO findings and I want to see how we can move forward and make sure we safeguard America's cybersecurity. Mr. Chair, I yield.

[The statement of Ranking Member Correa follows:]

STATEMENT OF RANKING MEMBER J. LUIS CORREA

MARCH 7, 2018

Almost daily, we learn of nefarious attempts by Russia, China, and others to impact our cyber systems, including election systems and critical infrastructure.

Our National security, our economy, and in many ways our daily lives depend on a stable, safe, and resilient cyber space.

The Department of Homeland Security plays a critical role in protecting the Nation's cyber space, which includes not only DHS's own computer systems and information, but also those belonging to other Federal civilian agencies and our critical infrastructure, including election systems.

To fulfill this role, DHS must have a cybersecurity workforce that is well-trained, resilient, and dedicated to the mission.

However, according to the Government Accountability Office, DHS has not taken the steps necessary to staff the Department with cyber professionals properly.

Specifically, DHS has not identified or reported to Congress on its Department-wide cybersecurity critical workforce needs.

Additionally, according to GAO, DHS overstated the number of filled and vacant cybersecurity positions assigned with the proper identification codes for the specific role.

Without appropriate tracking, DHS will not be positioned to effectively examine its cybersecurity workforce, identify its critical skill gaps, or improve its workforce planning.

President Trump has claimed to be in support of strengthening Federal networks and critical infrastructure, which undoubtedly will require a more robust workforce.

DHS has been given a range of tools to help bolster the cyber workforce, including special hiring authority for cybersecurity positions that allows DHS to expedite the hiring process, provide monetary incentives, and adopt a nimble approach to recruitment and retention.

I look forward to speaking with witnesses today about the specifics of the GAO findings and ways we can move the Department in a positive direction.

Mr. RATCLIFFE. Thank the gentleman. The Chair now recognizes the Chairman of the subcommittee on Oversight and Management Efficiency, the gentleman from Pennsylvania, Mr. Perry, for his opening statement.

Mr. PERRY. Good afternoon. I would like to thank Chairman Ratcliffe for holding this hearing today and including the Oversight and Management Efficiency subcommittee in this very important and timely discussion of the Department of Homeland Security's efforts to strengthen its cybersecurity work force. I also thank the Ranking Member of the subcommittee, Mr. Correa, as well as the witnesses that are willing to be here today.

In today's world our Nation and its critical infrastructure face an increasingly diverse and sophisticated array of cybersecurity threats from both State and non-State actors. Adversaries across

the globe have invested heavily in building out cyber capabilities and have demonstrated an increasing capacity to successfully execute cyber attacks against the United States and our allies.

As the lead civilian agency for securing the Nation's public and private critical infrastructure, which is dependent on IT systems and electronic data, the Department of Homeland Security and its work force play a critical role in protecting the Nation's cyber space.

Given this role, data continuing to show cyber personnel shortages at DHS must remain a top concern for both DHS and this committee. Demand for cyber-related positions continues to outpace the number of individuals qualified to fill them and agencies like DHS must find a way to compete with the private sector in attracting highly-skilled cyber workers.

To address these challenges the committee has passed several pieces of legislation in recent years that were signed into law, providing DHS with additional hiring authorities to better recruit and retain a qualified cyber work force. The Homeland Security Cybersecurity Workforce Assessment Act, enacted into law as part of the Border Patrol Agency Pay Reform Act of 2014, Public Law No. 113–277, required DHS to survey its work force and identify, categorize, and code all vacant and non-vacant cybersecurity positions.

The Act aimed to help DHS assess its current cyber work force in order to identify skills gaps and critical needs and improve strategic work force planning to more effectively recruit, hire, train, and retain cyber personnel. Unfortunately, according to a recent U.S. Government Accountability Office Report, DHS has failed to implement the actions required by this Act in a timely, accurate, or complete manner.

GAO audited 6 components and found that the Department has not met any, any of the deadlines established by the Act. Two-and-a-half years after the statutory deadline to identify the code positions, 3 of the 6 components studied still have not identified all of their cyber positions and, as of August 2017, the Department has only assigned employment codes to 79 percent of its identified cyber positions. Further, while DHS has identified cyber work force capacity and capability gaps, it has not submitted to Congress and the U.S. Office of Personnel Management required reports on critical needs aligned with the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework.

Congress has acted to provide DHS with the tools to help meet the work force needs demanded by the current cyber threat environment. The Department's failure to utilize these tools is unacceptable.

Bureaucratic delays in hiring the personnel needed to secure our Nation's cyber space are detrimental to our National security. Sadly, the failure to properly implement cyber-related hiring authorities is emblematic of the systemic hiring issues continuing to plague the Department.

A management report released by DHS's Office of the Inspector General last fall aptly summarized that the Department and its components continue to encounter significant hiring difficulties related to long hire times and a lack of human resource staff, automated system, and processes to determine needed staff.

Just last week, the Oversight and Management Efficiency Subcommittee heard testimony on the ineffectiveness and delays associated with the Department's fitness determination process, an integral part of the contract work force's on-boarding process.

These problems are especially alarming, given the significant responsibilities facing DHS as it prepares to meet cyber work force needs and undertake the border security-related hiring surge mandated by the President.

I want to thank our panel for testifying this afternoon and I look forward to hearing an update on the Department's implementation of Public Law 113–277's requirements, as well as how DHS's Management Directorate is working with components to improve hiring processes.

I thank you and yield back the balance.

[The statement of Chairman Perry follows:]

STATEMENT OF CHAIRMAN SCOTT PERRY

MARCH 7, 2018

Good afternoon. I would like to thank Chairman Ratcliffe for holding this hearing today and including the Oversight and Management Efficiency Subcommittee in this very important and timely discussion on the Department of Homeland Security's efforts to strengthen its cybersecurity workforce.

In today's world, our Nation and its critical infrastructure face an increasingly diverse and sophisticated array of cybersecurity threats from both state and non-state actors. Adversaries across the globe have invested heavily in building out cyber capabilities and have demonstrated an increasing capacity to successfully execute cyber attacks against the United States and our allies.

As the lead civilian agency for securing the Nation's public and private critical infrastructure, which is dependent on IT systems and electronic data, the Department of Homeland Security (DHS) and its workforce play a critical role in protecting the Nation's cyber space. Given this role, data continuing to show cyber personnel shortages at DHS must remain a top concern for both DHS and this committee. Demand for cyber-related positions continues to outpace the number of individuals qualified to fill them and agencies like DHS must compete with the private sector in attracting highly-skilled cyber workers.

To address these challenges, this committee has passed several pieces of legislation in recent years that were signed into law providing DHS with additional hiring authorities to better recruit and retain a qualified cyber workforce. The Homeland Security Cybersecurity Workforce Assessment Act, enacted into law as part of the Border Patrol Agent Pay Reform Act of 2014 (Public Law 113–277), required DHS to survey its workforce and identify, categorize, and code all vacant and non-vacant cybersecurity positions. The act aimed to help DHS assess its current cyber workforce in order to identify skills gaps and critical needs, and improve strategic workforce planning to more effectively recruit, hire, train, and retain cyber personnel.

Unfortunately, according to a recent U.S. Government and Accountability Office (GAO) report, DHS has failed to implement the actions required by this act in a timely, accurate, or complete manner. GAO audited six components and found that the Department has not met any of the deadlines established by the act. Two-and-a-half years after the statutory deadline to identify and code positions, three of the six components studied still have not identified all of their cyber positions and, as of August 2017, the Department has only assigned employment codes to 79 percent of its identified cyber positions. Further, while DHS has identified cyber workforce capacity and capability gaps, it has not submitted to Congress and the U.S. Office of Personnel Management (OPM) required reports on critical needs aligned with the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework.

Congress has acted to provide DHS with the tools to help meet the workforce needs demanded by the current cyber threat environment. The Department's failure to utilize these tools is unacceptable. Bureaucratic delays in hiring the personnel needed to secure our Nation's cyber space are detrimental to our National security.

Sadly, the failure to properly implement cyber-related hiring authorities is emblematic of the systemic hiring issues continuing to plague the Department. A man-

agement report released by DHS's Office of the Inspector General last fall aptly summarized that the Department and its components continue to encounter significant hiring difficulties related to long hire times and a lack of human resources staff, automated systems, and processes to determine needed staff. Just last week, the Oversight and Management Efficiency Subcommittee heard testimony on the ineffectiveness and delays associated with the Department's fitness determination process, an integral part of the contract workforce's on-boarding process.

These problems are especially alarming, given the significant responsibilities facing DHS as it prepares to meet cyber workforce needs and undertake the border security-related hiring surge mandated by the President.

I want to thank our panel for testifying this afternoon and I look forward to hearing an update on the Department's implementation of Public Law 113–277's requirements, as well as how DHS's Management Directorate is working with components to improve hiring processes.

Thank you and I yield back the balance of my time.

Mr. RATCLIFFE. Thank the gentleman.

The Chair now welcomes and recognizes the Chairman of the full committee, gentleman from Texas, Mr. McCaul.

Mr. MCCAUL. Thank you, Chairman Ratcliffe and Ranking Member Correa for your leadership on this very vital issue. Every day nation-state actors, such as Russia, China, Iran, and other cyber criminals are increasingly hacking into U.S. companies and Government networks to conduct espionage or steal intellectual property.

With tens of millions of Americans relying on computer networks and IT for both personal and professional reasons, the risks apply to almost everyone. Recognizing these threats, I made strengthening the cybersecurity mission at the Department of Homeland Security one of my top priorities as Chairman of the Committee on Homeland Security.

It is an issue that has united both parties. I am proud to say that we have accomplished a great deal. Just this morning, the full committee passed a bill that would strengthen the ability of our cyber response teams to react to attacks on America's critical infrastructure.

This past December, the House approved my landmark bill to create a stand-alone operational organization to elevate the cybersecurity mission of DHS. In recent years, we passed both bills that clarified the cybersecurity roles and authorities between the Department of Homeland Security and OMB, and the FBI and NSA and strengthened the cyber threat information-sharing system with liability protection as well.

In 2014, we passed an important bill to expedite hiring authority at the Department to bolster its cybersecurity work force. At the time, I believe it was made clear that this authority would help combat cyber threats.

I must say though, unfortunately, the Department has never used this hiring authority. This hearing today will focus on some of the reasons for this delay. With the number of threats that continue to gather by the day, I do find this a bit disturbing. One of our responsibilities as Members of this committee is oversight and to make sure that the Department is fully implementing the work force authorities that we provided here in the Congress.

To combat cybersecurity threats, we need DHS to hire the best possible work force because there is just too much at stake. I am hopeful, always in a positive productive way though, that we can learn why this delay has happened.

I look forward to working with the Department as always and other Members of our committee to make sure that these authorities that have been granted the Department are being used.

When it comes to Homeland Security, I think the American people need to have the best possible work force in place. While I do find this delay troubling, I also want to commend all three of you for the work that you do day in and day out at the NCCIC.

I hope I am hearing positive things that the Senate will actually pass our Cybersecurity and Infrastructure Protection Agency Bill which will elevate and prioritize the mission of cybersecurity within the Department.

With that, Mr. Chairman, I yield back.

[The prepared statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

MARCH 7, 2018

Every day nation-state actors, such as Russia, China, and Iran, and other cyber criminals are increasingly hacking into U.S. companies and Government networks to conduct espionage or steal intellectual property.

With tens of millions of Americans relying on computer networks and IT for both personal and professional reasons, the risks apply to almost everyone.

Recognizing these threats, I made strengthening the cybersecurity mission at DHS one of my top priorities as Chairman of the Committee on Homeland Security. It's an issue that has united both parties and I am proud to say we have accomplished a great deal.

Just this morning, the full committee passed a bill that would strengthen the ability of our cyber response teams to react to attacks on America's critical infrastructure.

This past December, the House approved my landmark bill to create a standalone, operational organization to elevate the cybersecurity mission of DHS.

In recent years, we passed bills that clarified the cybersecurity roles and authorities between DHS and OMB, and strengthened cyber-threat information sharing.

And in 2014, we passed important legislation to expedite hiring authority at DHS to bolster its cybersecurity workforce. At the time, it was made clear that this authority would help combat cyber threats.

Unfortunately, the Department has never used this hiring authority. The hearing today will focus on some of the reasons for this delay. With the number of threats that continue to gather by the day, I find this pretty alarming.

One of our responsibilities as Members of this Committee is to make sure DHS is fully implementing the workforce authorities provided by Congress.

To combat cybersecurity threats, we need DHS to hire the best possible workforce. There is too much at stake.

I am hopeful that we can learn why this delay has happened and I look forward to working with DHS and the other Members of our committee to make sure we are using the authorities that have been granted.

When it comes to Homeland Security, the American people need to have the best possible workforce in place.

Mr. RATCLIFFE. Thank the Chairman.

Other Members of the committee are reminded that opening statements may be submitted for the record. We are pleased to have a very distinguished panel of witnesses before us today on this important topic.

[The statements of Ranking Members Thompson and Richmond and Honorable Jackson Lee follow:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MARCH 7, 2018

Recruiting and retaining a qualified cybersecurity workforce at the Department of Homeland Security is a National security imperative.

Every day, we learn more about the efforts of our adversaries—from Russia and Iran to North Korea and China—to use their cyber tools to attack our economy, our critical infrastructure, and the pillars of our democracy, including our election systems.

In the wake of this evolving threat landscape, public and private-sector critical infrastructure owners and operators to look to the Department of Homeland Security's National Protection and Programs Directorate (NPPD) to share information on cyber threats, to provide cybersecurity assessments, and to deploy incident response teams following an incident, among other things.

Yet, when Assistant Secretary for Cybersecurity and Communications Jeanette Manfra testified before this panel last October, she told me that 24 percent of the fully-funded cybersecurity workforce billets at NPPD were unfilled.

In 2014, Congress gave DHS hiring authorities on par with the Department of Defense to address cybersecurity staffing challenges. Although DHS clamored for these authorities for several years prior to 2014, the Department does not plan to fully implement them until April 2019—5 years after Congress authorized expedited hiring.

We cannot afford to waste that kind of time.

Last month, FBI Director Wray, CIA Director Pompeo, NSA Director Rogers, and Director of National Intelligence Coats, DIA Director Ashley, and NGA Director Cardillo all testified before the Senate Intelligence Committee and unanimously agreed that Russia would continue its election meddling efforts into the 2018 mid-term elections.

Last week, NSA Director Rogers again confirmed that the Russian government is actively targeting U.S. election systems.

Secretary of State Tillerson also agrees that the Russians are targeting mid-term elections, yet has not spent any of the funds Congress appropriated to the agency to address the on-going threat to the integrity of our elections.

Congress granted the State Department $120 million to counter Russian election meddling, including $60 million to coordinate anti-propaganda efforts with agencies like the Department of Homeland Security.

That said, NPPD has an important role to play in this space and has, in many ways, stepped up.

I am pleased that it has prioritized services for election administrators, and that all of the 14 requested risk and vulnerability assessments will be concluded by next month.

