AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

REVIEWING FEDERAL IT WORKFORCE CHALLENGES AND POSSIBLE SOLUTIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

APRIL 4, 2017

Serial No. 115–6

Printed for the use of the Committee on Oversight and Government Reform



Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

25–717 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

Jason Chaffetz, Utah, *Chairman*

John J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Trey Gowdy, South Carolina
Blake Farenthold, Texas
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan

Elijah E. Cummings, Maryland, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Stephen F. Lynch, Massachusetts
Jim Cooper, Tennessee
Gerald E. Connolly, Virginia
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Stacey E. Plaskett, Virgin Islands
Val Butler Demings, Florida
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
John Sarbanes, Maryland

Jonathan Skladany, *Staff Director*
Rebecca Edgar, *Deputy Staff Director*
William McKenna, *General Counsel*
Sean Brebbia, *Counsel*
Michael Flynn, *Counsel*
Kiley Bidelman, *Clerk*
David Rapallo, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

Will Hurd, Texas, *Chairman*

Paul Mitchell, Michigan, *Vice Chair*
Darrell E. Issa, California
Justin Amash, Michigan
Blake Farenthold, Texas
Steve Russell, Oklahoma

Robin L. Kelly, Illinois, *Ranking Minority Member*
Jamie Raskin, Maryland
Stephen F. Lynch, Massachusetts
Gerald E. Connolly, Virginia
Raja Krishnamoorthi, Illinois

CONTENTS

Page

Hearing held on April 4, 2017 1

WITNESSES

Mr. Steven Cooper, Former Chief Information Officer, U.S. Department of Commerce
- Oral Statement 4
- Written Statement 6

Ms. Elizabeth Hyman, Executive Vice President, Public Advocacy, Comptia
- Oral Statement 12
- Written Statement 14

Ms. Lisa Depew, Head of Industry and Academic Outreach, McAfee
- Oral Statement 23
- Written Statement 25

Mr. Dan Waddell, Managing Director, (ISC)2
- Oral Statement 34
- Written Statement 36

Mr. Nick Marinos, Director, Information Technology, U.S. Government Accountability Office
- Oral Statement 41
- Written Statement 43

Ms. Debora Plunkett, Strategic Advisory Board Member, International Consortium of Minority Cybersecurity Professionals
- Oral Statement 63
- Written Statement 65

APPENDIX

Statement for the Record of Steven Weber Faculty Director, UC Berkeley Center for Long-Term Cybersecurity, Jesse Goldhammer, Associate Dean, UC Berkeley School of Information and Betsy Cooper, Executive Director, UC Berkeley Center for Long-Term Cybersecurity, submitted by Mr. Hurd .. 86

REVIEWING FEDERAL IT WORKFORCE CHALLENGES AND POSSIBLE SOLUTIONS

Tuesday, April 4, 2017

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:30 p.m., in Room 2154, Rayburn House Office Building, Hon. Will Hurd [chairman of the subcommittee] presiding.

Present: Representatives Hurd, Kelly, Raskin, Connolly, and Krishnamoorthi.

Mr. HURD. The Subcommittee on Information Technology will come to order. And without objection, the chair is authorized to declare a recess at any time. But I don't think we're going to have to today, which is rare for once, right? And I want it say good afternoon to everyone. Thanks for being here.

We are at a very pivotal time in our Nation's history. As technology becomes more and more a part of our lives, our society and institutions must keep pace. But the technology itself is only half the equation, as all of you know. Technology still requires people—people to monitor, upgrade, inspect, and safeguard the technology.

That is why we are here today: to discuss the human element and the policies we as a Congress need to advance the Federal IT workforce and make sure it is comprised of qualified IT and cybersecurity professionals.

Right now, Federal agencies are facing a shortage of IT and cybersecurity professionals in a highly competitive marketplace. During one of our last hearings on this subject, one witness testified that 209,000 cybersecurity jobs went unfilled in 2015. That's a pretty large number.

That's why I've been advancing the idea of a Cyber National Guard, which was first brought up to us at a field hearing in Chicago. So thank you, Robin Kelly. And this is really a way to talk about how do we recruit and hire qualified individuals to the Federal IT workforce and then retain their skills in the future on a rotational basis.

It's real simple. Most of these hearings I usually know the answer to the questions that I'm going to ask. This is one where I do not.

And the idea is this: What are the gaps in the CIOs' offices from GS–13 below. We have to figure out what that gap is, right, and we are working to do that so that we can figure out what are those jobs that we are trying to target. Do we do it by giving high school

kids scholarships to go to college? Do we do it by forgiving debt for people that have the jobs who need to go into those positions that we need? If it is giving scholarships, where do we find the money?

So that's the first piece. Once we identify the need, the first step is, how do we get young people into their first step being the Federal Government and the dot-gov space?

The second piece is, how do we, once they come and work for the government and they go out in the private sector, how do we get them back in on a rotational basis? What are the jobs that would be achieved through that rotational basis? The jobs are going to be different than the ones that we're trying to target by creating some kind of scholarship program.

The concept is actually quite simple. And then once we figure out how we get these people back in on a rotational basis, how often will they do that? You know, the National Guard is the proverbial 1 weekend a month, 2 weeks a year, but does that have enough—that's going to impact business processes at that company. Is it 10 days a quarter? Is it 15 days every 6 months? And what are those jobs that those people can be coming back into and working on?

These are the steps in the process, I see it three phases, once we identify what jobs we're going to target, and hopefully we have some time to explore these ideas here today.

And with that, it is my honor and my privilege to introduce not only the ranking member of this committee, but my good friend, Robin Kelly, from the great State of Illinois.

Ms. KELLY. Thank you, Mr. Chairman, and welcome to the witnesses. Mr. Chairman, thank you for calling today's hearing concerning the challenges to hiring IT professionals in the Federal Government.

In 2016, GAO said that the persistent cyber threat presented a risk to our national security. We should understand that the inability to attract and retain qualified cyber professionals throughout the government threatens our ability to address cyber threats. So the workforce issue this hearing is concerned with has the potential to impact the safety of each and every American and the stability of our country.

America's leading companies are facing a similar situation. (ISC)2 projects a shortage of 1.8 million cyber professionals across both the public and private sector by 2022. We obviously face similar challenges in hiring.

Both the public and private sectors face sophisticated cyber threats. Last month, the Justice Department charged two Russian intelligence officers with orchestrating a hack that stole data from 500 million Yahoo users, of which I was one. I shouldn't have to remind anyone that in January of this year our intelligence agencies also found that the Russian Government orchestrated a sustained campaign against our elections using various weapons, including cyber attacks on political parties.

While we view the public and private sector as separate, cyber criminals and nefarious state actors do not care about those distinctions. For instance, the data stolen from the Yahoo attack was used to spy on both bank executives and White House employees.

Addressing the threat requires that government and the private sector both succeed in finding qualified individuals. For one thing,

we desperately need to expand the pool the talent that we are both joining from and keep the professionals that are so critical to protecting the security of our Nation.

Talented women and minorities are not just being hired. Currently, women hold 28 percent of science and engineering jobs. Hispanics and African Americans hold 6 percent and 5 percent of those jobs, respectively. We need to improve these numbers as we grow the number of available IT professionals.

Another problem was created by the President himself. The President's hiring freeze is obviously a barrier to recruiting and hiring the IT professionals the government needs. Nextgov points out that the hiring freeze sends a message that IT professionals are not valued in the Federal Government. These highly desired candidates could instead choose to go to the private sector where they are heavily recruited.

Also, constant calls to cut the Federal workforce and strip them of protections will not help attract needed talent. Who would want to work for an employer that publicly criticizes them and constantly questions the need for them? Candidates with numerous options certainly would not.

I look forward to hearing the witnesses' ideas to address this issue and expand the pipeline of diverse, qualified, and valued candidates. It is important that the candidates we recruit to address the next generation of challenges are representative of our population at large.

I'm glad you came to Chicago and got that idea. Thank you, Mr. Chairman.

Mr. HURD. Thank you, Ranking Member Kelly.

I'm going to hold the record open for 5 legislative days for any members who would like to submit a written statement.

Now we are going to recognize our panel of expert witnesses.

I'm pleased to welcome Steven Cooper, the former CIO for the U.S. Department of Commerce, not a stranger to this committee.

Ms. Elizabeth Hyman, executive vice president of public advocacy for CompTIA.

Thanks for being here, Elizabeth.

Ms. Lisa Depew, head of industry and academic outreach for Intel.

You guys, I was just down in your facility in Austin.

Dan Waddell, managing director for (ISC)2.

Nick Marinos, director of information technology at the U.S. Government Accountability Office.

Thanks for being here, Nick.

Finally, Ms. Debora Plunkett, a Strategic Advisory Board member for the International Consortium of Minority Cybersecurity Professionals.

Welcome to you all. And pursuant to committee rules, all witnesses will be sworn in before you testify. So please rise and raise your right hand.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth, so help you God?

Thank you, and please be seated.

Let the record reflect that the witnesses answered in the affirmative.

To allow ample time for discussion, I would appreciate if you would limit your opening remarks to 5 minutes, and your entire written statements have been made part of the record. So I appreciate that.