But I understand that NPPD had to shift resources to complete the assessments, and I am concerned that it will need more resources—and more trained cybersecurity professionals—to meet the on-going obligations of the critical infrastructure subsector designation. As threats to the homeland continue to evolve, NPPD and its partners throughout DHS, will need a strong, qualified cybersecurity workforce.

Congress has given DHS the authorities and structures it needs to develop that workforce, and it is on DHS to implement them. Ultimately, as much as the increased demand for a qualified cybersecurity workforce poses a challenge, it also creates opportunities.

When DHS finally completes the process for coding its cybersecurity workforce, it will be able to target recruiting at more diverse talent pools—from community colleges to veterans' groups. I will be interested in learning what efforts DHS is undertaking to recruit untapped talent, as well as cultivate and retain its workforce.

STATEMENT OF HONORABLE SHEILA JACKSON LEE

MARCH 7, 2018

Chairman John Ratcliffe and Ranking Member Richmond, and Chairman Scott Perry and Ranking Member J. Luis Correa, thank you for this opportunity for the subcommittees to learn more about "Examining DHS's Efforts to Strengthen Its Cybersecurity Workforce."

This hearing will provide Members with an opportunity to hear from officials at the Department of Homeland Security (DHS) and the Government Accountability Office (GAO) about the status of DHS's efforts to identify, recruit, and retain a skilled cybersecurity workforce.

I look forward to the testimony of today's witnesses:

- Gregory Wilshusen, Director, Information Security, Government Accountability Office;
- Angela Bailey, Chief Human Capitol Officer, Management Directorate, Department of Homeland Security; and

- Rita Moss, Director, Office of Human Capital, National Protection and Programs Directorate, Department of Homeland Security.

The cybersecurity field's expanding shortage of professionals with over a quarter-million positions remaining unfilled in the United States alone and a predicted shortfall of 1.5 million cybersecurity professionals by 2019.

The solution must be to grow a greater pool of cybersecurity professionals that are prepared to fill positions within the Federal Government.

The challenge before the Homeland Security Committee is finding the right policy that will accomplish the goal of attracting and retaining cybersecurity professionals within the Federal Government.

I have focused on this problem and have mapped out a comprehensive approach to meeting the underlying problem: Increasing the pool of people who would receive essential education in science, technology, engineering, and mathematics from kindergarten through advanced degree programs.

In 2017, I was pleased to have been awarded the Executive Women's Forum's Women in Cybersecurity Leadership Award for my work in promoting advances in our cybersecurity policy.

CONGRESSWOMAN JACKSON LEE'S LEGISLATIVE EFFORTS TO CLOSE THE CYBERSECURITY WORKFORCE GAP

I introduced in the 114th and again in the 115th a compressive Cyber Security Education and the Workforce Enhancement Act, which seeks to prepare more women and minority students and early stage to mid-career professionals within the Federal Government for cybersecurity jobs. [See accompanying section-by-section]

In this Congress my bill is H.R. 1981, and it amends the Homeland Security Act to establish within the Department of Homeland Security's Office of Cybersecurity Education and Awareness Branch the goals of:

- Recruiting information assurance, cybersecurity, and computer security professionals;
- Providing grants, training programs, and other support for kindergarten through grade 12, secondary, and post-secondary computer security education programs;
- Supporting guest lecturer programs in which professional computer security experts lecture computer science students at institutions of higher education;
- Identifying youth training programs for students to work in part-time or summer positions at Federal agencies; and
- Developing programs to support underrepresented minorities in computer security fields with programs at minority-serving institutions, including Historically Black Colleges and Universities, Hispanic-serving institutions, Native American colleges, Asian-American institutions, and rural colleges and universities.

The goal of H.R. 1981 is to address under-representation of women and minorities in cybersecurity fields of employment.

CYBERSECURITY STATISTICS

In 2016, the Bureau of Labor Statistics reported that African-Americans comprised only 3 percent of the information security analysts in the United States, yet comprise nearly 13 percent of the National population.

Just 2 years ago a security analyst, a position which required a 4-year degree, was paid on average $88,890 per year.

The top computing security salaries range from $175,000 to $230,00 per year.

The most senior position was chief information security officers (CISOs), which typically earns $400,000 or more per year.

In 2017 the United States employed nearly 780,000 people in cybersecurity positions, with approximately 350,000 current cybersecurity employment vacancies.

In 2017, nearly 65 percent of large U.S. companies have a Chief Information Security Officer, up from 50 percent in 2016.

Women hold only 11 percent of cybersecurity positions globally, while filling 25 percent of tech jobs, and comprising 50 percent of the population.

There is a similar situation with African Americans which comprise only 7 percent of the cybersecurity workforce, and Hispanics, who account for 5 percent of cybersecurity positions although they make up 13 percent of the Nation's population.

Finally, two out of three high school students indicate that no one has ever spoken to them about a career in cybersecurity.

These facts mean that we should not have any shortages for computing security jobs, but that these vacancies exist because of barriers to entry like education.

SOLUTION FOR EXPANDING THE FEDERAL CYBERSECURITY WORKFORCE

The solution is expanding the diversity of those who are cybersecurity professionals by tapping human capital already within the Federal Government in new hires or mid-career changes, when we identify that someone has the aptitude and desire to become a computing security professional.

AFRICAN AMERICAN PIONEERS IN COMPUTER SCIENCE

Katherine G. Johnson, of Hidden Figures fame, graduated from college at age 18. In 1952, she began working at NASA in its aeronautics area as a "computer," where she performed the calculations that assured that when astronauts were sent into orbit they could be safely returned to earth.

Roy Clay Sr. is known as the Godfather of Silicon Valley. Mr. Clay was at the cutting edge of computing and technology through his leadership of HP's first foray into the computer market with its 2116A computer.

He was inducted into Silicon Valley Engineering Council's Hall of Fame in 2003.

Mark Dean co-created the IBM personal computer and was instrumental in the development of the company's PC 5150, which was sold to the public in 1981.

Mr. Dean also contributed to the development of the color PC monitor, the first gigahertz chip, and the industry standard Architecture (ISA) system bus.

The personal computers' impact on our world is unmistakable.

In the early days of the computing technology age, computers were only available to governments and large institutional organizations because of their size and complexity.

The age of personal computing has paved the way for mobile computing and handheld computing devices like smart phones.

WOMEN AND THE HISTORY OF COMPUTING

Augusta Ada King-Noel, Countess of Lovelace was an English mathematician and writer, chiefly known for her work on Charles Babbage's proposed mechanical general-purpose computer.

She was the first to recognize that the machine had applications beyond pure calculation, and created the first computer program to give Babbage's machine instructions to carry out a task.

As a result, she is often regarded as the first to recognize the full potential of a "computing machine," and the first computer programmer.

Grace Hopper was an American computer scientist and United States Navy rear admiral, who became the first programmer of the Harvard Mark I computer and she invented the first compiler for a computer programming language.

The Executive Women's Forum (EWF) recognizes the contributions women have made and seeks to expand opportunities for women.

The Executive Women's Forum was founded in 2002, with a mission of inspiring leaders, transforming organizations, and building businesses through education, leadership development, and the creation of trusted relationships.

Today, the EWF has over a thousand members Nation-wide—from emerging leaders to senior executives, all of whom benefit from the organization's programs and events.

EWF members support each other in achieving their goals and advancing their careers by celebrating each other's accomplishments and acknowledging the ideas and contributions of the women around us.

Most notably, each year EWF presents Women of Influence Awards to individuals who have made outstanding contributions in the corporate, Government/academic, and vendor sectors.

The EWF's, "2017 Global Information Security Workforce Study: Women in Cybersecurity" report delivers troubling statistics on areas we are missing the mark in maximizing the participation of women in the cybersecurity workforce.

Fifty-one percent of women report various forms of discrimination in the cybersecurity workforce.

Women who feel valued in the workplace have also benefited from leadership development programs in greater numbers than women who feel undervalued.

In 2016 women in cybersecurity earned less than men at every level.

We know that cybersecurity expertise is a critical component of National security; however, Federal agencies have traditionally struggled to recruit, retain, and manage a robust cybersecurity workforce.

The International Consortium of Minority Cybersecurity Professionals (IC–MCP) launched in 2014 with a mission to bridge this "great cyber divide" in the cybersecu-

rity profession. ICMCP offers programs and services to these groups to assist them in gaining skills and visibility to promote their careers, including:

- Mentoring opportunities for entry and mid-career cybersecurity professionals
- Networking opportunities
- Skills workshops.

In 2015, I was pleased to host the International Consortium of Minority Cybersecurity Professionals for its first meeting held on Capitol Hill.

The vision of ICMCP is to build a pipeline of cybersecurity professionals at all levels, and support them throughout their careers.

ICMCP efforts have the potential to broaden the pool of available experienced cybersecurity professionals.

This Congress I introduced H.R. 1981, the Cyber Security Education and Federal Workforce Enhancement Act, which creates programs to support underrepresented minorities in computer security fields.

I understand that the supply of educated and certified cybersecurity professionals is too few when compared with the thousands of positons that are in need of them.

As a result, talented candidates can demand higher salaries, more flexible hours, and other benefits that are incompatible with the Federal hiring process.

Priorities within the workforce have also changed.

For instance, millennials change employers more frequently than their predecessors and place a high value on flexible work schedules and professional development opportunities.

I strongly believe that we have untapped talent within the Federal workforce, and we have potential pools of talented young people who are in underrepresented communities around the Nation that we must reach during their formative education to prepare them for potential cybersecurity careers.

We are not supporting DHS with a policy that would allow the agency to pursue talent regardless of where it might be found.

So long as DHS attempts to compete for cybersecurity talent in the same market where the private sector businesses are competing, the results will not change.

We must be creative and engage in broader thinking that does not limit our view of who can be a cybersecurity professional.

POTENTIAL FOR DHS TO SUCCEED IN RECRUITMENT AND RETENTION OF CYBERSECURITY PROFESSIONALS

The 2017 Global Information Security Workforce Study: Women in Cybersecurity issued by the Executive Women's Forum, stresses what we already know; some segments of the workforce are underrepresented—in the cybersecurity field. Women professionals make up only 11 percent of the cybersecurity workforce despite the escalating growth in the field.

The participation of women in cybersecurity is at 11 percent although women reported higher levels of education.

These underrepresented groups offer an opportunity to increase the cybersecurity workforce in the near and long term.

This is important because both Gen Y and Gen Z have significant numbers of minorities who could significantly close the cybersecurity gap.

I look forward to working with the Chair and Ranking Members on how H.R. 1981 might offer a path toward increasing diversity in the Federal cybersecurity workforce.

Thank you.

STATEMENT OF RANKING MEMBER CEDRIC L. RICHMOND

MARCH 7, 2018

Since this is our third hearing on cyber workforce, I assume that most of us understand the gravity of failing to fill cybersecurity vacancies throughout the Federal Government and, in particular, at DHS. So, let me start by saying the same thing I have said at the last three hearings——

First, if we're serious about "right-sizing" the Federal Government's cyber workforce we need to look beyond 4-year universities. There is untapped talent in unconventional places, and we will find it if we look for it.

Second, we need strong and consistent leadership from the White House. The President must come out and say that the cybersecurity posture of the Federal Government has a direct impact on our economy, our National security priorities, our critical infrastructure, and even the integrity of our elections.

And finally, we have to improve morale at DHS so it can recruit and retain that cybersecurity talent it needs to carry out its mission.

With respect to DHS's cyber workforce, Congress has been responsive. We heard DHS when it told us that it was having trouble competing with the private sector for top cyber candidates, and in 2014 we gave DHS the authority for faster, more flexible hiring.

But we also realized that DHS can't manage what it doesn't measure—so, we directed it to perform a three-step process to assess its own cybersecurity needs:

Step 1—identify its cybersecurity positions;

Step 2—bring those positions into alignment with formal OPM data standards, so it can track where cyber positions are located within the Department and start to address skills gaps;

And Step 3—identify any areas where there are serious gaps in workforce capabilities, or areas of "critical need."

This assessment is supposed to inform a comprehensive cybersecurity workforce strategy that includes a multi-phased recruitment plan—targeting a range of potential candidates from experienced professionals, the unemployed, and disadvantaged communities—to build a more robust cyber workforce at DHS. This workforce strategy would, in turn, inform the broader Department-wide Cybersecurity Strategy required under legislation I authored in 2015.

But DHS has yet to complete its cybersecurity needs assessment and the deadlines for both these strategies has long passed—yet neither strategy has been delivered to Congress. In fact, this is the third Congressional hearing where I have asked about the status of the Department-wide Cybersecurity Strategy that was due in March 2017.

I expect that today, I will hear the same excuses I have heard every other time I have asked about the DHS Cybersecurity Strategy: DHS plans to release the strategy soon, but the new leadership—and there is, once again, new leadership—needs a chance to review it. As much as I understand the need to let the new administration set its own policy, we cannot ignore the fact that these delays are undermining DHS's ability to carry out its mission.

Moreover, I am troubled by the length of time we are being asked to wait for the reports we need to do our job as authorizers. Despite these on-going challenges, I look forward to a productive discussion about how we can work together to make sure DHS has the tools, resources, and authorities to maintain a qualified cybersecurity workforce—and do so in a manner that is timely and responsive to Congress.

Mr. RATCLIFFE. Mr. Greg Wilshusen is the director of information security issues for the Government Accountability Office. He leads cybersecurity and privacy-related audits of the Federal Government and critical infrastructure. Thank you for taking the time, for being here from what I am sure is very busy caseload.

Ms. Angela Bailey is the chief human capital officer in the Management Directorate at DHS. Ms. Bailey came to DHS from the Office of Personnel Management. I look forward to hearing how OPM and DHS can work more in unison on cyber work force issues.

Finally, Ms. Rita Moss is the director of the office of human capital at the National Protection and Programs Directorate at DHS. She attended the United States Naval Academy. We thank her for her service there and thank you for being here before our committees today.

I would now ask all three of our witnesses to stand and raise your right hand so I can swear you in to testify.

[Witnesses sworn.]

Mr. RATCLIFFE. Let the record reflect that the witnesses have answered in the affirmative. You all may be seated. The witnesses' full written statements will appear in the record.

The Chair now recognizes, Mr. Wilshusen for 5 minutes for an opening statement.

STATEMENT OF GREGORY WILSHUSEN, DIRECTOR OF INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Ratcliffe, Chairman Perry, Chairman McCaul, and Ranking Member Correa. Thank you for the opportunity to appear at today's hearing to discuss the Department of Homeland Security's efforts to strengthen its cybersecurity work force.

My testimony is based on a report we issued last month on DHS's actions to identify and report on cybersecurity positions and specialty areas of critical need, as called for by the Homeland Security Cybersecurity Workforce Assessment Act of 2014.