We are going to start off with Mr. Cooper for your opening remarks for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF STEVEN COOPER

Mr. COOPER. Chairman Hurd, Ranking Member Kelly, members of the subcommittee, thank you for inviting me to appear before you today. I am honored to join this panel to offer a few ideas regarding the Federal IT workforce.

Having been trained by the best government lawyers, I would like to state at the outset that the opinions and ideas I will share are my own and not offered on behalf of any government agency or industry organization.

Mr. HURD. So noted.

Mr. COOPER. Thank you.

I have had the privilege of serving as a public CIO in three different departments over the last 15 years before retiring in January as the CIO of the Department of Commerce. I am honored to have served as an appointee in both Republican and Democratic administrations—and as a career govie—all at the senior executive level. I share this background because I strongly believe in improving the skills, capability, effectiveness, and esprit de corps of the Federal IT workforce is a bipartisan issue.

I have directly addressed many of the challenges we will likely discuss today and have experienced success in overcoming many, but not all, of these challenges and can share my experience and learning with the subcommittee.

I can't cover all that I'd like to in my opening remarks, so I want to highlight three persistent challenges which may not be as visible or well known to members of the subcommittee, industry, and the GAO.

First, position descriptions. A position description, or PD, is required before any recruiting action can occur. Human resources reviews and approves all PDs before a position can even be posted.

Very few IT personnel, including myself, are trained and skilled at writing robust PDs. The current library of IT PDs within an agency or available from OPM do not adequately reflect the skills needed by today's workforce, much less what is coming at us in the next few years. Too many are obsolete.

Even more concerning to me, PDs don't even exist for emergent roles related to digital forensics, data science, artificial intelligence, the internet of things, drone technology, autonomous vehicles. I think you get my point.

In my experience, not having an up-to-date HR-approved PD cause delays of up to 6 months in the recruiting process. One idea to fix this, with collaboration from OMB, the Federal CIO Council, and the Federal Chief Human Capital Officers Council, tasked

OPM as the lead agency to develop a PD library of preapproved current and emerging IT roles available for use by any Federal agency. I'd even toss in State and local government.

Second, promotions. When an individual's first hired into the Federal workforce, the position they fill carries a grade level for pay and promotion purposes. In many agencies the person cannot be promoted to a higher grade without competing for that position because there is no approved way to do what I think of from the private sector and referred to in government sometimes as an in-line promotion without competition, particularly for supervisory positions. Competition is good, and the best do rise to the top.

And here is the unintended consequence of this process. I had some of my most qualified cyber employees leave my offices, either for industry or for another department, because we did not have open positions for which they could compete to be promoted at a time they are were ready; or they were not selected and then chose to leave for another agency who could offer a promotion.

My idea to fix this? Again, task OPM as the lead agency to create and standardize career ladders by role to allow in-line promotions for qualified employees when they are ready for promotion. You can kind of get a lot of information about this from the private sector.

Third, filling cybersecurity positions. When I left Commerce in January, there were 10 cyber vacancies in my office. With a continuing resolution and the hiring freeze in place, those positions remain empty as I speak.

How do we address this shortage? Chairman Hurd has spoken previously about the concept of the Cyber National Guard. I fully support the concept of having trained, skilled cyber personnel at the ready who can be put into service with very short notice, much like the FEMA disaster corps, another model.

Another service model could reflect a formal agreement or contract like the military reserves. This Cyber Reserve Corps could drill each month alongside their government counterparts and could be activated for longer periods of time to assist agencies in response to a breach or to assist in deployment of new security patches. Those are just two examples.

I've also spoken previously about a loan employee program, similar in concept to the IPA program with academia, which could provide skilled IT managers and technical professionals for up to 2 years.

In closing, I know I have not addressed all the challenges facing the Federal IT workforce in my opening statement. However, I am confident that with the leadership of the committee members and the GAO, solutions to existing problems can be found in a collaborative partnership between government and industry.

I look forward to your questions.

[Prepared statement of Mr. Cooper follows:]

STATEMENT OF STEVEN COOPER

"Reviewing Federal I.T. Workforce Challenges and Possible Solutions"

Subcommittee on Information Technology of the Committee on Oversight and Government Reform

Tuesday, April 4, 2017

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

Thank you for inviting me to appear before you today. I am honored to have this opportunity to provide input to the ongoing dialogue addressing challenges which adversely impact the recruitment, development, and retention of the Federal IT Workforce and offer a few ideas about potential solutions. I would like to state at the outset that the opinions and ideas I will share are my own, and are not offered on behalf of any government agency or industry organization.

I have had the privilege of serving as a Federal CIO in three different departments over the last 15 years – as the first CIO of the Department of Homeland Security; as the CIO of the FAA's Air Traffic Organization, and then as the Deputy and Acting CIO of the FAA; and most recently, as the CIO of the Department of Commerce. I am honored to have served as an appointee in both a Republican and a Democratic Administration, as well as in a career role, all at the Senior Executive Level. I share this background because first and foremost, I strongly believe that improving the skills, capability, effectiveness, and *esprit de corps* of the federal IT workforce is of bipartisan interest. Second, because I have directly addressed many of the challenges we will likely discuss today. And last, and perhaps most important, because I have experienced success in overcoming many, but not all, of these challenges, and can share my experience with the subcommittee.

I want to highlight three persistent challenges which get in the way of recruiting and retaining talent in the federal workforce which may not be as visible or well known to members of the Subcommittee, industry, and the GAO.

1. Position Descriptions

A position description, or PD, is required before any recruiting action can occur. Human Resources reviews and approves all PDs. Very few IT personnel are trained and skilled at writing or developing PDs. The current library of IT PDs held available within an agency, or from OPM do not always reflect the skills needed by today's workforce. Simply put, too many are obsolete, and even more concerning, *do not exist* for key roles related to cybersecurity, digital forensics and risk management, data science, artificial intelligence, predictive analytics, the Internet of Things, drone technology, autonomous vehicles, and emerging technologies. In my experience, not having an up-to-date, HR approved PD caused delays of up to six months in the recruiting process.

An idea to fix this across government: Task OPM as the lead agency, with support from OMB, the federal CIO council and the federal CHCO council, to develop a PD library of HR approved current and emerging IT roles available for use by any federal agency.

2. Promotions, Career Growth, and Retention

When an individual is first hired into the federal workforce, the position they fill carries a grade level for pay and promotion purposes. In many cases, the person cannot be promoted to a higher grade without competing for that position. To make my point, consider this: if a person is hired into government at a GS-9 position out of college, and then must compete for each grade level promotion, that person must successfully emerge as the highest rated candidate six separate times in their career to achieve a GS-15 grade level. And this is true only if there are open positions at each grade level for which an employee can compete. Using cybersecurity as a real example, I had some of my most qualified employees leave my office either for industry or for another department because there were either no open positions at their next grade level, or they were not selected.

Contrast this with my experience in the private sector. At one of the Fortune 200 companies for which I worked, hiring of entry level and mid-level positions,

including IT, were done via a formal process run by the operational managers as a team across each operating unit. Each manager participating was trained in the selection process, which required a three-day course including mock interviews and graded evaluations. This company hired the best candidates with the intention of retaining these employees for a career, not just to fill a vacant position. Once hired, the company ensured each employee had a coach to develop a career path. Once each employee reached two years of employment with the company, they went through an evaluation process to identify high potential and high performing employees. These employees were then put on a fast track which identified in advance positions which would enable these employees to grow and gain key skills as well as enable them to be promoted as they were deemed ready to take on more responsibility. The promotions were done without competition in most cases. This approach ensured and proved very successful in retaining and rewarding the most valued employees. This approach is not possible in the federal government.

An idea to fix this across government: Task OPM as the lead agency, with support from OMB, the federal CIO council and the federal CHCO council, to standardize career ladders to allow in line promotions for qualified employees when they are ready for promotion.

3. Filling Cybersecurity Positions

When I left Commerce, there were 10 unfilled cyber positions. With the CR and the hiring freeze in place, those positions remain empty as I speak. How do we address this shortage?

Chairman Hurd has spoken previously about the concept of a Cyber National Guard. I have spoken previously about a 'loaned employee' program, similar in concept to the IPA program with academia. One concept to directly address the lack of skilled cybersecurity professionals in the federal workforce is to have trained, skilled personnel 'at the ready' who can be put into service with very short notice like the FEMA disaster corps. Another model could reflect a formal

agreement or contract, like the military reserves. This cyber reserve corps could drill each month in federal agencies alongside their government counterparts, and could be activated for longer periods of time to assist agencies in response to a breach, or particularly harmful new malware.

In closing, I know I have not addressed all the challenges facing the federal IT workforce regarding recruiting, development, and retention. However, I am confident that with the guidance of the committee and GAO, solutions to the problems that exist can be found in a collaborative partnership between government and industry.

Thank you for allowing me to participate in this hearing. I look forward to answering any questions you may have.

Appendix A - I offer my simplified table of problems and solutions.

Problem	Cause	Solution
Recruiting – can't hire top candidate(s)	• Salary too low • No position at needed grade level • No hiring bonus • No relocation funding	• Authority for special pay or incentives related to key skills like cybersecurity
Recruiting – takes too long	• Approved PDs not easily available or don't exist • Veteran's Preference does not always produce best qualified candidates	• Create library of approved PDs for use by all agencies • Direct hiring authority for key skills like cybersecurity (exists currently for cyber)
Recruiting – can't attract top candidates	• Don't want to work in government	• Provide scholarships in return for agreed term of federal service • Provide student loan forgiveness in exchange for agreed term of federal service
Retention	• Employees leave for promotion or higher pay • Employees do not feel recognized or rewarded for their work	• Pay a retention bonus • Give a competitive cash award for employees/teams providing significant operational solutions

Career Development	• Certifications lacking • Skills lacking	• Pay a bonus for obtaining selected certifications • Reimburse employees for education directly related to obtaining selected skills on a sliding scale (100% for an A, 75% for a B, 50% for a C, 25% for a D, 0% for an F)
Insufficient skilled candidates	• Returning Vets and unemployed workers may not have needed skills •	• Training programs with community colleges and universities for cyber skills, needed IT skills

Mr. HURD. Thank you, Mr. Cooper. I look forward to asking you questions.

Ms. Hyman, you're now recognized for 5 minutes.

STATEMENT OF ELIZABETH HYMAN

Ms. HYMAN. Terrific. Thank you.

Good afternoon and thank you, Mr. Chairman, Ranking Member Kelly, for inviting us here today. I'm here on behalf of CompTIA, which is a nonprofit tech trade association. We represent approximately 2,000 member companies, 3,000 academic and training partners, and 100,000 registered users for our organization.

Government and the private sector have a shared challenge: to have in place the right skilled workforce to utilize technology, enhance productivity, and mitigate and manage security threats. And this is what I'd like to discuss briefly today.

In many ways the creation of CompTIA certifications—and I should add that we are the leading global provider of vendor-neutral IT workforce certifications, and we in many ways have created a de facto framework, along with our brethren certification bodies. CompTIA provides a route from entry to advanced-level skills called the cybersecurity career pathway recommendation, and it takes a beginner in IT and it equips them with 5 to 10 years of the equivalent knowledge, skills, and abilities needed by all cybersecurity professionals.

We have sought to share the lessons that we've learned in developing and deploying these certifications with the government as it has sought to create frameworks and standards to train and validate government employee IT skills, and particularly in cybersecurity.

A few successful public-private partnerships for your consideration today. The Department of Defense has worked closely with the training and certification community as they developed its 8570 and successor 8140 initiatives. These require that DOD personnel and contractors with information assurance responsibilities in their job roles have to have industry-recognized certifications.

Also of note and a part of the fiscal year 2016 omnibus appropriations bill is the Federal Cybersecurity Workforce Assessment Act, and it directs the Federal Government to take stock of the certifications held by the existing cyber workforce to determine what skills may be missing currently in that workforce.

NIST has also collaborated with CompTIA and our partner Burning Glass to develop a real-time heat map for supply and demand of cybersecurity workers in the United States. This is called CyberSeek, it is available at CyberSeek.org.

CompTIA is also supportive of the DHS National Initiative for Cybersecurity Careers and Studies, the NICCS portal, and the National Initiative for Cybersecurity Education. And in my comments I discuss those—the written testimony—at greater length.

I'd also like to share that CompTIA as a certifying body regularly conducts research gauging the value and impact of certifications. Our research confirms that testing after training helps to set a baseline of expertise among staff, provide career path guidance, improve the performance of a team, retain talented staff, and helps to evaluate staff with promotions or career development.

There's no question that technology sector jobs are growing. Nevertheless we struggle to fill job openings every year with roughly a million job postings in the IT sector. This is not to say that every job posting must or will be filled, but with nearly 800,000 tech workers expected to retire through 2024, this only adds to what we call the skills gap. Therefore, we will all need to focus on innovative ways to attract more people to tech careers, and particularly in the area of cybersecurity, and there's a few areas that I'd like to highlight.

We ourselves have put forward a proposal to be included in the fiscal year 2018 NDAA for a "Service to Cyber Warriors" program that would provide a stipend for veterans and members of the Armed Forces to cover the expenses of IT training, materials, certifications, and other employment-seeking services.

We also supported the introduction of the State Cyber Resiliency Act, which on the workforce front encourages States to develop cyber resiliency plans to fulfill the essential functions of mitigating talent gaps in the State government cybersecurity workforce.

The DOD Cyber Scholarship Program Act and the Cyber Scholarships Opportunity Act were recently introduced in Congress. The overarching goal of these legislative proposals is to build a robust cybersecurity workforce. These proposals, in our view, could only be strengthened by recognizing training and industry-recognized certifications as yet another pathway in addition to 2- and 4-year college opportunities.

Finally, CompTIA also supports apprenticeships and vocational models for building out our Nation's IT workforce and cybersecurity workforce. We are now working with a number of House and Senate offices on a legislative proposal, not yet introduced, which is called the Championing Apprenticeships for New Careers and Employees in Tech Act, with the goal of scaling up the number of apprenticeships in our country.

In summary, we are grateful that you've raised this topic today. We strongly believe that the Federal Government can be a leader in building the tech workforce. It can do so by continuing to support the great work that has already been done by DOD, NIST, and other agencies, by insisting that educational pathways include not only 2- and 4-year college educational programs, but also industry-recognized certifications and experiential learning, and by developing and resourcing innovative programs that will encourage more people to enter into a tech and cybersecurity career through the government.

And I thank you for the opportunity to share this with you and look forward to your questions.

[Prepared statement of Ms. Hyman follows:]

CompTIA.

The Computing Technology Industry Association
Subcommittee on Information Technology of the House Oversight and Government Reform Committee Hearing Testimony: "Reviewing Federal I.T. Workforce Challenges and Possible Solutions"
April 4, 2017

Introduction to CompTIA

We commend the Subcommittee on Information Technology of the House Oversight and Government Reform Committee for holding this hearing to solicit input regarding federal information technology (IT) workforce challenges and solutions, particularly in cybersecurity and as it relates to industry certifications.

CompTIA is a non-profit, high-tech trade association with approximately 2,000 member companies, 3,000 academic and training partners, and over 100,000 registered users.

CompTIA is the second largest IT certifying body in the world with more than two million vendor-neutral certifications issued globally. The CompTIA certifications most commonly recommended or required by federal agencies (CompTIA A+, CompTIA Network +, CompTIA Security+, and CompTIA Advanced Security Practitioner) are International Standard ANSI/ISO/IEC 17024 certified. [1]

Through all our activities, CompTIA is dedicated to advancing industry growth and workforce development through educational programs, market research, networking events, professional certifications, and public policy advocacy.

---

[1] In March, CompTIA unveiled a new exam to this suite of offerings: CompTIA Cyber Security Analyst or the CSA+ certification, which offers broad-spectrum validation of knowledge and skills required to configure and use cyber-threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization.

CompTIA welcomes the opportunity to discuss the federal workforce amidst a world defined by digitization and interconnectivity. Shortcomings in IT and cybersecurity expertise and experience make for an ever-more precarious situation. Government and the private sector alike have a challenge: to have in place the right skilled workforce to utilize technology, enhance productivity, and mitigate and manage security threats. We would like to share with you CompTIA's experience in working with the Federal government to enhance IT workforce skills; why we believe that workforce certifications fill a vital role in skilling the federal workforce; and what creative solutions for ensuring we have a skilled and able federal workforce are currently being discussed.

Helping to Establish Frameworks and Knowledge through Public-Private Partnerships

In many ways, the creation of CompTIA certifications, and those of many of our bretheren certifying bodies, have established a *de facto* framework for cybersecurity providing a pathway from entry-level to expert. For example, nearly a half million people are CompTIA Security+ certified. Cyber is also a crucial component of foundational IT certifications like CompTIA A+ and Network+. And CompTIA recently introduced Cyber Security Analyst (CSA+) to address the growing importance of big data analytics in cyber defense.

CompTIA exams are refreshed continually and undergo a complete rebuild every three years. They include practical knowledge based and performance based (simulation) questions that require test takers to have the knowledge they need to fill job roles. For credentials to remain valid after three years IT pros must commit to continuing education to prove their knowledge is up to date with the latest trends.

As the number of CompTIA certification holders has grown, we have sought to share and translate many of the lessons learned in creating and deploying these certifications with government as it has sought to create frameworks and standards to train and validate government employee skills in IT and cybersecurity.

To summarize, certifications are used to help professionalize the cyber workforce and help provide a common lexicon of the skills needed across the public and private sector. To this end, CompTIA would like to make the Committee aware of effective strategies and programs that are

currently being used to promote public and private sector cooperation in ensuring a robust and high-skilled IT workforce.

The Department of Defense (DoD) has worked closely with the training and certification community to consistently up-skill workers. Many certification organizations have participated in the 8570[2] and successor 8140[3] initiatives. These initiatives, which require DoD personnel and contractors with information assurance titles (as defined by DoD) to have certain cybersecurity certifications, are vital for the U.S. Government workforce. This requirement ensures individuals are trained and certified in the skill sets required by their job. DoD's cyber workforce management strategy not only enhances our national security and ensures value from taxpayer investments in IT training, but it also assists DoD in meeting its IT/cybersecurity personnel retention goals. DoD training and certification programs have also supported the consistent goal across several administrations to help our veterans transition their skills to civilian employment once their military service has ended.