Before I proceed, if I may, I would like to recognize members of the audit team who were instrumental in developing my statement and conducting the work underpinning it. Tamika Lutin and David Hong who are with me today, led this work while Chris Carrey, Ben Atwater, Alexander Andreg, Wayne Emillion, and Louis Rodriguez made significant contributions.

DHS has made important progress in identifying, categorizing, and assigning the employment codes to its cybersecurity positions. For example, as of December 2016, it reported identifying about 10,725 positions.

However, the Department's actions have neither been timely nor complete. Procedures established by DHS to perform these activities were issued 13 months past the due dates specified into 2014 Act and did not include steps for identifying position vacancies as the act required.

The act also required DHS to assign employment codes created by OPM to all of its cybersecurity positions. This action was to be completed by September 2015. However, as of August 2017, 23 months after the due date, the Department had not completed the coding assignment process.

In August 2017, the Office of Personnel Management reported to Congress that DHS had coded 95 percent of the Department's identified cybersecurity positions. Yet, we determined that only 79 percent of the positions were coded. The 95 percent estimate was overstated because DHS excluded uncoded vacant positions.

DHS has taken steps to identify its work force capability gaps and reported these to Congress in March 2017. However, it did not identify or report to Congress its critical cybersecurity critical needs using the work categories and specialty areas defined in the National cybersecurity framework. In addition, the Department has not annually reported its critical needs to OPM as required and has not developed plans with clearly-defined time frames for reporting.

To assist the Department, we made six recommendations in our February report. For example, we recommended that DHS develop procedures on how to identify and code vacant cybersecurity positions and develop guidance for identifying specialty areas of critical need.

To help clarify responsibility and provide accountability, we recommended that the Department identify for each component the individual who is responsible for leading the component's efforts and in performing the work force assessment activities. We also

recommended that each component's procedures for identifying and coding cyber positions be reviewed to ensure consistency with Departmental guidelines. DHS concurred with our recommendations and estimated that it would implement them all by June, 2018.

Implementing our recommendations should better position the Department in meeting the requirements of the Homeland Security Cybersecurity Workforce Assessment Act and help DHS to better understand its needs for recruiting, hiring, developing, and retaining the cybersecurity work force with the skills necessary to accomplish the Department's varied and essential cybersecurity mission.

Until it does, DHS may lack assurance that it has the data necessary to effectively manage the recruitment and retention of a cybersecurity work force that is responsible for protecting departmental and Federal networks as well as the Nation's critical infrastructure from cyber threats.

This concludes my opening statement. I would be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

MARCH 7, 2018

Chairmen Ratcliffe and Perry, Ranking Members Richmond and Correa, and Members of the subcommittees: Thank you for the opportunity to appear at today's hearing to discuss the Department of Homeland Security's (DHS) efforts to strengthen its cybersecurity workforce. In its important role of securing the Nation's cyber space, DHS is responsible for protecting the confidentiality, integrity, and availability of its own computer systems and information, and for leading the coordination with partners in the public and private sectors to protect the computer networks of Federal civilian agencies and the Nation's critical infrastructure from threats. As such, having an effective cybersecurity workforce is essential to accomplishing the Department's mission.

Toward ensuring that it has an effective workforce, the *Homeland Security Cybersecurity Workforce Assessment Act of 2014* (hereafter referred to as "the act")[1] required 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 employment code to each cybersecurity position.[2] The act also required DHS to identify and report on its cybersecurity workforce areas of critical need.

In addition to the aforementioned requirements for DHS, the act included a provision for GAO to analyze and monitor the Department's efforts to address its requirements. My testimony today provides an overview of our recently-issued (February 2018) report, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*, based on our review of the its efforts.[3]

In preparing this statement, we relied on our work supporting the February report. This work included comparing the Department's actions to identify, categorize, and assign employment codes to its cybersecurity positions and to identify its cybersecurity workforce areas of critical need with the required activities specified in the act. We analyzed that information, including data on the coding of cybersecurity workforce positions, and also administered a data collection instrument to six com-

---

[1] The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* 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.

[2] The employment codes are standard codes for Federal job classifications that were developed by the Office of Personnel Management (OPM), in alignment with the *National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework*. See Office of Personnel Management, *The Guide to Data Standards* (Washington, DC: November 15, 2014).

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

ponents of DHS.[4] Further, we interviewed relevant officials from the DHS Office of Chief Human Capital Officer (OCHCO) and from the selected DHS components. We also interviewed relevant officials at the Office of Personnel Management (OPM).

The work on which this statement is based was conducted in accordance with generally accepted Government auditing standards, which require audits to be planned and performed 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 such a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

DHS leads the Federal Government's efforts to secure our Nation's public and private critical infrastructure information systems against cyber threats. As part of these efforts, cybersecurity professionals can help to prevent or mitigate the vulnerabilities that could allow malicious individuals and groups access to Federal information technology (IT) systems. The ability to secure Federal systems depends on the knowledge, skills, and abilities of the Federal and contractor workforce that designs, develops, implements, secures, maintains, and uses these systems.

The Office of Management and Budget 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.[5] This shortage may leave Federal IT systems vulnerable to malicious attacks. Experienced and qualified cybersecurity professionals are essential in performing DHS's work to mitigate vulnerabilities in its own and other agencies' computer systems and to defend against cyber threats.

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.[6] We have also identified a number of 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.[7] 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.

Federal Initiative and Guidance Are Intended to Improve Cybersecurity Workforces

In recent years, the Federal Government has taken various steps aimed at improving the cybersecurity workforce. These include establishing a National initiative to promote cybersecurity training and skills and developing guidance to address cybersecurity workforce challenges.

Founded in 2010, the National Initiative for Cybersecurity Education (NICE) is a partnership among Government, academia, and the private sector, and is coordinated by the National Institute of Standards and Technology (NIST). The NICE mission promotes cybersecurity education, training, and workforce development in coordination with its partners. The initiative's goal is to increase the number of skilled cybersecurity professionals in order to boost National IT security.

In 2013, NICE published the *National Cybersecurity Workforce Framework* to provide a consistent way to define and describe cybersecurity work at any public or private organization, including Federal agencies.[8] In 2014, OPM developed guidance for assigning 2-digit employment codes for each cybersecurity work category and specialty area identified in the 2013 NICE framework.[9] Federal agencies can use

---

[4] The six components we reviewed are: Departmental Management and Operations, National Protection and Programs Directorate, Science and Technology Directorate, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, and U.S. Secret Service.

[5] Office of Management and Budget, *Federal Cybersecurity Workforce Strategy*, Memorandum M–16–15 (Washington, DC: July 12, 2016).

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

[7] GAO, *Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges*, GAO–17–533T (Washington, DC: Apr. 4, 2017).

[8] National Institute of Standards and Technology, *NICE Cybersecurity Workforce Framework* (Version 1.0) (Gaithersburg, MD: April 2013).

[9] Office of Personnel and Management, *The Guide to Data Standards* (Washington, DC: November 15, 2014).

the codes to identify cybersecurity positions in personnel and payroll systems, such the system of the National Finance Center.[10]

To further enhance efforts to strengthen the cybersecurity workforce, NICE subsequently revised the framework in 2017 to include 33 cybersecurity-related specialty areas organized into 7 categories—securely provision, operate and maintain, protect and defend, investigate, collect and operate, analyze, and oversee and govern. The revision defined work roles in specialty areas and cybersecurity tasks for each work role,[11] as well as the knowledge, skills, and abilities that a person should have in order to perform each work role.[12] Also, in 2017, OPM issued guidance creating a unique 3-digit employment code for each cybersecurity work role.[13] In October 2017, NIST issued guidance that reflected the finalized 2017 NICE framework and included a crosswalk of OPM's 2-digit employment codes to the 3-digit codes.[14]

DHS's Cybersecurity Workforce Performs a Wide Range of Critical Missions

DHS is the third-largest department in the Federal Government, employing approximately 240,000 people, and operating with an annual budget of about $60 billion, of which about $6.4 billion was reportedly spent on IT in fiscal year 2017. In leading the Federal Government's efforts to secure our Nation's public and private critical infrastructure information systems, the Department, among other things, collects and shares information related to cyber threats and cybersecurity risks and incidents with other Federal partners to enable real-time actions to address these risks and incidents.

The Department is made up of 15 operational and support components that perform its critical mission functions. Table 1 describes the 6 components that we included in our review.

DHS Component	Description
U.S. Customs and Border Protection (CBP)	CBP is to safeguard America's borders, thereby protecting the public from dangerous people and materials while enhancing the Nation's global economic competitiveness by enabling legitimate trade and travel. CBP's cybersecurity workforce primarily protects the component's internal systems, networks, and data.
Departmental Management and Operations (DMO)	DMO is to provide support to the Secretary and Deputy Secretary in the overall leadership, direction, and management of DHS and all of its components. DMO is responsible for DHS's budgets and appropriations, expenditure of funds, information technology systems, facilities and equipment, and the identification and tracking of performance measurements. DMO's cybersecurity workforce is to develop and implement DHS's cybersecurity-related workforce policies and programs and protect DHS's systems, networks, and data. As part of DMO, the Office of Chief Human Capital Officer (OCHCO) is responsible for personnel policy development and implementation. The Office of the Chief Information Officer, among other things, is to develop and implement information security programs.

[10] The National Finance Center personnel and payroll systems are used by DHS and other agencies for processing personnel and payroll information. In addition, they are DHS's system of record for employment codes assigned to cybersecurity employees.

[11] National Institute of Standards and Technology, *NICE Cybersecurity Workforce Framework*, Special Publication 800–181 (Gaithersburg, MD: August 2017).

[12] According to the National Institute of Standards and Technology, work roles are the most detailed groupings of IT, cybersecurity, or cyber-related work. Examples of work roles include an authorizing official, a software developer, or a system administrator.

[13] Office of Personnel Management, *Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions* (Washington, DC: Jan. 4, 2017).

[14] National Institute of Standards and Technology, *OPM Federal Cybersecurity Coding Structure* (Gaithersburg, MD: Oct. 18, 2017).

DHS Component	Description
National Protection and Programs Directorate (NPPD)	NPPD is expected to protect and enhance the resilience of the Nation's physical and cyber infrastructure, working with partners at all levels of government and the private and nonprofit sectors, to share information and build greater trust to make physical and cyber infrastructure more secure. NPPD is the lead component for fulfilling the Department's National, non-law enforcement cybersecurity missions, as well as providing crisis management, incident response, and defense against cyber attacks for Federal Government networks.
U.S. Secret Service (USSS)	USSS is to protect designated protectees, investigate threats against protectees, as well as investigate financial and computer-based crimes; it is also expected to help secure the Nation's banking and finance critical infrastructure. USSS's cybersecurity workforce primarily conducts criminal investigations and protects its systems, networks, and data.
Science and Technology Directorate (S&T)	S&T is to conduct basic and applied research, development, demonstration, testing, and evaluation activities relevant to DHS. S&T's cybersecurity workforce is expected to conduct cybersecurity research and development for the Homeland Security Enterprise, and protect its systems, networks, and data.
U.S. Citizenship and Immigration Services (USCIS)	USCIS is responsible for overseeing lawful immigration to the United States. Its mission is to provide accurate and useful information to USCIS customers, grant immigration and citizenship benefits, promote an awareness and understanding of citizenship, and ensure the integrity of National immigration system. USCIS's cybersecurity workforce primarily protects its systems, networks, and data.

Source.—GAO analysis of DHS information./GAO–18–430T

DHS Is Required to Assess Its Cybersecurity Workforce

The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* required DHS to perform workforce assessment-related activities to identify and assign employment codes to its cybersecurity positions. Specifically, the act called for DHS to:

1. Establish procedures for identifying and categorizing cybersecurity positions and assigning codes to positions (within 90 days of law's enactment).
2. Identify all filled and vacant positions with cybersecurity functions and determine the work category and specialty area of each.
3. Assign OPM 2-digit employment codes to all filled and vacant cybersecurity positions based on the position's primary cybersecurity work category and specialty areas, as set forth in OPM's *Guide to Data Standards*.[15]

In addition, after completing the aforementioned activities, the act called for the Department to take steps to identify and report its cybersecurity workforce areas of critical need. Specifically, DHS was to:

4. Identify the cybersecurity work categories and specialty areas of critical need in the Department's cybersecurity workforce and report to Congress.
5. Submit to OPM an annual report through 2021 that describes work categories and specialty areas of critical need and substantiates the critical need designations.

The act required DHS to complete the majority of these activities by specific due dates between March 2015 and September 2016.

Within DHS, OCHCO is responsible for carrying out these provisions, including the coordination of the Department's overall efforts to identify, categorize, code, and report its cybersecurity workforce assessment progress to OPM and Congress.

[15] At the time the *Homeland Security Cybersecurity Workforce Assessment Act of 2014* was enacted, DHS was to use OPM's 2014 data standards guide (Office of Personnel Management, *The Guide to Data Standards* (Washington, DC: November 2014). The purpose of the guide is to help agencies identify and code their cybersecurity positions. Employment codes can be used in human capital systems to measure areas of critical need.

DHS HAS NOT FULLY IDENTIFIED CYBERSECURITY POSITIONS OR ASSIGNED EMPLOYMENT CODES IN A COMPLETE AND RELIABLE MANNER

The act required DHS to establish procedures to identify and assign the appropriate employment code, in accordance with OPM's *Guide to Data Standards*, to all filled and vacant positions with cybersecurity functions by March 2015.[16] In addition, DHS's *April 2016 Cybersecurity Workforce Coding* guidance states that components should ensure procedures are in place to monitor and to update the employment codes as positions change over time.[17]

Further, the *Standards for Internal Control in the Federal Government* recommends that management assign responsibility and delegate authority to key roles and that each component develop individual procedures to implement objectives. The standards also recommend that management periodically review such procedures to see that they are developed, relevant, and effective.[18]

DHS OCHCO developed Departmental procedures in May 2014 and recommended implementation steps for coding positions with cybersecurity functions for the Department's components. However, OCHCO did not update its procedures to include information on identifying positions and assigning codes until April 2016—13 months after the due date specified by the act.

In addition, the procedures were not complete because they did not include information related to identifying and coding vacant positions, as the act required. Moreover, the Departmental procedures did not identify the individual within each DHS component who was responsible for leading and overseeing the identification and coding of the component's cybersecurity positions.

Further, although components were able to supplement the Departmental procedures by developing their own component-specific procedures for identifying and coding their cybersecurity positions, OCHCO did not review those procedures for consistency with Departmental guidance. The Department could not provide documentation that OCHCO had verified or reviewed component-developed procedures. In addition, OCHCO officials acknowledged that they had not reviewed the components' procedures and had not developed a process for conducting such reviews.

OCHCO officials stated that several factors had limited their ability to develop the procedures and to review component-developed procedures in a timely and complete manner. These factors were: (1) A delayed Departmental decision until April 2016 as to whether certain positions should be considered cybersecurity positions; (2) a belief that each component had the best understanding of their human capital systems, so procedure development was best left up to each component; (3) a condition where each of the six selected DHS components recorded and tracked vacant positions differently; and (4) cybersecurity specialty areas for vacant positions were not known until a position description was developed or verified and a hiring action was imminent. Without assurance that procedures are timely, complete, and reviewed, DHS cannot be certain that its components have the procedures to identify and code all positions with cybersecurity functions, as required by the act.