The DoD model has been so successful that CompTIA encourages the U.S. Government to lead by example and encourage other federal civilian agencies to adopt similar comprehensive programs. Related to this, CompTIA encourages Congress to review and consider updating the Government Employees Training Act (GETA)[4] to ensure that all federal government agencies have the flexibility needed to use resources allocated for IT training to pay for industry-recognized certifications where appropriate. It has been demonstrated through research individuals in training learn and retain more when they understand a certification exam will be required at the end of the process.

We also know the U.S. Government relies on the use of industry-recognized certifications for professional development. This is evidenced by the Department of Homeland Security's (DHS) National Initiative for Cybersecurity Careers and Studies (NICCS) portal, which highlights that certifications play a large role in getting people the skills they need to enter the cyber workforce.

Further, the FY16 Omnibus Appropriations Bill included the Federal Cybersecurity Workforce Assessment Act, directing the federal government to take stock of the certifications held by the

[2] DoD 8570.01-M, Information Assurance Workforce Improvement Program, December 19, 2005 (with updates)
[3] DoD Directive, Number 8140.01, August 11, 2015
[4] Title 5, U.S. Code, Ch. 41, Sec 4100

existing cyber workforce to determine what skills may be missing. We understand implementation is underway and encourage the Committee to conduct oversight of these assessments and to provide federal agencies with the resources needed to implement any mitigation plans proposed to address skills gaps and the absence of certifications.

The National Initiative for Cybersecurity Education (NICE) is also a critical element to properly training the nation's workforce. As you may know, NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. CompTIA worked with NIST to map our certifications to the NICE workforce framework categories. We have provided as an appendix, a visual representation of that mapping to present a clearer picture of how CompTIA certifications validate cyber knowledge and skills categorized in the NICE framework. Significantly, the DoD 8140 directive aligns job roles with the NICE framework.

CompTIA has also worked closely with the National Institute of Standards and Technology (NIST) to provide real-time information concerning the location of qualified IT workers. To that end, in 2015, CompTIA, in partnership with Burning Glass Technologies, received a three-year grant from NIST to develop an interactive cyber jobs heat map that shows the demand for and availability of critical cybersecurity jobs (mapped to the NICE Framework) across the nation. The project, which is being funded through NICE, provides data to help employers, job seekers, policy makers, training providers, and guidance counselors meet today's increasing demand for cybersecurity workers. The heat map was released in October 2016 under the name **CyberSeek.org**. A few high level data points:

- According to CyberSeek, every year in the U.S. there are 128,000 openings for Information Security Analysts, but only 88,000 workers currently employed in those positions – a talent shortfall of 40,000 workers for cybersecurity's largest job.
- There are 220,000 additional openings requesting cybersecurity-related skills, and employers are struggling to find workers who possess them. Jobs requesting cloud security skills, for example, remain open 96 days on average – longer than any other IT skill.

Understanding the types of cyber jobs that are in demand and where supply falls short is vital to ensuring that we are preparing individuals with the right skills for the jobs in demand.

The Value of Training and Certification

We also believe it is critical we in the certification industry constantly gauge the value and relevancy of certifications. To that end, CompTIA conducted research on managers' perceptions of the importance of testing after training. Our research on this topic targeted DoD, which we believe has set the "gold standard" for building a robust IT and cybersecurity workforce. CompTIA's Military Career Path Study found that 74 percent of active duty military personnel with staff management responsibilities classified testing after training to confirm knowledge gains as "very important."[5] Further, these managers reported that testing after training also helped to set a baseline of expertise among staff, provide career path guidance, improve the performance of a team, retain talented staff, and evaluate staff for promotions or career advancement.[6]

According to a study conducted by the International Data Corporation (IDC) and sponsored by CompTIA, candidates and staff with CompTIA A+ and CompTIA Security+ certifications perform better than staff that is not certified. According to the research, certified employees are: (1) more confident; (2) more knowledgeable; (3) reach job proficiency more quickly; (4) more reliable; and (4) perform at a higher level.

When IT professionals are confident in their abilities, they are more likely to be forward thinking, proactively anticipate issues, and solve problems before those problems impact organizational performance. Further, certified professionals are 85 percent more likely to believe they have the knowledge and skills needed to successfully fulfill their jobs.[7] As a result, these certified security professionals are better positioned to properly assess risks, design and implement interventions, and correct policy weaknesses.

Because most of today's hiring environments prioritize experience above professional credentials, it is also important to note that CompTIA's research has found that after ten years of security experience or support experience, certified staff has between 20 and 25 percent more core domain knowledge than those with the same experience who are not certified. Once on the

[5] CompTIA 2014 "Military Career Path Study: Assessing the Role of Training and Certifications."
[6] Id.
[7] CompTIA 2014 IT Support and Security Performance Study: The Impact of CompTIA Certifications on Organizational Performance.

job, certified IT professionals have also been found to perform up to 53 percent better than those without certification in critical, job-related activities.[8]

Further, certifications help to put program managers at greater ease with the capabilities of their staff. Ninety-three percent of human resources (HR) executives believe certifications are beneficial, as they offer a competitive edge in the job market, heightened career advancement opportunities, and increased value to employers and their organizations.[9] According to employers, the top benefits of IT certification are: (1) the ability to understand new or complex technologies; (2) higher productivity; and (3) more insightful problem, solving.[10] In addition, CompTIA has found that roughly 8 in 10 hiring managers say it is challenging to find the right candidates with the right skill sets to fill vacant IT positions and verifying job candidates' credentials can be a challenge.[11]

Creating a Pipeline for IT and Cybersecurity Talent

While CompTIA is best known for validating the skills of the existing and aspiring IT and cybersecurity workforce, we recognize a steady talent pipeline is needed to ensure the IT and cybersecurity workforce of the future. Our nation is struggling to fill job openings with roughly 1 million open IT job postings each year. This is not to say that every job posting must or will be filled, but many of these are desirable positions, especially as several of these job vacancies have an average starting salary of $50,000 with growth into the six figures.[12]

We believe IT/cybersecurity should be given strong consideration as a profession for individuals looking to enter or re-enter the workforce or make a career change. This is especially true because a formal degree is not the only entry point for a successful career in IT/cybersecurity. If formal education is needed, very often a two-year community college degree will suffice. There are also a number of training programs that are not tied to academic institutions, but offer industry-recognized certifications to start individuals on career pathways in cybersecurity. To clarify, there is a varying level of cyber worker. The "cyber ninja," who is at the top of the IT/cyber workforce pyramid, may require a lot more training and formal education. However,

---

[8] Id.
[9] CompTIA 2015 IT Careers Blog: Four Reasons HR Execs Love Certifications.
[10] Id.
[11] Id.
[12] Source: Burning Glass Technologies.

many cybersecurity and IT jobs do not require a four-year college degree and present solid employment opportunities.

We are aware of efforts at the federal level aimed at creating tuition reimbursement for cybersecurity degrees. We ourselves have put forward a proposal, to be included in the FY18 National Defense Authorization Act (NDAA), for a "Service to Cyber Warriors" program that would provide financial assistance in the form of a stipend, available to veterans and members of the Armed Forces without any requirement of prior IT experience, industry-recognized certification, or advanced degree. Under our proposal, up to $5,000 in stipend funds may be made available to a participant to cover the expenses of IT training, training materials, industry-recognized certification exam voucher fees, and other employment seeking services.

We acknowledge that creating a workforce pipeline is only part of the problem; the federal government also faces significant retention challenges. Due to our extensive work with DoD, we know the Department's ability to remain competitive with the private sector in compensation can impact retention goals. Therefore, we are also proposing a bonus payment of up to $10,000 for Program participants who agree to enter into a contract service agreement for full-time employment in a cyber work role at a federal, state, or local government agency for a period of time to be specified by the Secretary of Defense.[13]

A number of similar proposals have recently been introduced in Congress. For example, CompTIA has supported the State Cyber Resiliency Act introduced in the House by Representatives Kilmer (D-WA) and Comstock (R-VA) and in the Senate by Senators Warner (D-VA) and Gardner (R-CO). On the workforce front, this legislation encourages states to develop cyber resiliency plans to fulfill the essential functions of mitigating talent gaps in the state government cybersecurity workforce, enhancing recruitment and retention efforts, and bolstering the knowledge, skills, and abilities (KSAs) of state government personnel to protect against cyber threats and vulnerabilities. Further, the bill allows states to use implementation grant funds to establish programs, such as scholarships or apprenticeships, to provide financial assistance to state residents who pursue formal education, training, and industry-recognized

[13] Priority will also be given to those who agree to seek employment in a state with low cybersecurity workforce supply and high cybersecurity workforce demand, as identified by the National Institute of Standards and Technology (NIST) (via CyberSeek).

certifications for careers in cybersecurity as identified by NICE and commit to working for state government for a specified period of time (based on Virginia's successful Cybersecurity Public Service Scholarship Program).

Also, recently introduced are the DoD Cyber Scholarship Program Act and the Cyber Scholarships Opportunity Act. CompTIA supports the overarching goal of these legislative proposals to build a robust cybersecurity workforce. We believe these proposals could only be strengthened by recognizing training and industry-recognized certifications as yet another pathway to upskilling the federal workforce. We believe the federal government can continue to demonstrate leadership and work towards swifter and more cost-effective achievement of its IT/cyber workforce goals by prioritizing resources for training and industry-recognized certifications. CompTIA believes such initiatives could have tremendous impact among members of the federal workforce who are not enrolled in four-year institutions.

Finally, CompTIA also supports apprenticeships and vocational models for building out our nation's IT/cybersecurity talent pipeline. We believe the real-world experiences that can be gained through these types of apprenticeship and vocational positions can only enhance an individual's training for a successful career in IT/cybersecurity. We are now working with a number of House and Senate offices on a legislative proposal, called the Championing Apprenticeships for New Careers and Employees (CHANCE) in Tech Act, to scale up the number of tech apprenticeships in our nation.

Conclusion: The IT Skills Gap

All of these proposals address the issue of a skills gap. According to the Bureau of Labor Statistics, by 2022, more than 25% of U.S. workers will be 55 years old or older, up from 14% in 2002. In the sphere of IT, nearly 800,000 workers are expected to retire through 2024.[14] And even within the federal government, according to the Office of Personnel Management (OPM), from 2006 through 2015 there were nearly 24,000 retirements from the federal civilian workforce of IT management personnel.[15]

[14] CompTIA Research Brief: "Assessing the IT Skills Gap", March 2017
[15] United States Office of Personnel Management, "Executive Branch Retirement Statistics: Fiscal Years 2006-2015."

Across the board, we are seeing IT talent leave and a shortfall of talent taking their place. While the notion of a skills gap is a seemingly straightforward concept, below the surface, there are many nuances to the story. At the most basic level, skills gap can be characterized as the variance between the performance employers desire from their workforce and what workers can or choose to deliver. Things get murky when skills gap discussions venture into other workforce challenges, such as gaps in labor supply, pipeline, locations, or generational. For example, what may be thought of as a skills gap by an employer may in fact be a difference in millennial work styles. Obviously, knowing what to fix must precede discussions of how to fix it.

In closing, as this Committee considers innovative ways in which to address meeting a skills gap in the federal workforce, it should consider the various nuances that we have outlined. Generational, financial, and career path considerations are all equally as relevant in the federal workforce as it is in the private sector.

Mr. HURD. Thank you.

And, Ms. Depew, I think I incorrectly identified—it's a new thing, right? That is McAfee rather than Intel. But I would like to thank you and your colleagues at Intel for planting the seed in Chicago on this important topic. And now you're recognized for 5 minutes in your opening remarks.

STATEMENT OF LISA DEPEW

Ms. DEPEW. Good afternoon, Chairman Hurd, Ranking Member Kelly, and distinguished members of the subcommittee. Thank you for the opportunity to testify today.

I am Lisa Depew, head of industry and academic outreach for McAfee. I've spent nearly 20 years in the technology industry in a wide range of engineering positions, focusing the last few years on cybersecurity.

I am pleased to address the committee on Federal IT workforce challenges, an important issue McAfee understands well. My testimony will briefly describe the problem, offer some specific solutions, and recommend cultural changes to mitigate our cybersecurity skills shortage.

In 2016, Intel Security and the Center for Strategic and International Studies undertook a study titled "Hacking the Skills Shortage," based on global survey of IT professionals. Eighty-two percent of those surveyed reported a lack of cybersecurity skills within their organization, 71 percent agreed that the talent shortfall makes organizations more vulnerable to attackers, and 25 percent say that the lack of sufficient cybersecurity staff has actually contributed to data loss or theft and reputational damage.

The cybersecurity workforce shortage is projected to reach 1.8 million by 2022, according to the most recent Global Information Security Workforce Study. We see a significant lack of diversity in the workforce as well. Bureau of Labor Statistics numbers indicate in North America women constitute only 14 percent of the information security workforce and African Americans comprise only 3 percent of information security analysts in the U.S.

The cybersecurity skills shortage is particularly acute in the Federal Government. Tony Scott, the Federal Government's former CIO, indicated an estimated 10,000 openings in the Federal Government for cyber professionals that couldn't be filled because the talent supply simply wasn't available.

McAfee would like to make the following recommendations for closing the skills gap.

First, expand the current CyberCorps program. The CyberCorps Scholarship for Service program is designed to increase and strengthen the cadre of Federal information assurance specialists that protect government systems and networks by supporting collegiate students with funding, internships, and work opportunities.

Policymakers should expand funding for this initiative. For context, $40 million pays for roughly 1,500 students to complete the scholarship program. We recommend extending funding to the $180 million range. Supporting 6,400-plus scholarships would make a significant dent in the estimated 10,000-worker Federal cyber skills deficit.

Additionally, government should consider creating a complementary community college program. A strong security operation requires multiple levels of skills, not all of which require 4-year or graduate degrees. Having a flexible scholarship program at a community college, including practical skills training and ability to earn a transferable 2-year cybersecurity certificate, could benefit a wide variety of applicants, while providing the profession with additional necessary skills.

Private companies could partner with local community colleges to establish cybersecurity-focused curricula and offer private sector practitioners as guest lecturers. The Federal Government could fund all or part of the tuition remission for students, with students again working the number of years in Federal service equal to time spent in the program.

Community colleges tend to attract a variety of students, including recent high school graduates, but also returning veterans and other adults who have pursued alternate careers. The community college option could also further ethnic and racial diversity. A community college program should not substitute, but rather complement the existing CyberCorps program.

In addition to workforce development programs, we must make systemic cultural changes to close the cyber skills gap. First, we must increase cyber safety awareness. Practicing cyber safety must become as routine to America's youth as washing hands and putting on their seat belts.

Additionally, we need to make cybersecurity accessible and appealing to a broader range of potential professionals. Graduation rates of female engineers are highest in biomedical and environmental engineering, fields where students can draw a direct correlation to helping humanity. If we better articulate the value of cybersecurity in protecting people's personal and professional lives, we have a target-rich environment of highly skilled girls and women who could be joining the ranks to fill that 1.8 million-person deficit.

In conclusion, there is much we can do to close the cybersecurity skills gap. It will take a true public-private partnership, expansion of funding and programs, and a fundamental shift in cyber safety awareness and the perception of cybersecurity as a profession.

Thank you, and I will be happy to answer any of your questions.

[Prepared statement of Ms. Depew follows:]

STATEMENT FOR THE RECORD OF

LISA DEPEW, HEAD OF INDUSTRY AND ACADEMIC OUTREACH, MCAFEE

BEFORE THE U.S. HOUSE OF REPRESENTATIVES

INFORMATION TECHNOLOGY SUBCOMMITEE OF THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

ON REVIEWING FEDERAL IT WORKFORCE CHALLENGES AND POSSIBLE SOLUTIONS

April 4, 2017 2:00 PM, 2154 Rayburn House Office Building

Good afternoon, Chairman Hurd, Ranking Member Kelly, and distinguished members of the Subcommittee. Thank you for the opportunity to testify today. I am Lisa Depew, head of industry and academic outreach for McAfee.

I am pleased to address the Committee on federal IT workforce challenges, which we all know is an issue that must be addressed. I will focus on developing cybersecurity professionals, as that is one of the greatest areas of need and also one that we at McAfee know well. My testimony will briefly describe the problem, offer some specific solutions, and conclude by discussing some of the larger issues that are integral to our cybersecurity skills shortage.

First, I would like to provide some background on my experience. For the past two and a half years, I have worked closely with McAfee's Chief Technology Officer, Steve Grobman, to identify, evaluate, and prioritize compelling new technologies and work with technical leaders throughout the company to identify and resolve challenges while building industry-leading security solutions. Currently I drive technical leadership development among our engineering community, focusing on how to maximize growth and impact of McAfee's technical talent. I expand innovation initiatives by driving collaboration with organizations like the Society of Women Engineers and university programs to accelerate partnerships and opportunities between private sector, non-profits, and academia.

Prior to joining the field of cybersecurity, I spent 15 years at Intel Corporation in a wide variety of engineering and business operations roles including microprocessor and memory design, desktop and data center customer enabling, building and managing automation services infrastructure, and streamlining support operations for millions of business PCs worldwide. I have been recognized inside and outside corporations for my advocacy for women in technology and have consulted nationally and internationally on methodologies to attract and retain a diverse and inclusive workforce.

MCAFEE'S COMMITMENT TO CYBERSECURITY

I'm extremely pleased to be able to announce that as of today, McAfee is an independent cybersecurity company which, as a standalone business, is one of the world's largest pure-play cybersecurity firms. We're built on the belief that "Together is Power," and our strategic vision focuses on innovation, trust and collaboration. We recently announced a whole new ecosystem of integrated platforms, automated workflows, and orchestrated systems based on an open

communications fabric that will enable all of us in cybersecurity to work together in ways never before thought possible. So this is a special day for us, and it's a great time to be addressing this important subcommittee.