Accordingly, our February 2018 report included recommendations that DHS: (1) Develop procedures on how to identify and code vacant cybersecurity positions, (2) identify the individual in each component who is responsible for leading that component's efforts in identifying and coding cybersecurity positions, and (3) establish and implement a process to periodically review each component's procedures for identifying component cybersecurity positions and maintaining accurate coding.[19] DHS concurred with the recommendations and stated that it would implement them by April 30, 2018.

DHS Has Not Yet Completed Required Identification Activities

The act required DHS to identify all of its cybersecurity positions, including vacant positions, by September 2015. Further, the act called for the Department to use

---

[16] Office of Personnel Management, *The Guide to Data Standards* (Washington, DC: November 15, 2014). OPM guidance created unique 2-digit employment codes for categories and specialty areas identified in the NICE framework.

[17] U.S. Department of Homeland Security, Office of the Chief Human Capital Officer, *Cybersecurity Workforce Coding* (Washington, DC: April 22, 2016).

[18] GAO, *Standards for Internal Control in the Federal Government*, GAO–14–704G (Washington, DC: Sep 10, 2014).

[19] GAO–18–175.

OPM's *Guide to Data Standards* to categorize the identified positions and determine the work category or specialty area of each position.[20]

As of December 2016, the Department reported that it had identified 10,725 cybersecurity positions, including 6,734 Federal civilian positions, 584 military positions, and 3,407 contractor positions.[21] Nevertheless, as of November 2017, the Department had not completed identifying all of its cybersecurity positions and it had not determined the work categories or specialty areas of the positions. In explaining why the Department had not identified all its positions, OCHCO officials stated that components varied in reporting their identified vacant positions because the Department did not have a system to track vacancies.

Of the 7 work categories and 33 specialty areas in the NICE framework, DHS reported that its 3 most common work categories were "protect and defend", "securely provision," and "oversight and development;" and its 2 most common specialty areas were "security program management" and "vulnerability assessment and management." However, DHS could not provide data to show the actual numbers of positions in each of these categories and specialty areas.

According to OCHCO officials, the Department was still in the process of identifying positions for the 2-digit codes and would continue this effort until the 3-digit codes were available in the National Finance Center personnel and payroll system in December 2017. At that time, OCHCO officials stated that the Department intends to start developing procedures for identifying and coding positions using the 3-digit codes.

DHS Has Not Completely and Accurately Assigned Employment Codes

The act also required DHS to assign 2-digit employment codes to all of its identified cybersecurity positions. This action was to be completed by September 2015.[22]

However, as of August 2017—23 months after the due date—the Department had not completed the coding assignment process. Although, in August 2017, OPM provided a progress report to Congress containing DHS data which stated that 95 percent of DHS-identified cybersecurity positions had been coded,[23] our analysis determined that the Department had assigned cybersecurity position codes to approximately 79 percent of its identified Federal civilian cybersecurity positions.[24] The primary reason for this discrepancy was that DHS did not include the coding of vacant positions, as required by the act. Further, OCHCO officials stated they did not verify the accuracy of the components' cybersecurity workforce data. Without coding cybersecurity positions in a complete and accurate manner, DHS will not be able to effectively examine its cybersecurity workforce; identify skill gaps; and improve workforce planning.

Thus, in our recently-issued report, we recommended that OCHCO collect complete and accurate data on all filled and vacant cybersecurity positions when it conducts its cybersecurity identification and coding efforts. DHS concurred with the recommendation and stated that, by June 29, 2018, it intends to issue memorandums to its components that provide instructions for the components to periodically review compliance and cybersecurity workforce data concerns to ensure data accuracy.

DHS HAS NOT IDENTIFIED OR REPORTED ITS CYBERSECURITY WORKFORCE AREAS OF CRITICAL NEED

According to the act, DHS was to identify its cybersecurity work categories and specialty areas of critical need in alignment with the NICE framework and to report this information to the appropriate Congressional committees by June 2016. In addition, a DHS directive required the DHS chief human capital officer to provide guidance to the Department's components on human resources procedures, including identifying workforce needs.[25]

---

[20] Office of Personnel Management, *The Guide to Data Standards* (Washington, DC: November 15, 2014). OPM guidance outlined categories and specialty areas in alignment with the NICE framework.

[21] Department of Homeland Security, *Comprehensive Cybersecurity Workforce Update: 2016 Report* (Washington, DC: March 16, 2017).

[22] Identification and code assignment is inclusive of both filled and vacant positions with cybersecurity functions.

[23] Office of Personnel Management, *Progress Report on the National Cybersecurity Workforce Measurement Initiative* (Washington, DC: August 3, 2017). This report was 20 months late. OPM officials stated that they did not meet the December 2015 deadline because DHS had not provided sufficient data at that point.

[24] Per DHS's August 2017 coding progress dashboard, 5,298 of 6,734 identified positions had been coded. Vacant position coding progress was not provided.

[25] Department of Homeland Security, *Human Capital Line of Business Integration and Management*, Directive No. 258–01 (Feb. 6, 2014).

As of February 2018, the Department had not fulfilled its requirements to identify and report its critical needs. Although DHS identified workforce skills gaps in a report that it submitted to Congressional committees in March 2017, the Department did not align the skills gaps to the NICE framework's defined work categories and specialty areas of critical need.

In September 2017, OCHCO developed a draft document that attempted to crosswalk identified Department-wide cybersecurity skills gaps to one or more specialty areas in the NICE framework. However, the document did not adequately help components identify their critical needs by aligning their gaps with the NICE framework because it did not provide clear guidance to help components determine a critical need in cases in which a skills gap is mapped to multiple work categories.

According to OCHCO officials, DHS had not identified Department-wide cybersecurity critical needs that aligned with the framework partly because OPM did not provide DHS with guidance for identifying cybersecurity critical needs. In addition, OCHCO officials stated that the components did not generally view critical skills gaps in terms of the categories or specialty areas as defined in the NICE framework, but instead, described their skills gaps using position titles that are familiar to them. In the absence of relevant guidance to help components identify their critical needs, DHS and the components are hindered from effectively identifying and prioritizing workforce efforts to recruit, hire, train, develop, and retain cybersecurity personnel.

DHS also did not report cybersecurity critical needs to OPM in September 2016 or September 2017, as required. Instead, the Department first reported its cybersecurity coding progress and skills gaps in a March 2017 report that it sent to OPM and Congress to address several of the act's requirements.[26] However, the report did not describe or substantiate critical need designations because DHS has not yet identified them.

Additionally, DHS had not developed plans or time frames to complete priority actions—developing a DHS cybersecurity workforce strategy and completing its initial cybersecurity workforce research—that OCHCO officials said must be completed before it can report its cybersecurity critical needs to OPM. According to OCHCO officials, the report that the Department submitted to Congress in March 2017 had contained plans and schedules. However, we found that the March 2017 report did not capture and sequence all of the activities that DHS officials said must be completed in order to report critical needs. Until DHS develops plans and schedules with time frames for reporting its cybersecurity critical needs, DHS may not have insight into its needs for ensuring that it has the workforce necessary to carry out its critical role of helping to secure the Nation's cyber space.

In our report, we recommended that DHS: (1) Develop guidance to assist DHS components in identifying their cybersecurity work categories and specialty areas of critical need that align to the NICE framework and (2) develop plans with time frames to identify priority actions to report on specialty areas of critical need.[27] DHS concurred with the recommendations and stated that it plans to implement them by June 2018.

In summary, DHS needs to act now to completely and accurately identify, categorize, and assign codes to all of its cybersecurity positions, and to identify and report on its cybersecurity workforce areas of critical need. Implementing the six recommendations we made in our February 2018 report should better position the Department to meet the requirements of the 2014 act. Further, doing so will help DHS understand its needs for recruiting, hiring, developing, and retaining a cybersecurity workforce with the skills necessary to accomplish the Department's varied and essential cybersecurity mission.[28] Until DHS implements our recommendations, it will not be able to ensure that it has the necessary cybersecurity personnel to help protect the Department's and the Nation's Federal networks and critical infrastructure from cyber threats.

Chairmen Ratcliffe and Perry, Ranking Members Richmond and Correa, and Members of the subcommittees, this concludes my statement. I would be pleased to respond to your questions.

Mr. RATCLIFFE. Thank you, Mr. Wilshusen.

The Chair now recognizes Ms. Bailey for 5 minutes.

---

[26] Department of Homeland Security, *Comprehensive Cybersecurity Workforce Update: 2016 Report* (Washington, DC: March 16, 2017).

[27] GAO–18–175.

[28] GAO–18–175.

STATEMENT OF ANGELA BAILEY, CHIEF HUMAN CAPITAL OFFICER, MANAGEMENT DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. BAILEY. Good afternoon Chairman Ratcliffe, Chairman Perry, Ranking Member Richmond, and Ranking Member Correa, and distinguished Members of the subcommittees. Thank you for the opportunity to appear before you today to address cybersecurity work force issues at the Department of Homeland Security.

As Secretary Nielsen described during her November 2017 confirmation hearing, cyber attacks against our Federal networks and the control systems that run our critical infrastructure are continually increasing, with attacks growing ever more complex and each more sophisticated than the last. Cyber criminals and nation-states are continually looking for ways to exploit our hyper-connectivity in reliance on IT systems.

Our enemies will not rest and neither will we. 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 work force is a top priority for senior leadership including me. I recognize the difficulty of securing the right cybersecurity talent today and tomorrow. But we must proceed with urgency and ingenuity. I am committed to thoroughly understanding our work force requirements and implementing the best possible human capital solutions to recruit, retain, and manage the cybersecurity talent our mission demands.

My team and I are working closely with human capital and cybersecurity leadership across the Department, including the National Protection and Programs Directorate, the DHS chief information officer, and our component CIOs on three priorities.

No. 1, analyze and plan for our complex set of cybersecurity talent needs. No. 2, recruit and retain the highly-qualified employees with capabilities vital to mission success. No. 3, innovate by implementing a new 21st-Century personnel system to revolutionize cybersecurity talent management.

I am working with the deputy undersecretary for management, the assistant secretary for cybersecurity and communications, the CIO, and the Cybersecurity Workforce Coordinating Council to finalize the personnel system. The Secretary in coordination with the 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 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. I am committed to making our new cybersecurity personnel system operational. I would like to increase our collaboration with Congress, including these subcommittees, to keep you informed to the progress.

Thank you, again, for our continued support of the Department's cybersecurity responsibilities and the employees charged with executing them. I look forward to your questions.

[The joint prepared statement of Ms. Bailey and Ms. Moss follows:]

JOINT PREPARED STATEMENT OF ANGELA BAILEY AND RITA MOSS

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 cyber attacks against our Federal networks and the control systems that run our critical infrastructure are continually increasing, with attacks growing ever more 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 2-digit position codes based on the original version of the Framework to the new 3-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 3-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 under way 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. On-going 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 5 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 2- and 4-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 2017 and fiscal year 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 on-site 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 on board approximately 300 employees, cutting the time-to-hire by up to 6 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, DC.

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 H.R. 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 1970's, and by combining leading practices and many new ideas, have designed a flexible, 21st 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 on-going 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.

Mr. RATCLIFFE. Thank you, Ms. Bailey.

The Chair now recognizes Ms. Moss for 5 minutes.

STATEMENT OF RITA MOSS, DIRECTOR, OFFICE OF HUMAN CAPITAL, NATIONAL PROTECTION AND PROGRAMS DIRECTORIATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. MOSS. Chairman Ratcliffe, Chairman Perry, Ranking Member Correa, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today.

The Department of Homeland Security serves a critical role in safeguarding and securing cyber space, a core homeland mission. DHS's National Protection and Programs Directorate, NPPD leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure.

I am the human resources director for NPPD, with almost 25 years of leadership experience in Federal human capital. I came to DHS just over a year ago. In this role I am responsible for planning, developing, directing, and evaluating NPPD's human capital strategy and operations.

As a component of DHS, we are very much aligned with the Department's approach and guidance in effectively recruiting and retaining cybersecurity talent, which is in high demand in Government as well as in the private sector and is a key imperative of the NPPD mission.

NPPD has been working closely with the Department in developing systems and programs to effectively recruit and retain cybersecurity talent. We are thoroughly engaged at every level in the design and development of the new personnel system for cyber positions.

NPPD is represented at the SES level by our deputy assistant secretary for cybersecurity and communications who co-leads the Cybersecurity Workforce Coordinating Council. I support the council as NPPD's human capital expert.

NPPD cybersecurity managers and employees at the working level are also engaged in numerous working groups and focus groups to inform the design and impact of the new system. We believe that our needs are well-represented and our input is valued.

In my role as H.R. director for NPPD, I have made data analytics a priority. As an organization, we cannot figure out where we are going, what barriers exist or develop effective solutions without first understanding what is working and what is not working in our efforts to recruit and retain cyber talent.

Over the last year, we have invested a lot of energy and effort in developing our metrics such as stats on internal movement, location of lag times in hiring, grade distribution, et cetera, and analyzing our processes. We are now utilizing that data to determine what gaps exist and develop new strategies to address them.

NPPD has also been very adept and creative in leveraging the various authorities granted to us as well as existing OPM regulations and workplace flexibilities to attract and retain our talent. We are actively exercising various hiring authorities such as direct hire, internships, and noncompetitive hiring, incentive programs such as student loan repayment, and retention incentives and recruitment strategies such as social media and on-site interviewing to attract and retain our cyber work force. We will continue to do

so and provide those insights into the development of the new personnel system.

I want to conclude my testimony by thanking the committee for passing the Cybersecurity and Infrastructure Security Agency Act of 2017. Earlier today, your colleagues in the Senate took the next step to move this bill forward. If enacted, this legislation will mature and streamline NPPD. Importantly, it will rename our organization to clearly reflect our essential mission.

Establishing our brand under a renamed agency is essential to our work force, our recruitment efforts and effective stakeholder engagement. We must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future.

We appreciate this committee's leadership. Thank you for your interest in growing and developing the Nation's cybersecurity work force. I look forward to your questions as well.

Mr. RATCLIFFE. Thank you, Ms. Moss.

We will turn now to questions from the Members. The Chair now recognizes the gentleman from Virginia, Mr. Garrett for 5 minutes.

Mr. GARRETT. Thank you, Mr. Chairman.

I am incredibly frustrated and I have a finite amount of time and Mr. Wilshusen, I presume I am close to pronouncing that correctly. You are going to miss the brunt of this because you are from GAO.

You attended the Naval Academy. You understand the concept that a leader is responsible for all unit he accomplishes or fails to accomplish, right? They taught that in the Army leadership. I am sure the Navy is no different.