The Cybersecurity Skills Shortage – By the Numbers

In 2016 Intel Security and the Center for Strategic and International Studies (CSIS) undertook a study titled Hacking the Skills Shortage based on a global survey of IT professionals. Some of the findings about the cybersecurity talent gap include:

- 82 percent of those surveyed reported a lack of cybersecurity skills within their organization.
- 71 percent agreed that the talent shortfall makes organizations more vulnerable to attackers, and 25 percent say that lack of sufficient cybersecurity staff has actually contributed to data loss or theft and reputational damage.
- The most desirable skills cited in all eight countries surveyed were intrusion detection, secure software development, and attack mitigation.
- 76 percent of respondents say their governments are not investing enough in programs to help cultivate cybersecurity talent and believe the laws and regulations for cybersecurity in their country are inadequate.

Since that July study, the numbers haven't improved any. The cybersecurity workforce shortage is projected to reach 1.8 million by 2022, according to the most recent Global Information Security Workforce Study. And the number of women in the field has not increased at all, coming in at only 11% globally, according to a Women in Cybersecurity report by the Executive Women's Forum and $(ISC)^2$. In North America, women constitute only 14 percent of the information security workforce. The numbers are even worse for African Americans, who comprise only three percent of information security analysts in the U.S., according to the Bureau of Labor Statistics figures cited in an article in Forbes. Compare these numbers to predicted spending on cybersecurity: Cyber economy research firm Cybersecurity Ventures has predicted that global spending on cybersecurity products and services will surpass $1 trillion cumulatively between 2017 and 2021 and that annual cybercrime costs will reach $6 trillion in 2021. Both figures indicate the serious need for more trained professionals.

The cybersecurity skills shortage is particularly acute in the federal government. Tony Scott, the federal government's former CIO, said in a GovLoop article, "There are an estimated 10,000 openings in the federal government for cyber professionals that we would love to fill, but there's just not the talent available." Given the vital role such government agencies as DoD, DHS and the intelligence agencies play in protecting the United States, this skills gap is disquieting and merits particular attention from policymakers.

One strategy for addressing the cybersecurity skills deficit is to use automation – through machine learning and artificial intelligence. We at McAfee take advantage of this, and our tools incorporate automation in strategic ways. Legacy IT systems, however – like many of those in the federal government – lack the ability to take advantage of the most contemporary security architectures and development techniques. While it is possible to isolate or wrap security around

a legacy system, the approach is far inferior to a well-designed secure implementation designed for the security challenges of 2017 and beyond.

This speaks to the need for investments in IT modernization and modern cybersecurity solutions, which the President's draft executive order addresses. We support these much-needed policy changes. In the meantime, however – and even after legacy IT is retired, replaced and modernized with current generation cybersecurity capabilities – we will still need many more skilled cybersecurity professionals.

RECOMMENDATIONS

What follows are some recommendations for closing the skills gap.

Expand the Current CyberCorps Program

The CyberCorps Scholarship for Service (SFS) program is designed to increase and strengthen the cadre of federal information assurance specialists that protect government systems and networks. The program is structured as such: The National Science Foundation (NSF) provides grants to about 70 institutions across the country to offer scholarships to 10-12 full-time students each. Students get free tuition for up to two years in addition to annul stipends -- $22,500 for undergraduates and $34,000 for graduate students. They also get allowances for health insurance, textbooks and professional development. Some universities also partner with the Department of Homeland Security (DHS) on these programs.

Students generally must be juniors or seniors and must qualify for the program by attaining a specific GPA, usually at least a 3.0 or higher. Upon completing their coursework and a required internship, students earn a degree, then go to work as security experts in a government agency for at least the amount of time they have been supported by the program. After that, they can apply for jobs in the public or private sector.

With additional funding, the CyberCorps SFS program certainly could be expanded to more institutions and more students within each of those schools. To date, the federal government has made a solid commitment to supporting the SFS program, having spent $45 million in 2015, $50 million in 2016, and the most recent Administration's budget requested $70 million. As a baseline, an investment of $40 million pays for roughly 1,500+ students to complete the scholarship program.

Given the size and scale of the cyber skills deficit, policymakers should significantly increase the size of the program, possibly something in the range of $180 million. At this level of funding, the program could support roughly 6,400 scholarships. Such a level of investment would make a dent in the federal cyber skills deficit, estimated to be in the range of 10,000 per year. At the same time, this level of investment could help create a new generation of federal cyber professionals that can serve as positive role models for a countless number of middle and high school students across the country to consider the benefits of a cyber career and federal service. Indeed, this positive feedback loop of the SFS program might well be its biggest long-term contribution.

We also recommend that the program include a "give-back" component. The students who enter this program are compensated well, they receive paid internships during their course of study,

and they are in line for federal jobs when they graduate. Yes, they are required to work for the federal government for time equivalent to what they spent in the program, but unlike many other graduates, they have a job in their field where they are enhancing their resumes and skill sets for the future. They also ought to become ambassadors in the community for the program and for solving the cybersecurity talent shortage. They should be asked to participate in a teaching or advocacy role. We would not suggest prescribing the role; rather, the graduates could use their own creativity to propose how they plan to give back. The CyberCorps SFS program should suggest some possibilities, including volunteering in middle and high schools to teach cyber skills on a regular basis, acting as mentors to students, and taking students under their wing during internships the program might establish with the federal government.

Create a Community College Program

While the CyberCorps program serves college juniors and seniors who are already well along the learning path, another program, or an expansion of the SFS program, could seek to attract high school graduates who don't yet have specific career aspirations. Private companies could partner with a community college in their area to establish a course of study focusing on cybersecurity. The federal government could fund all or part of the tuition remission for students. Interested students would be taught both by college faculty and private sector practitioners. For example, an IT company could offer several faculty members/guest lecturers who would participate during a semester. Students would receive free tuition – paid by a federal program, perhaps with private sector contributions – but they would not receive a stipend for living arrangements, as 4-year college students do in the CyberCorps program. Students would receive a two-year certificate in cybersecurity that would be transferrable to a four-year school. Like the CyberCorps program, graduates would spend the same amount of time as their scholarship period, working in a guaranteed government job.

Community colleges tend to attract a variety of students – including recent high school graduates but also returning veterans and other adult students who might have pursued other careers or might even be working full- or part-time. The community college option could also further ethnic and racial diversity in a cyber program – something that is badly needed. This diversity would be a plus rather than a minus for the cybersecurity profession, as the field requires a diverse set of skills and individuals. Not all of these skills are strictly technical, and for those that are technical, not all require high levels of formal education. You don't need a Ph.D. – or even a bachelor's degree – to work in cybersecurity. For instance, a four-year degree is not necessarily required to work in a security operations center (SOC). A strong security operation requires different levels of skills, and having a flexible scholarship program at a community college could benefit a wide variety of applicants while providing the profession with other types of necessary skills.

A program like this has the benefit of bringing in private sector experts, interesting younger students who have not yet made a commitment, interesting veterans, attracting a diverse range of students, and probably costing the government less – once the start-up costs were accounted for. Such a program should not substitute but rather complement the existing, highly valued CyberCorps SFS program.

We Need Cultural Changes to Close the Cyber Skills Gap

Cybersecurity is one of the greatest technical challenges of our time. We need more people – in addition to continually advancing technology, of course – to address this challenge. So far, we've addressed specific programs that can train individuals who have reached at least 18 years of age and might have some interest in pursuing a cybersecurity career. Now I want to step back and take a wider look at the challenges we as a society face in developing those people. I want to focus on three in specific:

- Empowering more children to understand and embrace STEM, security and privacy
- Changing the image of a cybersecurity professional, and finally,
- Addressing the gender and diversity gaps

We Need More Awareness of STEM, Security and Privacy

We've heard it before, we'll hear it again, but it still deserves an important mention: We need to invest more in exposing grade school and middle school students to science, technology, engineering and math (STEM). "The future of the economy is in STEM," says James Brown, executive director of the STEM Education Coalition in Washington, D.C., adding the most recent Bureau of Labor Statistics finding that employment in STEM jobs is projected to grow to more than nine million between 2012 and 2022. That sounds like a conservative estimate to me, and indeed it probably is. While various initiatives have sprung up to address the STEM education problem, we're not there yet – and we need to be. We need a broad-based STEM investment plan to solve this long-term problem.

But it's not just STEM awareness that children need at an early age. It's also awareness of security and privacy. As adults we hear about breaches in the news, and some of us understand cyber is a corporate board room topic, but does the average grade school and middle school student learn about the importance of cyber safety? Do they understand what that means beyond "don't share your password"? Where does security sit on the average college student's list of priorities? Look at topics affecting America's youth today: the shifting economy, cyberbullying, high rates of human trafficking (most which is executed via social media and digital transactions). We have a great opportunity to increase awareness about security as at affects the workforce at large (1.5 million unfilled jobs today and growing, steady pay, high job security) but also in a way that appeals to our millennial generation – a group passionate about causes, especially human interest ones— and generation X youth, who are learning about how to keep themselves and their friends safe. We need both traditional and creative approaches to reach these students, possibly through gamification.

We also need to systemically change the conversation around cybersecurity and raise awareness with young children in the community. America needs to instill stronger cyber safety awareness. How many times do we wash our hands a day, because we know it's key to staying healthy? How many kids put on their seatbelts without thinking, because it's a routine behavior to stay safe? We need to get to that same level of unconscious competence and cybersecurity precaution with our digital lives, and education must start with our youth. Then, once our children are attuned to cyber safety being a part of their daily lives, making the jump to choosing a career as creator/leader/protector in cyber becomes a simpler sell.