Ms. Bailey, you said our enemies will not rest and neither will we. But as I look at this list of GAO findings, there were at least 395 nights that we went to bed and rested before we accomplished items on this list.

So you have people on this committee—Ms. Demings, who has a carrier in law enforcement, so too Mr. Higgins. Chairman McCaul, he was a Federal prosecutor. Mr. Perry, he was in the military. We have an FBI agent. I was in the military and was a prosecutor and I can darn guarantee you that there were a lot of nights that we had stuff that we were mandated to do that we didn't go to bed. That we literally didn't rest because we were mandated to do it.

So while I look at Public Law 13277, and I look at these bullets, established procedures to identify and categorize and cybersecurity positions within 90 days March 2015, 13 months behind. Identify all positions with cyber functions and determine specialty areas within 9 months, still incomplete. Assign 2-digit codes to all cybersecurity positions based on priority work category within 9 months, incomplete.

Identify cybersecurity—and this is from September 2015, identify cybersecurity work rules to the critical needs of Congress, June, 2016, not yet identified. There is one more. Report critical needs to OPM annually, assigned September 2016. Not yet addressed.

Now, I got a series of questions for each of you and again you escaped this. Again, thank you for your service, right? I know what you do isn't easy, but if our enemies aren't resting and they are not. I just was fortunate enough to meet with the foreign ministers from the Baltic States, right—Estonia, Latvia, Lithuania—who understand something about cyber attacks.

I have spoken with people from the Ukraine who understand something about cyber attacks. I understand that there are a lot of people who really concerned with things like EMP. The reality is as you all know; a cascading cyber threat could kill 50 percent of the population in this country in 12 months.

I am not making this stuff up. So these are the laws passed by Congress under the Constitution of the United States and here are my questions. I am going to give them to you in a litany and then give each of you time.

What is your level of accountability? What is your fear if you miss a date that's established by law? What is the worst thing you think can happen? When was the last time someone was fired for not accomplishing a task mandated by law?

I am dead serious. I want to know who and what did they fail to do? Has anyone who is previously responsible for a legally-mandated task subsequently been promoted after having failed to accomplish that task in a timely manner?

I am dead serious. Because in the world from which I come as a prosecutor, as an elected official, and as a soldier, you get an assignment with a drop-dead date and you do the assignment. You guys are great. I apologize that my enmity is attacking you. But we serve the American people. These threats are not anything to worry about until they happen. So has anyone who is responsible for one of these tasks that haven't been accomplished subsequently been promoted, who failed to accomplish the task and what were they promoted to? Why?

So, again, what is your level of accountability? What is your greatest fear that could happen possibly if you don't do something Congress directs you by law to do? Have we promoted anyone who failed to accomplish these tasks?

What do we intend to do to be more responsive in the future? I hate to think that it is like being the parent to a 17-year-old who goes, "Yes, sir, I will do it." Then never does it and giggles behind your back.

Because Congress is supposed to matter and I think in our hearts we want the same thing. So I got—I am sorry about 45 seconds for each of you.

Thank you for you indulgence. I am not—and again, it is not a personal attack. But I mean you get it. You all know this is wrong, 13, 16, 18 months out.

Ms. BAILEY. I was scrambling to write down your questions, sir. So I don't fully——

Mr. GARRETT. OK. Well, here is my biggest one. Has anyone failed to accomplish a legally-mandated task by virtue of Public Law 13277 been subsequently promoted?

Ms. BAILEY. No, sir.

Mr. GARRETT. Has anyone ever been fired for failure to make a time line mandated by law by Congress?

Ms. BAILEY. No.

Mr. GARRETT. So what is the greatest fear of an individual who is tasked with these particular responsibilities should they fail to accomplish that task? What is their fear? I won't get promoted. In the Army it was I want a good evaluation, so that I can get promoted ahead of my peers.

What is the fear of someone who goes home one night thinking, well, I am not going to finish this today knowing that it is past the deadline?

Ms. BAILEY. I think if I could answer it this way. I don't know that it is fear. I think it is actually just disappointment that they don't have the ability to perhaps get everything done in a given day that they try to get it done.

So they have got a lot of competing priorities sitting on their plate. This is by far one of their most important. But they have to do that in context of everything else that they are trying to do at the same time.

So the very same work force that is trying to do the coding and which by the way we have as of today over 6,000 positions are coded into 3-digit. I realize that that is not the substantial progress that you are looking for, but——

Mr. GARRETT. I don't want progress. Pardon, I don't try to be mean to you and I know I am over. I want completion by the assigned date or you coming to us going here is why we are not going to finish in time.

Ms. BAILEY. Understand, Sir.

Mr. GARRETT. Again, I am not trying to beat you guys up.

Ms. BAILEY. We have a time——

Mr. GARRETT. I know it is not easy.

OK, again, I thank the Chair for his indulgence. But please take this sense of urgency. This is a bipartisan thing where we are protecting the same people. We need to be better about holding you to account and you need to be better about looking at this timing going, "Darn, this is hard. We are going to get it done."

Because that is what we do in law enforcement, that is what we do in the military, that is what our teachers do when they are first year teachers, lesson planning. It is what we owe all the citizens we serve.

Thank you. Apologize for going over.

Mr. RATCLIFFE. The gentleman yields back.

The Chair recognizes the gentleman from California, Mr. Correa.

Mr. CORREA. Thank you, Mr. Chairman.

Just a question to DHS, my colleague stated the issues and I, we have given you flexibility. We have given you incentives to hire folks, to get people on-line, to fill these vacancies.

Ms. Bailey, you pointed out there is a lot of—it sounds like you don't have the resources, individuals that are supposed to execute just aren't getting around to executing. I am not going to put words in your mouth, but my question to you is what other resources do you need to fill these vacancies?

Of course, the other question if you can, there are some errors I would imagine, errors in coding of some of these positions. Do we know how many vacancies we actually have?

Ms. MOSS. Ms. Bailey, please.

Ms. MOSS. In terms of hiring, I looked at our numbers right before while preparing for this. Over the last 2 years, we have approximately 1,077—I am sorry, 1,087 cyber positions.

We actually hired over 500 during that time frame. So we were actually hiring a lot of people throughout the course of the last few years. We also are suffering attrition along with the rest of the

cyber work force in Government and out of Government. So although hiring is occurring, attrition is also occurring. So it is not that we are not hiring individuals. We are also trying to overcome the deficit——

Mr. CORREA. That is a plausible explanation.

Ms. MOSS. Yes.

Mr. CORREA. So my question is: How do we get you over? How do we help you get there to make sure that we are fully staffed in this critical area of Government?

Ms. MOSS. I am not certain that any new legislation is needed. We are implementing, as Ms. Bailey said, new cyber talent management system I think will give us more flexibilities. We are also hiring people that are younger interns that we are growing and developing within the organization.

So, I think that will help shape our work force. When NPPD first stood up, the urgency was to hire people that are competent and skilled. There is a limited number of people that are competent and skilled in cyber talent. So now, we are trying to grow people from within by hiring people at lower grade level——

Mr. CORREA. Ms. Moss and Ms. Bailey, I am not going to put any words in your mouth, but it sounds to me that you are going through a growth process here.

Ms. MOSS. Yes.

Mr. CORREA. It is still going to take time to get there?

Ms. MOSS. We are growing, yes.

Mr. CORREA. It is a critical area and we are still going to have some problems getting there. What about the issue of miscoding on some of these positions? Do we actually know how many positions are vacant? Or is that something that is still a floating number out there?

Ms. MOSS. We actually know how many positions are vacant. We are in the process now of updating our coding to the 3-digit code. So, we are training our managers in how to use the new NICE framework to code their positions so that is under way currently as we speak.

Mr. CORREA. The same question to the GAO, sir. In your opinion, what can we do to speed up hiring of some of these folks to see these most important positions that we need to have filled right away?

Mr. WILSHUSEN. Well, I think one of the first things is to identify what your critical needs are to make sure that you are hiring the right people with the——

Mr. CORREA. Prioritizing?

Mr. WILSHUSEN. Skills that you need. Prioritizing——

Mr. CORREA. Can we do that? Or is that——

Mr. WILSHUSEN. Well, that is one of the things that have yet to be done——

Mr. CORREA. Has failed to be done.

Mr. WILSHUSEN [continuing]. To identify the specialty areas of critical need. So, I think that is going to be key, it's being able to know what type of staff, what type of skillsets do you need and then go out and try to hire them. Recognize that is going to be challenging in terms of hiring those types of individuals because

they are in demand, not only across Federal agencies, but also in the private sector.

So it is going to really be imperative to make sure that we know exactly what type of individual with the skillsets that we need in order to accomplish our mission. That is one of the steps that DHS still needs to do.

Mr. CORREA. I would like to look at both of these agencies, come up with a list of recommendations to what is it that we need to do to help you get there to finish your job. Again, this is not a finger pointing, but rather trying to figure out what the bottlenecks are and trying to move past them.

Mr. Chair, I yield the remainder of my time.

Mr. RATCLIFFE. Thank the gentleman.

The Chair now recognizes the gentleman from Pennsylvania, Mr. Perry.

Mr. PERRY. Thanks, Mr. Chairman.

Ms. Bailey, I am looking at some information from the GAO study here that says that as a requirement of the act of 2014, you are supposed to—your agency is supposed to assign the 2-digit employment codes and that as far as I can tell for this, it is still ongoing.

Now, I understand there is subsequent legislation that requires a 3-digit code. So in light of that, are you still trying to assign the 2-digit codes or have you abandoned that and now are moving to the 3-digit code? Or is there a reason to have both? Or is that——

Ms. BAILEY. Yes, sir. So the 3-digit code builds off the 2-digit code and what it does is it just makes it a further refinement, I think is the best way to describe this.

Mr. PERRY. OK.

Ms. BAILEY. So the 2-digit code work has continued, always will continue. What we are doing is refining that by adding in the 3-digit code.

Mr. PERRY. So when you say—I just want to understand this, so when you say always will continue, does that mean it will never be done or——

Ms. BAILEY. Correct. Our cyber work force as people move in and out, as positions move in and out, as our enemy comes up with new and advanced ways of doing things, we are always going to be redefining what it is to be cybersecurity.

Mr. PERRY. OK. I agree with you and I get that. I figured that would be your answer. But at some point you have a base of information and then you are modifying from that to keep up with the current times, right? I mean——

Ms. BAILEY. Correct.

Mr. PERRY. So to me, at some point, everything is going to be assigned to 2- or 3-digit code, everything. Then you are going to have to change it to keep up.

Ms. BAILEY. Right.

Mr. PERRY. So my question is when is that going to happen, because the due date was September 2015 for the 2-digit code. It is March 2018 right now, so——

Ms. BAILEY. Right. We have assigned—we actually, I just want to clarify something. Although, we have not been provided I think what you would say formal guidance in everything, we have been

at this since 2011. So we meet in almost a monthly basis in working with the components to put together the kinds of guidance that they actually need, which is why Ms. Moss is able to continue on. They are not sitting around waiting on formal guidance.

So by April, the end of April, 2018, which is to be next month, this Department will have all of its cyber positions coded under the 3-digit code. We have a commitment to do that. We have talked to both the DAS and the under secretary within management along with component leadership. Everybody understands that this is something that we have got to finalize by April 2018.

Mr. PERRY. So we are talking about at the end of April, because we are talking a month away.

Ms. BAILEY. Yes.

Mr. PERRY. Less than a month away.

Ms. BAILEY. Correct.

Mr. PERRY. So you are saying at the end of April this is not going to be an issue.

Ms. BAILEY. At the end of April.

Mr. PERRY. At least this component of it.

Ms. BAILEY. Correct.

Mr. PERRY. Which is, well, I think it is way too long. I empathize with Mr. Garrett's position because I feel the same way. It just takes too long. We had a hearing last week regarding the hiring practices, including for cybersecurity positions and as it relates to the fitness determination as a part of the on-boarding process.

What I came away with is that the Department—this is my impression, for whatever reason has some aversion to the risk of hiring somebody. If there is anything at all that is flagged, they just drag their feet.

The contractor can't find out what the problem is. Nobody knows what the fitness standard is. There is nothing published. It is amorphous, it changes from position to position. It costs the American taxpayer a huge amount of money. It puts everybody further and further behind. The cybersecurity issue is an issue, believe it or not, I imagine other Members do, I go home to my district and people ask me about it. They are concerned about it and then they want to know what they can do and what is being done. Quite honestly, I don't have a lot of good answers for them.

So, what I also got out of that hearing is that there is nothing required legislatively for the Department to change its procedures and practices. I see absolutely no reason why the contracting officer needs to be involved in that part of the process, right?

The contracting officer makes sure that the contract is fit and the contractor is performing the work as appropriate. He doesn't need to be involved, he or she doesn't need to be involved in the hiring process, yet, a would-be contractor has to go to them to find out what the issue is. Why they can't hire somebody.

They go to somebody else and then they come back and they say, "Well, we can't tell you. And we don't know when it is going to get better and we can't tell you why." Why can't you? Why can't you—you are the CHCO, right? That's the chief human capital officer.

Ms. BAILEY. Yes.

Mr. PERRY. You are the CHCO.

Ms. BAILEY. Right.

Mr. PERRY. Why can't you just change that and streamline that? That we put you in charge because you are smart, you are capable, and you can make decisions. Why is that not happening?

Ms. BAILEY. Well, if it is contractors, it doesn't actually fall under my——

Mr. PERRY. But the process, the process of hiring.

Ms. BAILEY. Right. So the process of hiring, yes, does fall under me, but I partner with our chief security officer with regard to that.

Mr. PERRY. OK. Who is in charge, you or the security officer?

Ms. BAILEY. With regard to the security process, it would be Rich McComb, our chief security officer. But we have partnered, I will tell you in the 2 years since I have been at DHS, we have issued reciprocity guidance that has gone out to everyone.

We are now at the 70 to 80 percent of our cases in which we can do reciprocity. We actually do it. We have issued guidance to say that if somebody is not going to be able to pass their security clearance and you know that, then revoke the offer and move on to the next——

Mr. PERRY. But this is before the clearance, right? This is before the—this is fitness. These are the fitness standards. I forget the other one, one is for contractors and one for employees.

Ms. BAILEY. Right.

Mr. PERRY. With all due respect, the hearing I had last week tells me that whatever process you implemented 2 years ago is not sufficiently working. With all due respect.

Ms. BAILEY. OK.

Mr. PERRY. So I would invite you to revisit that. I am happy to have a discussion with you.

Mr. Chairman, I yield.

Mr. RATCLIFFE. Chair now recognizes the gentlelady from Florida, Ms. Demings, for 5 minutes.

Mrs. DEMINGS. Thank you so much, Mr. Chairman.

Thank you to our witnesses for being here. It is a tough job. But I do share the sense of urgency with my colleagues. It is an important job. I was in another place this morning talking about we have enemies in this country who spend every waking minute trying to figure out how they can defeat our systems, and so this is an important work.

Ms. Bailey, you indicated that you are not sitting around waiting for guidance, but I would think that some guidance would be helpful in terms of recruiting and training and retaining, preparing our current work force. So could you please describe for the committee any guidance that has been developed and dispersed at the Department to assist in identifying cyber work force needs?

Ms. BAILEY. Yes. I mean, what I should have said is the components weren't sitting around waiting for formal guidance. But with regard to the guidance, we have actually, in working with the Human Capital Leadership Council, we have put out several, at least 15 different pieces of guidance quite frankly on what are all the hiring authorities that you can use today, what are some of the best recruiting methods that we can actually use, how do we go ahead and retain these folks given the authorities that we currently have in place today, what are the things that we know that

we need to actually implement with regard to our new personnel system and where we want to go.

So we actually have been holding design sessions with the subject-matter experts along with the hiring, or the H.R. specialists to actually make sure that we are identifying what the specific needs are, because we do know what our critical needs are. We have over 33 different specialty areas that have been identified for cybersecurity, which ranges within 40 different occupations.

We are using a 21st-Century NICE framework of coding and then we have to take that after we code these positions. We have to turn around and try to recruit, hire, and pay people on a first part of the 20th-Century system, because the two aren't actually matched together. So while we have all this good coding that is going on every hearing, and it is absolutely critical and it is important, we have to live in the system in which we have to operate until today.

So when I go out and we try recruit somebody, we have a question that we ask ourselves all the time. How are you going to get top talent when in some cases if they have a bachelor's degree they are only equivalent to a GS–5, which means that I can only pay them about $3 more than the minimum wage in most States.

So we are absolutely going to have a recruiting problem when we have those kinds of pay scales associated with the GS schedule, which is why we have put a tremendous amount of effort into designing this new personnel system that we plan to roll out in the very near future. We have to go through the regulatory process, make sure that everything is aligned. We have briefed OMB on it. We have briefed the CIO council at the White House on it. We brief OPM on it next week. So we are making significant——

Mrs. DEMINGS. So you are encouraged by the new process that you hope to roll out very soon.

Ms. BAILEY. I am extremely encouraged, because what we have done, as we have said, we live in a 21st-Century world. We can no longer just put Band-Aids on a 20th-Century system and call it a day, because it is not working. So if we are going to do all this work over here in coding in the 21st-Century codes, which make absolutely perfect sense, makes no sense to me whatsoever that we have to turn around and try to recruit, hire, and retain and pay people in a system that was designed in the 1940's. So those are some of the things that we are actually working on together to make sure that we can get implemented.

Mrs. DEMINGS. Ms. Moss, anything you would like to add to that statement?

Ms. MOSS. I would say in terms of actual operations, that is certainly true. We have a hard time. We do leverage OPM flexibilities in terms of recruitment incentives, retention incentives, but that is a paper process. There are a lot of hoops to jump through so that elongates our hiring process. So we have found workarounds, but we are looking for a long-term solution, which we are going to get with the new system that is being developed.

Mrs. DEMINGS. OK.

Thank you, Mr. Chairman. I yield back.

Mr. RATCLIFFE. I thank the gentlelady.

Chair now recognizes the gentleman from New York, Mr. Donovan, for 5 minutes.

Mr. DONOVAN. Thank you, Mr. Chairman.

You answered most of my questions just now, because the Chairman held a roundtable with some other people from industry a while back. We had folks from Microsoft, Intel, Facebook, Google, a couple of other companies. Just to put things in perspective, you are talking to a guy whose VCR still flashes 12, so I do not understand any of this stuff.

But they told us the difficulty they are having recruiting. They have 500,000 jobs right now that they cannot fill and I think in 10 years it will be a million. They are looking to start trying to get interest in young people into the jobs that are going to be needed to be filled by industry. I can't even imagine how difficult it is for you to recruit at the pay scales.

In some places and many of my colleagues here have served in the military and military seems to have difficulty, but some incentives to retain talent in especially special areas that are needed. Is there a category for like essential services in our Government that we could get out of the GS classification ratings and say this is a need that we have to fill? And maybe we don't follow those protocols.

As you said, Ms. Bailey, that was set up in 1940. Is there a mechanism in place now for that?

Ms. BAILEY. Well, actually Congress gave us—thank you—gave us that authority to actually write our own rules. So what we are doing right now is we are completely not just reinvigorating, we are redesigning and stepping away from the traditional classification and qualification system, because it does not work for what we are trying to hire today.

I would tell you, with respect to the military, in fact, NPPD has over a 50 percent of NPPD's staff in this area are veterans, so that is remarkable. It is a highly sought-after source for us to recruit from, is from the veteran population.

But thank you to the Congress we do have the authority now to go ahead and actually do what you are suggesting, because we are never going to be able to make the significant progress we want to make by putting another step on the GS, right, or by raising something by just one degree. That is never going to work. You have to re-think.

First of all, the talent we are trying to hire does not want a 30-year career with the Federal Government. They just don't. That is OK. So we have to figure out ways to have legislation, which it wouldn't necessarily take for in the competitive side. But with our new authority that we have been given, we are actually baking into that disability for folks to go in and out of Government without having to be restrained by time in grade and all the ridiculous rules that folks are under these days, that really actually is a detraction for them to actually want to come back into the Government.

We want them to work for us for 3 to 5 years. We want them to leave and go to the companies that you just mentioned. But then we want to stay in touch with them and we want to bring them back, so that we can have this infusion of both private sector and

Federal sector, and that is what our new personnel system will actually allow us to do.

Mr. DONOVAN. The other thought I had was possibly if industry, again, is having their own difficulties in recruiting. But I do not know if you would call it on a loan basis or something, but the real talented people whose are getting paid these very reasonable salaries in the private sector would be able to come in and work for their Government as a—I do not want to say a loaner from J.P. Morgan, but a program where we could take some talent from industry and for some, whether it is a love of country or whatever incentive we could give companies to loan us some of their talented people to help us in some of the things that you are dealing with might be another idea.

Mr. Chairman, after Ms. Bailey I will yield the remainder of my time.

Yes, Ms. Bailey, would you comment on that?

Ms. BAILEY. I was just going to say that, yes, like the Loaned Executive Program is something that we use. We also bring folks into what is called IPA, which is basically academic talent and stuff. So there are different hiring authorities that we can use to have an infusion of that talent come in and we do make use of those, so thank you.

Mr. DONOVAN. Wonderful. Thank you very much.

I yield the remainder of my time, Mr. Chairman.

Mr. RATCLIFFE. I thank the gentleman.

Chair now recognize the gentlelady from Texas, Ms. Sheila Jackson Lee, for 5 minutes.

Ms. JACKSON LEE. I thank the Chairman very much and I appreciate very much this particular hearing.

I want to thank the full committee, the subcommittee Chair, and subcommittee Ranking Member and full committee Chair and full committee Ranking Member on working with me on my zero-day legislation, which I think is the underpinning of what we are talking about in terms of having that staff, that experienced staff to deal with the ultimate events that may happen both in the public sector and the private sector, and having them be qualified and having a continuing channeling of staff.

I would like to—staff personnel that are dealing with the issue of cybersecurity, which some years ago, Mr. Chairman, as you well know, cybersecurity was under Transportation Security and Infrastructure. We began looking at where cyber impacts us, which is everywhere from water systems, sewer systems, the electric grid and beyond. So I believe that it is important to take note of a number of statistics that I hope to get a hearing on particular legislation that I have.

Just like to cite the Bureau of Labor Statistics in 2016 reported that African-Americans comprise only 3 percent of the information security analysts in the United States yet comprise 13 percent of the population. The numbers at one time, top computing security salaries, $175,000, $230,000. I think we had positions in the Government at $88,000. In 2017, the United States employed nearly 780,000 people in cybersecurity positions with approximately 350,000 vacancies. In 2017, nearly 65 percent of large U.S. companies had a chief information security officer, which is good. It is up

from 50 percent. Women hold only 11 percent of cybersecurity positions globally filling 25 percent of tech jobs and comprising 50 percent of the population. There is a similar situation with African-Americans, Hispanics, who account for 5 percent of cybersecurity positions, African-Americans 7 percent.

Those numbers are simply to look or give us the parameters of the space that we should be in in our recruiting and collaboration on the question of providing a pathway for individuals. So, Mr. Chairman, I am interested in having a hearing on H.R. 1981, the Cyber Security Education Workforce Enhancement Act, which I have introduced. But I do want to ask both Ms. Bailey and Ms. Moss, and I want to thank Mr. Wilshusen for his product of DHS's needs to take urgent action to identify its position in critical skills requirements.

So I see that there is a beginning structure that you all are working on. This legislation penetrates outside of the immediate need and begins to build a farm team. So recruiting information, assuring cybersecurity, and providing computer security professionals, this particular office would be called the Office of Cyber Security Education Awareness branch providing grants training and other support for kindergarten through grade 12, secondary and post-secondary computer security education programs, guest lecturer programs, identifying youth training programs, developing programs to support the underrepresented and working with a number of organizations that would have outreach to those organizations.

So, Ms. Bailey and Ms. Moss, I would hope that those kinds of outreach, though you may have them, having them more established and getting the farm team established, that will ultimately fit into the scheme of young people coming in from a diverse background, staying a couple of years and then going out and coming back in, which I think is an excellent model. Could you work with that added outreach that my legislation speaks of?

Ms. BAILEY. I will start and then Rita can elaborate on this a little bit more. So the answer is yes. We actually have been having these conversations with regard to where do you start the outreach, where do you actually start the recruiting? I am of the belief that really we need to start this actually in elementary school and then we need to build it from there.

The public school systems are actually begging us to help them establish what the curriculum is that we need for these folks to be successful, because not everybody is going to be on a 2- or 4-year college track. Some are going to come straight out of high school. But when we have a system today that when you come out of high school, the most that you can probably make is around minimum wage, it is not going to help them sustain or actually be able to support their families or anything else.

If we are going to hire from all segments of society, which is what our basic merit principle—not suggest—require as part of the statute, then I think that, to your point, we need to establish programs and such in which we can actually attract from all segments of society.

Ms. JACKSON LEE. Thank you.

Ms. Moss.

Ms. BAILEY. So getting into the schools I think is important.

Ms. JACKSON LEE. Thank you.

Ms. Moss.

Ms. MOSS. OK. Yes, cybersecurity education is part of our mission at NPPD, so we are certainly passionate about that and we are happy to see that you are passionate about it as well. In the mean time, one of the things that we have started doing is looking at the Scholarship For Service, pathway intern programs to reach out to a more diverse population of students. So we are using those tools right now to leverage diversity across our cyber work force.

Ms. JACKSON LEE. Thank you.

Mr. Chairman, I am prepared to yield back. I wanted to ask unanimous consent to put H.R. 1981 in the record.

Mr. RATCLIFFE. Without objection.*

Ms. JACKSON LEE. And would further encourage discussions about hearings on the very points that the two witnesses have made that expands the opportunity. I just mention coding is something that can be taught out of high school and they can go into a very, very productive employment that would have young people supporting families and being very productive. So I look forward to it.

I thank the witnesses very much for their testimony. I yield back.

Mr. RATCLIFFE. I thank the gentlelady.

The Chair now recognizes the gentleman from Louisiana, Mr. Higgins, for 5 minutes.

Mr. HIGGINS. Thank you, Mr. Chairman.

I thank the Americans before us for testifying today.

Ms. Bailey, thank you for your service. In your written statement, you identified three priorities, the second of which was to recruit and retrain, and retain, highly-qualified employees with capabilities vital to mission success. The relationship with DHS and your effort to recruit and retain, is there any mechanism to recruit out of our college campuses?

Ms. BAILEY. Oh, absolutely. I mean, that is——

Mr. HIGGINS. Can you share that with us, please?

Ms. BAILEY. So with regard to our college campuses, some of the things that we make sure that we do is last year alone, we actually spoke to over 1,300 students at 122 different universities and colleges across the United States, and that includes both 2-year and 4-year colleges. So to that extent——

Mr. HIGGINS. That is encouraging. That is the answer we anticipated and hoped to hear. It states that DHS has reported at least 12 of 15 components as having cybersecurity positions. However, DHS could not provide data to show the actual numbers of positions in each of these categories in specialty areas.

So how are we, and this means you, how are you connecting the dots between the jobs that you are discussing with our students at American universities and connecting the location of the residents of these young Americans to the jobs that would be associated in the specialty areas of cybersecurity if you don't know what those

*The information has been retained in comittee files and is also available at *https://www.congress.gov/115/bills/hr1981/BILLS-115hr1981ih.pdf.*

specialty areas are? How are you having a complete conversation with a young American that is, say, a sophomore or junior in college and will consider entering a career with DHS and serving the country in that way?

Might I add that money for a soldier, sailor, airman, or Marine is not the motivating factor of serving, it is service to country. I would suggest that service in protecting our homeland should be reflective of that same patriotic spirit. I believe these positions can be filled despite the lack of funding as it is referred to today, and if we can appeal to the patriotic spirit of young Americans in colleges. These are the young men and women that are coming out of there which have 21st-Century cyber skills that none of us have.

If you haven't been able to identify the specialty positions within the various components of DHS, then how are you having a complete conversation with a young American man or woman at a college university in Louisiana or Alabama or Florida or California?

Ms. BAILEY. Well, sir, we have identified. We have identified that we have over 33 specialty areas. We have mapped them to the NICE framework. What we have not done timely is coded all those positions into our payroll system and make sure that we have accounted for them, but we have done that work. We know exactly what our specialty areas are. We know exactly where the different—and we have had to map those against the 40 different occupational series, so we know exactly what it is that we need.

We know where those positions are in every single component. We know that the top series are things like IT specialist info, computer forensics, coders, law enforcement. We have a law enforcement element of this. We have intel analysts that are part of this and we have management and program analysts, just to name a few.

Mr. HIGGINS. That is also an encouraging answer. So you are helping us here fill in some blanks. Let me just ask. If I am a student in the IT field at University of Louisiana in Lafayette, one of the top IT universities in the country, and there is a component of DHS in my area where I live and I speak to a recruiter for DHS, can you identify a job for me when I graduate in 2019 or 2020 that I may want to pursue? Because from our hearing last week, it takes a year to get hired. So if I wanted to pursue that job, can you connect me with that job if I am a student right now at a university in America?

Ms. BAILEY. Absolutely. To what Ms. Moss was speaking about, that is where we use things like the Pathways Program, which is the internship program. So we can actually hire that student out of the university as you suggested. We can hire them today. We can get them trained where they can work for us over the summers, they can work for us on their spring breaks, their winter breaks. Then at the end of that, we can what is called convert them today, convert them full-time into the position of which we need into that future.

Mr. HIGGINS. All right. Well, these are encouraging answers.

I have several other questions. Mr. Chairman, permission to submit my answers in writing to the witnesses. I yield back.

Mr. RATCLIFFE. I thank the gentleman.

Chair now recognizes the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank all of our witnesses for your testimony here today on a very important topic.