We Need to Rebrand Cyber

What does the average person envision when they think "cybersecurity"? We have to move beyond the stereotype of "hacker in a hoodie." This persona commonly elicits images of male, devious, and loner. Yet security is increasingly about creative, collaborative, and together. High-impact, valuable cybersecurity professionals can—and do—come from all walks of life, with broad and varied backgrounds. It is their diverse skills and experience that enable them to identify the corner case, look at the technology in a way other than it was intended, and think outside the box to determine how an attacker might exploit a system. The legacy tech innovator Bell Labs proved that diverse teams produce more creative, high-quality products. Similarly, a diverse incident response team will look at solutions from a multitude of perspectives and be more holistic and resilient in addressing the breadth of tomorrow's cybersecurity challenges. The attacker only has to be right once; the defense has to be accurate 100% of the time. A more diverse set of capabilities, mindsets and domains of expertise will enable the creative, broad, holistic thinking that will continue to be crucial to America's national defense.

We need to reframe how we "sell" cyber, and that starts with talking in a way that will resonate with America's youth. When you ask a 10-year old, "Who wants to be a cybersecurity professional?", I dare say you'll get a lot of blank stares. But when you say, "Who wants a job where they get to be creative and help people? Who likes to work on teams and solve puzzles?" you get a much larger pool of raised hands—girls' and boys'.

We also need to increase our focus on diversity. Diversity isn't about checking a box to meet a gender or ethnicity requirement. It's about building a robust team with a rich blend of capabilities and perspectives. I'll use a sporting analogy, as a tribute to my Cubs fan husband and our sports enthusiast CEO, Chris Young. Building a diverse organization is like drafting a baseball team. You need highly talented individuals, without question. But fielding a team of nine exceptional pitchers is not the recipe for success. The strength of high-performing teams is in having a variety of experts, each world-class in his or her domain. It's the collaboration and execution across the domains that empowers the team to win. This also means focusing on diversity of race, ethnicity, gender and age – all of which can expand a team's perspective and ultimately serve customers more creatively and effectively.

Cyber-attacks are certainly diverse and complex; worldwide incidents range in scope from organized crime to recreational vandalism to hacktivism to state sponsored cyberattacks. We cannot understate the importance of diversity and partnerships in orchestrating effective cybersecurity defense. It's about having the breadth and the depth of backgrounds, skills, and experiences that enable a team—and the worldwide cyber community—to respond to and mitigate innumerable threats, many of which haven't even been invented yet. "Together is Power" is not just a tagline. It's a fundamental requirement to cybersecurity practitioners being successful in our mission.

The great company I recently worked for, Intel, has long had a commitment to diversity, believing that "creating an inclusive environment [enables] all Intel employees [to] be full empowered to take on the world's most complex and challenging problems," according to Danielle Brown, Intel chief diversity and inclusion officer. In the new McAfee, we plan to sustain a commitment to diversity and inclusion. It's not only the right thing to do; it's the smart thing to do.

We Need to Close the Gender Gap

The cybersecurity profession stands to profit greatly from diversity across many sectors. As a woman in cyber, I want to zero in briefly on closing the cyber gender gap. To again cite the Women in Cybersecurity report, only 14 percent of cybersecurity professionals in the U.S. are women. Clearly, training and recruiting more women could help alleviate the skills gap. Let me suggest some ways we can help do that. Interestingly, many of what society traditionally considers "feminine" traits are highly valuable in cyber—collaboration, teamwork, creativity, and consensus-building, to name a few.

We need to make the cyber landscape a place where these skills are lauded, not minimized. If we want to appeal to broader audiences, we must be inclusive of broader skills and experiences. While hackathons holding timed competitions for those who can pick the most locks may appeal to the competitively driven traditional hacker, we should augment these offerings with additional engagements focused on collaboration, teamwork and solution-building. We can focus on skills needed for success--using neutral or positive terminologies. For example, we can swap "devious" for "clever"; nurture passions for creativity and puzzle-solving; turn "what can I break?" into "what can I help fix?"

Additionally, we can both appeal to more women and woo more philanthropy-minded individuals by better explaining how our work helps people. If you look at the stats for women engineering graduates, the numbers are highest in biomedical engineering and environmental engineering—fields where students can draw a direct correlation to helping humanity. Cyber is clearly a field that helps protect and empower people. If we brand the domain effectively, we have a target-rich environment of highly capable girls and women who could be joining the ranks to fill that 1.5M-person deficit.

We Can Address Multiple Challenges Simultaneously

Rather than starting from scratch, we have significant opportunities to build on existing infrastructure. Extensive work has been done already to inspire youth to become interested in coding—how do we augment that to include a focus on cyber? *Girls Who Code* has an extensive national base and is graduating its first collegiate classes. What can be done to encourage focus on secure coding in their curriculum? Do GWC and similar programs talk about job possibilities in cybersecurity? The Society of Women Engineers has a national membership of thousands; are we leveraging that community for skills retraining, seeking experts in adjacent fields, and providing role models for women in technology? What is being done for inner city multi-racial and multi-cultural youth? Foster youth are at risk of becoming "lost in the system" and are an extremely high at-risk group to be victims of human trafficking. Can we target this population for a skills-development pilot, offering them the opportunity for a cyber education while helping combat a larger societal problem?

The afore-mentioned study Hacking the Skills Shortage also includes recommendations for closing the cybersecurity skills gap through increased diversity and creative approaches to training. The authors write, "Our research suggests that cybersecurity education should start at

an early age, target a more diverse range of students, and provide hands-on experiences and training."

In my experience, people are far more passionate and committed to a cause they have personal experience with. Look at the athlete with a sporting injury who became a physical therapist or the child whose parent was killed who became a police officer. How do we leverage personal circumstances to entice and inspire youth toward a career that helps humanity through cybersecurity? We have to start thinking outside the box, and I suggest one way is to get more personal. That way we can both find and support people who will be in the career for the long haul.

Recruiting and Skills Identification

Regarding standing up a cybersecurity talent development program, it's easy to ask, "What degrees do I need?" or "What certifications should I require?" As a process-minded engineer, I fully understand the desire to have a formulaic approach to addressing this talent shortage problem. Discussions will be had. Processes will be built. I urge us to keep top of mind the long-term objective. Cyber moves quickly; we need people who can think and move quickly with it. McAfee's CTO Steve Grobman once said, "Computer Science is a great field for people who hate to be bored." Degrees and certifications are a great way to demonstrate current knowledge. As a hiring manager and technical talent developer, though, I care less about what you know now than what you have the capacity to understand and respond to two, three, or five years from now. Technology will change, the infrastructure will change, but the need to think critically and respond to a variety of challenges will not change. Complexity will only increase, and we need cybersecurity professionals who will evolve with it.

Prioritizing Time for Advocacy

Lastly, I would like to stress the importance of allocating time for advocacy by current cyber professionals to enroll and enlist the next generation. As a woman in tech (who spent several years working part-time as a new mother), I know firsthand the pressure to prove yourself—not only for your own career success, but as a representative of your culture or gender. It is extremely difficult to deliver excellence in your day job and carve time to engage and lift up the next generation. If we are going to inspire and empower a new and diverse corps of cybersecurity professionals, we must prioritize time for current role models to advocate, inspire, and recruit. McAfee strongly recommends that any future initiative include commitments by industry to provide diverse technical professionals—not only by gender and race, but skillset and experience—to teach and mentor. We also recommend that students accepted into a CyberCorps program spend time teaching cyber safety to America's K-12 youth. When we build an entire continuum—each stage of cybersecurity experts uplifting and empowering the generation after it—then we will truly, systemically achieve our national objective.

CONCLUSION

It has been an honor to appear before such a distinguished panel of policymakers. Both Chairman Hurd and Ranking Member Kelly merit praise for their dedication to closing the cybersecurity skills gap. This gap can be closed, but it will take a true public-private partnership to do so. Toward that end, we need to increase the funding level of the CyberCorps Scholarship for

Service program. The IT sector needs to collaborate closely with the government to ensure that students and recent graduates of this program are given many opportunities to take part in co-ops and internships that support the acquisition of cybersecurity skill sets. We also need to broaden our point of view of what it means to be a cybersecurity professional. The days of thinking about cyber experts in a one-dimensional manner – the guy with the hoodie – are over. The future is about ensuring that the widest diversity of people and skill sets are brought into the cybersecurity profession so we can meet the challenges of protecting public and private sector institutions from an array of cybersecurity threats.

Thank you, and I'll be happy to answer any of your questions.

Mr. HURD. Thank you.

Mr. Waddell, you are recognized for 5 minutes.

STATEMENT OF DAN WADDELL

Mr. WADDELL. Thank you, sir.

Chairman Hurd, Ranking Member Kelly, and distinguished members of the subcommittee, let me begin by thanking you for inviting me to speak on this very important issue. On behalf of the (ISC)2, we will look forward to working with you in the coming years to help ensure our country is safe, secure, and resilient against cyber attacks and other risks.

As a matter of introduction, (ISC)2 stands for the International Information System Security Certification Consortium. We are the largest nonprofit membership body of certified cyber, information, software, and infrastructure security professionals, with over 123,000 members worldwide, of which many are currently employed at or contracted by our Federal Government.