Ms. Bailey and Ms. Moss, I know that we have touched on the topic I want to address on work force, but your testimony describes DHS's initiatives to accelerate recruiting and hiring for cybersecurity professionals and to retain cyber staff through financial incentives. Yet, DHS cannot hire its way out of its work force shortages obviously, nor can it hope to compete with the private sector on compensation. So what investment is DHS making to train its work force and to develop cybersecurity skills in-house?

Ms. MOSS. At NPPD, one of the things that we utilize is the NICE framework to identify certifications that are critical for the success of the cyber mission. So we incentivize our employees to get those certifications through retention incentives. We currently have a number of employees. I would say a majority of our cybersecurity work force that get incentives to get certain certifications. So we are very much encouraging certification and additional training for our cyber work force.

Ms. BAILEY. We then used that, their excellent work that they did. We actually rolled this out Department-wide because one of the things we want to make sure of is that within the cybersecurity community within DHS that we did not have the haves and the have-nots. So we took the excellent work that NPPD did and we work with our cyber council with the component leadership.

To Ms. Moss' point, we actually have identified all the kinds of certifications whether it is specific ones to a cyber or it is things like critical thinking, decision making, teamwork, those kinds of things because they go hand-in-hand with this. So we made sure that outlined everything that we expect of our work force, and then we provide that through their individual development plans and then through tuition assistance and things like that to ensure that they get the accreditation that we actually need for them to accomplish their mission.

Mr. LANGEVIN. OK. Thank you. What about investments is DHS making into rotational job assignments to develop and retain cybersecurity staff?

Ms. BAILEY. I am sorry, sir. Vocational?

Mr. LANGEVIN. Rotational.

Ms. BAILEY. Oh, rotational?

Mr. LANGEVIN. Yes.

Ms. BAILEY. Do you know if you are—OK. So for rotational—we were just conversing here just to see which. Rotational assignments, actually, what we just started was a joint duty program, which is an excellent way for us to do these rotational assignments, to take people even sometimes outside of their cybersecurity and introduce them maybe to law enforcement or introduce them to intelligence or human resources for that matter. Because what we are really trying to do is create well-rounded professionals that can perform a variety of functions within DHS.

So we also do have a robust rotational program as well, and that includes rotations inside DHS and outside DHS. But we are large

enough and our components are diverse enough that we can really provide folks with a very robust rotational experience that gives them I think things that would be needed for their career advancement.

Mr. LANGEVIN. Have you considered expanding those experiences to include positions in State government, for example? I know that my State of Rhode Island and other States around the country are hungry for DHS professionals to come in and either them to learn from State experience and what are the challenges they are facing and as well as learning from DHS staff.

Ms. BAILEY. I will take that back, sir. It is an excellent idea. We just kind of got it going, but I tell you, folks are extremely excited about this so I would be glad to take that back.

Mr. LANGEVIN. Thank you.

Go ahead.

Ms. MOSS. I am sorry. I would also add. I am surprised Ms. Bailey did not mention this because we have talked about it several times. As part of the new cyber personnel system, part of that will be project management—I am sorry—project-based assignments, so that is going to be a huge part of the new cyber personnel system as well as a concept for that program.

Mr. LANGEVIN. Great. Thank you.

Ms. Bailey, I know that many of the Members here including the Chairman are supporters of the Scholarship For Service program run by NSF and OPM and the Department. I have certainly been consistently impressed by the caliber of participants and alumni in the program that I have met. I must say that the annual D.C. job fair, in fact, it is one of my favorite events to attend. How has SFS student helped alleviate the cyber work force deficit facing the Department?

Ms. BAILEY. I am going to let Rita speak to the specifics because NPPD knocks it out of the park when it comes to SFS. It is something that go back to whenever I worked even in the Department of Defense for something that I have been a huge supporter of. So you are absolutely right, this is high-caliber folks that we have been able to get in. It is starting to, I think, chip away especially at the entry level. We are using this quite significantly.

Ms. MOSS. We participated in the virtual job fairs and the in-person job fairs and have been able to hire on the spot a number of individuals into this program. We do not have the long-term results of that yet, but it is very effective in terms of getting them in and familiarizing them with our mission and DHS.

Mr. LANGEVIN. Very good. Thank you. I know that when I have been to those job fairs as you just pointed out, they are offering jobs on the spot we have had some 75 or 80 Government departments and agencies there with actual job offers and hired pretty quickly. So great opportunity for these young people and we are getting return on investment by having them in the Government for a period of time, and so part of their payback for their Scholarship For Service program.

So I have other questions, Mr. Chairman, that I will submit for the record. But thank you and I will yield back.

Mr. RATCLIFFE. I thank the gentleman.

I now recognize myself for 5 minutes.

Mr. Wilshusen, I will start with you. Both the Government and the private sector used a NICE framework to chart out work roles so that cybersecurity workers as well as the people responsible for hiring them can better develop their career paths in cybersecurity.

Your report, the GAO report, points to misalignments between what DHS has identified as a skill gap and the specialty areas in the NICE framework. For instance, the DHS work role entitled development operations is related to 12 different specialty areas in the NICE framework. So I guess my question is, since the overarching goal is matching DHS work roles with the NICE framework and not the other way around, shouldn't DHS maybe consider changing the categorization of the specialty areas to reflect that and to simplify the process?

Mr. WILSHUSEN. Well, the specialty areas are actually part of the National cybersecurity framework that NICE program and NIST have set up and that is one that is in use throughout the entire Federal Government.

What DHS has done is identified I guess the competencies and proficiency levels as part of its technical capability gaps in its program. There is, you are correct, between those competencies a, I guess, a one-to-many relationship. I think DHS has come up with a mapping, if you will, from our conversion table from their competencies to the work in specialty areas of the NICE program.

The reason why I guess the specialty areas are important in categorizing the positions according to that is the fact that that is something that provides a common lexicon and something that can be used throughout the Federal Government as well as throughout the Department. So that was one of the reasons why OPM and indeed the law requires agencies to use the specialty areas identified in the NICE National cybersecurity framework for identifying their cybersecurity positions.

Mr. RATCLIFFE. OK. Thanks for that.

Ms. Bailey, you said something and I want to make sure that the record is clear, because I thought it was maybe inconsistent with what I read in this report. So on page No. 8 of the report it says as of November 2017 the Department had not completed identifying all of its cybersecurity positions and it had not determined the work categories or specialty areas of the positions. That is from the report. Did I hear you testify differently?

Ms. BAILEY. We have gone through and we have identified the 33 different specialty areas and used this crosswalk and mapped things to that. So I think in some ways there is a smidge of a disagreement here perhaps with how it is being characterized.

So for us, our positions, they are all coded, but we have identified the positions that we are aware of. We have identified these positions. I can't even remember the date, but we had almost 95 percent of the positions that were filled.

You correct me if I am wrong, but I think what part of the issue here is that we hadn't actually identified our vacant positions. We had identified our filled positions. So of our filled positions, we had mapped those to the 33 different specialty areas, the critical need areas and also then the 40 different occupations. So I just want to be careful in how I am saying this, that of the positions that we

coded and we took care of, we have mapped all of them against that.

Mr. RATCLIFFE. OK. I want to make sure the record is clear.

Ms. BAILEY. Yes.

Mr. RATCLIFFE. So there is that smidge of a difference accurately characterized in your opinion, Mr. Wilshusen?

Mr. WILSHUSEN. I would say there is a couple of things, one is Ms. Bailey is correct, it is part of the reason why there is a difference between what was coded in terms of 95 percent versus 79 percent had to do with the vacant positions that were not being coded. But at the same time, we are still noting throughout the time that the number of cybersecurity positions were also supposed to be identified at a certain time by law.

What we are finding is that these numbers keep increasing. For example, back in I think it was—let me just get the exact date here. It was back in I would say it was December 2016 they had identified about 10,725 cybersecurity positions. More recently, we saw a draft report where DHS has identified over 14,000 cybersecurity positions. So any part of that could be the vacancies that are now being recognized but also I think it is the Department that is also expanding the identification of these cybersecurity positions throughout the Department.

Mr. RATCLIFFE. OK. Thank you.

Ms. Moss, I want to wrap up and ask you a question. You have had a number of questions from other members about cyber work force development and how that ties into educational effort. So I wanted to get on the record, and if someone asked you this specifically, I did not catch it. But I am interested to hear how your office works with SECIR, the Stakeholder Engagement and Cyber Infrastructure Resilience, office in its education and outreach efforts and how or whether those enhance the cybersecurity initiatives in your organization.

Ms. MOSS. SECIR is heavily involved in the centers for academic excellence, which is the driver for the Scholarship For Service program. As I noted before, we are heavily engaged in the Scholarship For Service and we do a lot of hirings surrounding Scholarship For Service.

There is one other point. Also with the NICE framework, they are involved in the development of the NICE framework, identifying the certifications that are important for the cyber mission. As I noted, we use those certifications to incentivize our folks through incentive pay.

Mr. RATCLIFFE. Terrific. OK.

Thank you all for being here today. We really appreciate your testimony. I thank the Members for being here and for their questions. As you have heard, Members of the committee do have some additional questions for some of you, so we will ask them to submit those and ask you to respond to those in writing. Pursuant to the committee Rule VII(D), the hearing record will remain open for a period of 10 days and——

Mr. CORREA. Mr. Chair, before you—just a couple of comments, if I may.

Mr. RATCLIFFE. You bet.

Mr. CORREA. I just wanted to reiterate my question which is how can we help you get there, how can we help you do your job? No. 2, hopefully we will have another committee hearing soon to follow up on how we can help DHS fulfill their mission. Thank you.

Mr. RATCLIFFE. You bet. I think that is a sentiment that has been expressed by a number of Members, but I appreciate the gentleman's comments. With that, that will conclude our hearing. Without objection, the subcommittee stands adjourned.

[Whereupon, at 3:25 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR GREGORY C. WILSHUSEN

Question 1. Across all GAO's recommendations for action, how would you recommend DHS prioritize accomplishing these recommendations given the overarching task of addressing critical workforce needs?

Answer. To address its critical cybersecurity workforce needs, DHS should give top priority to accomplishing the six recommendations in our February 2018 report on the Department's efforts to identify its cybersecurity workforce positions and critical needs.[1] Further, of the six recommendations, I recommend that the Department first implement our recommendations to:

- Collect complete and accurate data from its components on all filled and vacant cybersecurity positions when it conducts its cybersecurity identification and coding efforts, and
- Develop guidance to assist DHS components in identifying their cybersecurity work categories and specialty areas of critical need that align to the National Initiative for Cybersecurity Education Framework.

Implementing these two recommendations is especially important because they are essential to helping DHS identify the critical skills and cybersecurity personnel that the Department will need. Earlier this month, we sent a letter to Secretary Nielsen highlighting the two recommendations as priorities for the Department to address.[2] Beyond these two recommendations, however, DHS should also implement the other four recommendations that we made in in the report to bolster its cybersecurity workforce assessment efforts.

The six recommendations are aligned with the requirements presented in the *Homeland Security Workforce Assessment Act of 2014*, which required DHS to identify, categorize, and code its cybersecurity positions.[3] We found that the Department did not complete these activities by their statutorily-defined due dates, and efforts to do so are still on-going.

Without sufficiently completing all of these activities, the Department will not be positioned to effectively examine its cybersecurity workforce, identify skill gaps, and improve workforce planning to address its critical workforce needs. DHS concurred with each of our recommendations and stated that it plans to complete actions to address all six of the recommendations by June 29, 2018.

Question 2. GAO's report points to the commitment of DHS leadership as essential to successfully address the issues and management weaknesses identified in its audit. What more can DHS do, at the Secretary level, as well as the CHCO level, to ensure that implementation of cybersecurity authorities is a Department-wide priority?

Answer. DHS can take several actions to ensure that the implementation of cybersecurity authorities is a Department-wide priority. Specifically, the Secretary can: (1) Communicate the importance of maximizing the use of its existing hiring authorities and flexibilities for filling cybersecurity needs; and (2) hold senior managers and leaders, such as the Chief Human Capital Officer (CHCO), accountable for fulfilling their responsibilities. Identifying the individual in each component who is responsible for leading that component's efforts in identifying and coding cybersecurity positions as we recommended in our February 2018 report is an important step for establishing that accountability. By setting the tone at the top, the Sec-

[1] GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skills Requirements,* GAO–18–175 (February 6, 2018).

[2] Comptroller General of the United States Gene Dodaro, *2018 Homeland Security Priority Recommendations*, letter to the Honorable Kirstjen Nielsen, Secretary of Homeland Security (Washington, DC: April 3, 2018). This letter is not publicly available.

[3] The *Homeland Security Cybersecurity Workforce Assessment Act of 2014* 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.

retary will underscore the imperative of implementing the Department's cybersecurity authorities.

In addition, consistent with the recommendations in our February 2018 report, the CHCO can: (1) Ensure that the components report accurate and timely information to leadership so that leadership will be informed of the extent to which the Department is making progress in identifying its cybersecurity positions and critical skills requirements; and (2) provide more guidance to components on the importance of using the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework and how the work roles align to DHS's cybersecurity positions. By taking urgent and diligent action now to implement the recommendations in our February 2018 report, DHS should be better positioned to fulfill the requirements of the Homeland Security Workforce Assessment Act of 2014; accurately identify its cybersecurity positions and critical needs; and implement its cybersecurity authorities.

QUESTION FROM HONORABLE RON ESTES FOR GREGORY C. WILSHUSEN

Question. What do continuing hiring issues, like those identified by GAO's report, say about the overall maturity of DHS as a cohesive agency, 15 years after the Department's formation?

Answer. DHS's challenges in identifying its cybersecurity workforce positions and critical skill requirements indicate that the Department has not matured to the point where its human capital management functions are fully integrated and cohesive across the Department. As we reported in February 2018,[4] DHS did not completely and reliably identify and assign employment codes for cybersecurity positions because its processes were manual, undocumented, and resource-intensive. For example, the Department used manual data calls to collect information and understand components' coding efforts. In addition, the Department did not have documented processes to collect and verify data from its component agencies. Officials in the Department's Office of the Chief Human Capital Officer stated that the number of cybersecurity workforce personnel frequently changed, they could not review workforce data for reliability, as such a review was resource-intensive.

If implemented, the six recommendations that we made to DHS in our February 2018 report should help address the concerns we noted with regard to the Department's identification of its cybersecurity workforce positions and critical skill requirements, and the associated management weaknesses. DHS concurred with all of our recommendations and stated that it was working to implement them.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR THE DEPARTMENT OF HOMELAND SECURITY

Question 1a. One of the key reforms signed into law in 2014 were expedited hiring authorities for mission-critical cybersecurity positions that allowed DHS the flexibility to better recruit qualified cybersecurity personnel. However, those legislatively-mandated authorities have yet to be used to on-board a single cybersecurity worker nearly 4 years later.

When do you anticipate these expedited hiring authorities to be used for the first time?

Answer. DHS leadership and components are pushing to launch the new personnel system as quickly as possible, with a goal of hiring the first cadre of employees in 2019. In the *Border Patrol Agent Pay Reform Act of 2014* (Pub. L. No. 113–277), which added a new section (codified at 6 United States Code (U.S.C.) § 147) to the *Homeland Security Act of 2002,* Congress granted the Secretary new cybersecurity-focused human capital authority. The Secretary's authority allows DHS to create a new personnel system with alternative methods for defining jobs, conducting hiring, and compensating employees.

We have taken the time to craft a solution that we believe will allow the Department to compete in the competitive market for cybersecurity talent, and will solve our cybersecurity recruitment and retention challenges for the long term. The Department is grateful to Congress for this opportunity, and we are excited about the new personnel system. Due to the complex nature of implementing a new personnel system in the Federal Government, the Department's examination of comparable efforts by other Federal agencies has shown that it generally takes several years to complete.

---

[4] GA0–18–175.

As the Office of the Chief Human Capital Officer finalizes the design and prepares new policies and business processes, the Secretary is working to prescribe required regulation, in coordination with the Director of the Office of Personnel Management.

Question 1b. Why has it taken so long for the expedited hiring process to be implemented?

Answer. From a historical perspective, our examination of comparable efforts by other Federal agencies has shown that implementing a new Federal personnel system is complex, and can often take several years. There are a variety of factors that make implementing a new personnel system, including new processes for hiring, especially challenging.

First, the talent required to build a new personnel system is specialized and rare. DHS had to recruit and contract to build a team of expert industrial and organizational psychologists, Federal human capital policy experts, certified compensation specialists, economists, and employment and regulatory attorneys.

Second, DHS is working to update some foundational human resources concepts dating back to the first half of the 20th Century. Our systems for defining or classifying jobs, conducting hiring, and administering pay are based on laws from the 1940's. The Federal workforce has evolved from being predominantly clerical, and much of the cybersecurity workforce DHS requires is highly technical, with valuable senior-level expertise.

In replacing hundreds of pages of human capital regulation and policy that took decades to develop, and creating a system that looks to the future, DHS has to be methodical, avoiding the re-creation of bureaucratic barriers that impede us today. In the conventional civil service world (governed by title 5 U.S.C. and title 5 of the Code of Federal Regulations), so much is automatic and mechanical. An agency hires a person based on a brief assessment against rigid—often outdated—standards. A fixed table sets their pay, and pay increases are directly linked to time. As such, the payroll system has been programmed to automatically execute many pay increases. The conventional, tenure-based civil service assumes that someone gets better at doing a job after the passage of time, and will be their best at the job after 30 years. With cybersecurity and most work today, years of experience matter, but they are not the sole determinant of whether someone will be successful. To replace tenure as the main measurement tool, it is necessary to more thoroughly analyze candidates' skills prior to hiring them.

Third, DHS must take great care to ensure its new approaches to hiring and pay setting are fair and consistent. There are Merit System Principles to be upheld, and a variety of laws and regulations governing employment in the United States that must be taken into consideration. For example, the Uniform Guidelines on Employee Selection Procedures guide compliance of hiring and selection processes with requirements of Federal law prohibiting employment practices that discriminate on grounds of race, color, religion, sex, and National origin. Similarly, Title VII of the Civil Rights Act of 1964 prohibits employment-related discrimination against any individual because of race, color, religion, sex, or National origin. Also, the Equal Pay Act requires that men and women in the same workplace be given equal pay for equal work, which informs pay policies. In implementing new hiring and pay processes, DHS must incorporate the requirements of such laws, which often requires careful study, testing, and the generation of a variety of official documentation.

Fourth, DHS is trying to learn from the prior human capital experiments and failures. Many agencies that received similar authority in the past yielded to the inertia of the conventional civil service system, and made modest—sometimes cosmetic—changes to their approaches to hiring, compensation, etc. They have often seen modest results. There are also several examples of more innovative personnel systems that, after great investment, were summarily canceled due to litigation. DHS is focused on learning from these mistakes of the past so as not to repeat them.

Question 2a. You testified that "by the end of April 2018, this Department will have all of its cyber positions coded under the three-digit code." However, GAO noted that the number of identified cyber positions continues to increase over the years as this identification process moves along. I am concerned that positions cannot be coded if they continue to change or increase.

How certain are you that all cyber positions across components have been identified?

Answer. Cybersecurity workforce planning and analysis—of which position coding is one element—is an on-going activity. For several years, DHS has been tracking a core of several thousand positions with cybersecurity responsibilities, but as definitions have changed and Government-wide awareness of the criticality of cybersecurity has increased, the population has fluctuated. In the transition to 3-digit posi-

tion codes, components are closely scrutinizing their workforces and refining past analyses. Our new processes will yield accurate and current counts, ensure newly-created positions are appropriately coded, and monitor the accuracy of aggregate and component-level position data over time.

Question 2b. Will these positions be coded with only 3-digit codes or both 3-digit and 2-digit codes?

Answer. DHS will only use the 3-digit codes from which data about 2-digit codes can be extrapolated. DHS will code positions using 3-digit, Work Role codes in accordance with Pub. L. No. 114–113, but will continue to collect and report data about the Specialty Areas and Categories (2-digit codes) associated with cybersecurity positions required by Pub. L. No. 113–246 and Pub. L. No. 113–277 (see response to 3b).

Question 3a. The GAO report states that "According to OPM officials within Employee Services, agencies are not expected to continue coding to the 2-digit data standard and, instead, are to adopt the 3-digit data standard and complete coding the 3-digit standard by April 2018." However, in your testimony you said that DHS will continue to work on 2-digit codes.

Is producing both 2-digit and 3-digit codes a duplication of effort and efficient use of resources?

Answer. Starting in 2018, DHS will only be coding positions using 3 digits, but we will also be monitoring and reporting data by the 2-digit coding structure, as required by statute (see response to 3b). While the Department would welcome Congress' assistance in streamlining and simplifying its current set of overlapping cybersecurity workforce planning requirements, which result in largely duplicative work and multiple oversight reviews, DHS does not expect this 2- versus 3-digit code issue itself to be problematic. The National Initiative for Cybersecurity Education (NICE) Workforce Framework has a nested structure, with Work Roles (3-digit codes) representing the most granular level. Coding at the Work Role-level should allow for easy analysis of the necessarily aligned, higher-level Specialty Areas and Categories of the NICE Framework.

Question 3b. Why is the 2-digit coding effort continuing?

Answer. DHS is in the unique position of managing a series of cybersecurity workforce planning actions in alignment with three laws: The Border Patrol Agent Pay Reform Act of 2014 (Pub. L. No. 113–277); the Cybersecurity Workforce Assessment Act (Pub. L. No. 113–246); and the Federal Cybersecurity Workforce Assessment Act of 2015 (Pub. L. No. 114–113).

While Pub. L. No. 114–113 requires 3-digit coding by the Work Roles outlined in the latest version of the NICE Workforce Framework, Pub. L. Nos. 113–277 and 113–246 both require on-going reporting organized around the NICE Specialty Areas and Categories, which were the basis for 2-digit codes.

DHS will code positions using 3-digit, role-based codes, but will continue to collect and report data about the Specialty Areas and Categories associated with cybersecurity positions. As mentioned earlier, it would be more effective and practical if these requirements were streamlined.

Question 4. GAO reported that DHS components record and track vacant positions differently, and DHS responded that because of this issue, OCHCO could therefore not issue Department-wide guidance on vacant cyber positions. What are the specific changes that your office is making to standardize guidance so that all components are working from the same playbook?

Answer. DHS does not have a Department-wide information technology solution to track vacant positions, but the Office of the Chief Human Capital Officer (OCHCO) identified this issue as a Human Resources Information Technology (HRIT) Strategic Improvement Opportunity (SIO). In addressing this SIO, OCHCO established a process for components to report standardized position data tables for all vacant and filled Federal civilian positions.

DHS released revised cybersecurity position coding guidance on March 19, 2018. The guidance includes instructions for components to code both vacant and filled cybersecurity positions in the Department's National Finance Center (NFC) personnel system, but it also requires components to report filled and vacant cybersecurity positions via the position data table process. New position coding guidance will ensure OCHCO has consistent visibility into each component's coding of vacant cybersecurity positions via NFC and the position data table process.

Question 5a. Describe your interactions with OCHCO in fulfilling the requirements of Public Law No. 113–277. How has OCHCO helped NPPD in recruiting and retaining the workforce necessary for NPPD to carry out its essential cybersecurity mission?

Question 5b. In what ways do you feel that the interactions between OCHCO and NPPD's Office of Human Capital could be improved?

Answer. OCHCO has shown commitment to NPPD in its effort to recruit and retain the workforce necessary to carry out our essential cybersecurity mission. Our teams work closely together, across human capital and the cybersecurity technical leadership (across the Department), this includes the chief human capital officer, the chief information officer (CIO), and the 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.

Additionally, NPPD CS&C leadership along with the NPPD CHCO are active members on the DHS Cyber Workforce Coordination Council. As a collaborative team, 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.

Additionally, OCHCO supports NPPD's use of incentives (e.g., retention, recruitment, and student loan repayment) to attract and retain talent.

We've also leveraged authorities that provide flexibilities in our hiring, such as the DHS Schedule A cybersecurity hiring authority and the Government-wide IT (information security) direct hire authority. We maximize these authorities through open and continuous announcements or at hiring events. OCHCO has led joint hiring events for the Department which has assisted NPPD in filling critical cybersecurity roles across the organization. NPPD works closely together with other DHS human capital leaders and recruiters across components. NPPD participates in the OCHCO-led Corporate Recruiting Council, which 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, the OCHCO staff manages the cybersecurity pipeline development and outreach activities focused on 2- and 4-year academic institutions, including the National Centers of Academic Excellence in Cyber Defense and Cyber Operations, National and local community organizations, and professional associations. NPPD has leveraged these outreach events; in fiscal years 2016—fiscal year 2017 to date, we've had more than 58 CyberCorps Scholarship for Service (SFS) students in our program and anticipate hiring more than 70 students for fiscal year 2018. We've also had great success in leveraging the Pathways Intern Program, the PMF Program, and volunteer intern programs.

NPPD's Office of Human Capital and OCHCO have a very collaborative relationship and we are consistently engaged on major DHS initiatives. Examples of interactions include our involvement in the development of the competencies to support the DHS Cyber Talent Management System (CTMS); NPPD subject-matter experts served on panels to develop competencies for the cyber workforce alongside other cyber SMEs across DHS. Also, CHCO leadership has conducted a 2-day listening tour at NPPD, visiting every NPPD subcomponent to be briefed on each of their missions and human capital challenges. OCHCO has also leveraged the opportunity to meet with NPPD employees, affording them the opportunity to have an open dialog.

Questions From Honorable Ron Estes for the Department of Homeland Security

Question 1. What do continuing hiring issues, like those identified by GAO's report, say about the overall maturity of DHS as a cohesive agency, 15 years after the Department's formation?

Answer. The Department continues to mature and identify opportunities for increased collaboration and coordination among components. The Department's recruiting and hiring processes have matured significantly since its inception. DHS improved its time-to-hire in many of our mission-critical occupations. DHS is committed to creating a good applicant experience throughout the process from first point of contact to the final job offer and even through the employee life cycle. Our recent joint hiring events in cyber, veterans, students, and women in law enforcement are good examples of the Department's cohesive approach to hiring, as are our HRIT project, Human Capital Operational Plan (HCOP), Primary Mission Critical Occupations (PMCO) charts, Recruitment Outreach and Marketing Matrix (ROMM), and Strategic Outreach and Recruitment (SOAR) Plan.

Question 2. With data continuing to show shortages of specific cyber skills and talent gaps in the Department's cybersecurity workforce, what hiring improvement strategies, programs, and incentives has OCHCO developed to help recruit and retain highly-skilled professionals in the Federal workforce?

Answer. While OCHCO focuses on accelerating the implementation of a new cybersecurity-focused personnel system, the office simultaneously has looked at ways to improve cybersecurity recruitment and retention within the current system.

OCHCO developed and 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. We are also 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. This effort includes the new DHS H.R. Academy, which is aimed at training human resources professionals to improve the human capital support provided to all critical missions, including cybersecurity.

To address the cyber skills and talent gap challenges, OCHCO continues to focus its cyber recruitment and hiring efforts in several targeted areas. The first is increasing the recruitment of GS 5–9 employees. Attracting young professionals requires a targeted engagement and outreach program with post-secondary academic institutions as well as K–12. In fiscal years 2017 and 2018, OCHCO engaged with more than 1,300 students from 122 academic institutions, which includes 40 Centers of Academic Excellence. Additionally, OCHCO operates the Corporate Recruiting Council, which ensures cross-component coordination of recruitment activities and strategy development for mission-critical occupations, including cybersecurity. OCHCO also leads an outreach program focused on academic institutions and associations, including the National Centers of Academic Excellence in Cyber Defense and Cyber Operations. To improve the pipeline for talent, OCHCO is focused on providing greater internship offerings across DHS, including opportunities associated with the CyberCorps®: Scholarship for Service.

The Department plans to continue engagement with industry partners in 2018 to meet our human capital needs. The proposed plans include:

- Partnering with the Department of Defense to pilot their cybersecurity skills training program at DHS; and
- Engaging with industry stakeholders and science, technology, engineering, and math organizations to develop a comprehensive cyber pipeline curriculum for post-secondary and K–12 schools.

With regard to retention, OCHCO collaborated with the Office of the Chief Information Officer and other components to develop the Department's Cybersecurity Retention Incentive Plan, which helps components financially recognize significant training and certification accomplishments of cybersecurity employees. In addition, OCHCO assists components in their understanding of retention tools, such as tuition assistance, and is exploring strategies for encouraging their increased use across the Department.

Question 3a. I want to ensure that DHS has the proper workforce to carry out its cybersecurity mission. What is NPPD's biggest cybersecurity skill gap or critical need?

Question 3b. Would you say that NPPD has the adequate resources, manpower in particular, to function at the peak of its capability on a day-to-day basis?

Answer. The National Protection and Programs Directorate (NPPD) continues to evaluate the needs and requirements of its workforce, particularly in the face of new and emerging threats. We have reviewed every position in our workforce, aligning and coding all cybersecurity positions alongside the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Based on the NICE work roles, NPPD's greatest cyber skill gap/need includes:

- Cyber Defense Analyst;
- Cyber Forensics Analyst;
- Cyber Incident Responder; and
- Cyber Operator.

NPPD, like other Federal and private-sector organizations, strives to recruit and retain qualified cybersecurity personnel. To that end, NPPD continues to face challenges in quickly hiring qualified employees to join its cybersecurity workforce. Potential hires must go through a lengthy clearance and internal suitability process, which delays on-boarding qualified individuals. Coupled with attrition due to the pay and fringe benefits for cybersecurity positions in the private sector, the result is significant competition for high-performing and qualified employees. NPPD continues to assess its resources, particularly in line with the authorities it has been granted to execute across the various cybersecurity mission areas.