We are known for our certified information systems security professional, or CISSP. When employees earn their CISSP or any of our other certifications, it shows they have the knowledge and skills in order to perform in this field. Ideally, through our continuing professional educational requirements, they will be qualified throughout their lifetimes. Through our certifications, our training and education offerings, and our research, internet safety, and scholarship programs, we encourage cybersecurity students and professionals to help achieve our vision: to inspire a safe and secure cyber world.

However, accomplishing this vision is made more difficult when there is a lack of qualified cybersecurity professionals. You've heard the numbers and our study referenced here today, the Global Information Security Workforce Study. The 2017 version of this biannual study took place from June 2016 through September 2016 via a web-based survey and over 19,000 cybersecurity professionals from over 170 nations responded. And you can find more information on this at iamcybersafe.org.

We've heard the numbers, 1.8 million by the year 2022, as far as a talent gap is concerned. So what can we do collectively to solve this crisis?

Recently, the (ISC)2 executive management team gathered recommendations that we believe will be critical to the success of the cybersecurity workforce. Specifically, during a gathering in December 2016, members of (ISC)2's U.S. Government Advisory Council hosted former Federal Chief Information Security Officer Greg Touhill and a group of Federal agency CISOs and executives to discuss what was necessary to ensure the continuation of progress for the new administration.

As a result of that discussion, we offered several recommendations. I will briefly summarize three of them now. The entire list can be found in my written testimony.

One, harden the workforce. Everyone must learn cybersecurity. We have to break the commodity focus of simply buying technology and stopping there, without focusing on training all users. People need patching too. From the intern to the CEO, the mindset needs to be cybersecurity is everyone's job. To achieve this, we need to

encourage cybersecurity cross-training to promote cyber literacy across all departments within Federal agencies.

Two, incentivize hiring and retention. In today's world a sense of mission doesn't always override good pay. Incentives work. For example, following the cybersecurity hiring authorities passed by Congress in 2014, DHS NPPD provided pay incentives at 20 to 25 percent above an employee's annual pay to motivate and retain cybersecurity hires. The practice of incentive pay needs to be replicated throughout the Federal Government in order to attract experts from the private sector.

This perk also plays a key role in retaining cybersecurity talent. According to the Pew Research Center, millennials recent surpassed Gen X as the largest generation in the U.S. workforce. And our study found that paying for professional memberships and training are key drivers in job satisfaction with this demographic.

Three, civil service reform. The civil service system is broken and does not meet the government's needs. In our best effort to attract and retain top cyber talent, we are handicapped by the government's antiquated GS classification and pay system that makes it difficult to promote high achievers and reposition nonachievers.

We've talked about the Cyber National Guard concept, which would allow the Federal Government to repay student loans of both STEM and STEAM graduates who agree to work for a number of years in a Federal agency before returning to the private sector. This will serve as a natural extension to the existing Scholarship for Service program and will help to broaden the broader workforce development initiative.

Through these recommendations and the programs that we offer (ISC)2 hopes to establish an open avenue of communication with you, your staff, and others in Congress as we all work toward strengthen cybersecurity throughout the Federal Government, both now and in the future. We see this time of transition as an opportunity for our members to be a stabilizing force during an intrinsically uncertain process. (ISC)2 would like to offer its ongoing support to you and the other organizations represented here today by providing resources, research, and community.

Thank you, and I look forward to your questions.

[Prepared statement of Mr. Waddell follows:]

Testimony of
Dan Waddell
Managing Director, North America & Director of U.S. Government Affairs
(ISC)²

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

"Reviewing Federal I.T. Workforce Challenges and Possible Solutions"

April 4, 2017

Chairman Hurd, Ranking Member Kelly, and distinguished members of the Committees, let me begin by thanking you for inviting me to speak on this very important issue. On behalf of (ISC)², we look forward to working with you in the coming years to help ensure our country is safe, secure, and resilient against cyberattacks and other risks.

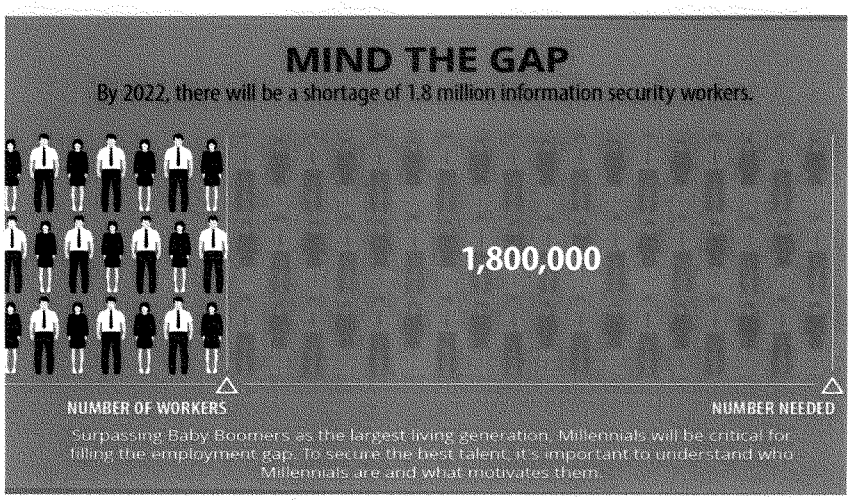
As a matter of introduction, (ISC)² stands for the International Information System Security Certification Consortium. We are the largest nonprofit membership body of certified cyber, information, software and infrastructure security professionals, with over 123,000 members worldwide – of which many are currently employed at or contracted by our federal government. Known for our Certified Information Systems Security Professional, the CISSP is the industry-leading certification for information security professionals. When employees earn their CISSP or any of our other certifications, it shows they have the knowledge and skills of true experts. Ideally, through our continuing professional education requirements, they will be qualified throughout their lifetimes. Through our certifications, our training and education offerings, and our research, internet safety and scholarship programs, we encourage cybersecurity students and professionals to start with us, stay with us and grow with us.

Since 1989, (ISC)² has provided a solid foundation for the life-long development of the industry's top talent. As a professional membership community, our role is to inform and educate wherever there is a void, in order to better safeguard people and their information assets. As an advocate for the professionalization of the cybersecurity workforce, our role is to be the voice of our members and the broader cybersecurity profession. Our ability to effectively fulfill these roles ultimately determines the success of our mission and our vision – to inspire a safe and secure cyber world.

However, accomplishing this vision is made more difficult when there is a lack of qualified cybersecurity professionals. Recently, (ISC)² and our charitable trust - the Center for Cyber Safety and Education – conducted the largest study of the cybersecurity profession – the Global Information Security Workforce Study (GISWS). The 2017 version of this bi-annual study took place from June through September 2016 via a web-based survey. Over 19,000 cybersecurity

professionals from 170 nations responded. Since its first release in 2004, this study gauges the opinions of cybersecurity professionals, and provides detailed insight into important trends and opportunities within the profession. It aims to provide a clear understanding of pay scales, skills gaps, training requirements, corporate hiring practices, security budgets, career progression and corporate attitudes toward information security that is of use to companies, hiring managers, industry professionals – and most importantly, for you here today.

This survey projects that the gap between available qualified professionals and unfilled positions will widen on a global scale to 1.8 million by 2022, as illustrated in the graphic below.



We will be releasing the U.S. Government-specific results on May 9th at our annual Washington, D.C. event - CyberSecureGov, and will include data from over 1,600 U.S. Government respondents.

So what can we do collectively to solve this crisis?

Recently, the (ISC)² executive management team gathered recommendations that we believe will be critical to the success of the cybersecurity workforce. Specifically, during a gathering in December 2016, members of (ISC)²'s U.S. Government Advisory Council hosted former Federal Chief Information Security Officer Greg Touhill and a group of federal agency CISOs and executives to discuss what was necessary to ensure the continuation of progress during the presidential transition. As a result of that discussion, we offered the following recommendations:

- ***Consider the Progress Already Made.*** Cybersecurity is a bi-partisan issue. Critical work has been done over the last 8 years to advance the cybersecurity workforce. $(ISC)^2$ was a strong advocate of the Cybersecurity National Action Plan (CNAP) which led to the creation of the first federal CISO position under the previous administration. That is why we recommend the *reinstatement of both the federal Chief Information Officer (CIO) and CISO positions, but with greater authority.* The next federal CIO and CISO must have the ability to positively affect change, have a depth of experience in both the technical and managerial aspects of cybersecurity, and must be advocates for effective, holistic cybersecurity solutions that include people, process and technology as equally essential components.
- ***Harden the Workforce.*** Everyone must learn cybersecurity. We have to break the commodity focus of simply buying technology and stopping there, without focusing on training all users. From the intern to the CEO, the mindset needs to be, "Cybersecurity is everyone's job." To achieve this, we need to encourage cybersecurity cross-training to promote cyber literacy across all departments within federal agencies.
- ***Incentivize Hiring and Retention.*** In today's world, a sense of mission doesn't always override good pay; incentives work. For example, following the cybersecurity hiring authorities passed by Congress in 2014, the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) provided pay incentives at 20-25% above an employee's annual pay to motivate new cybersecurity hires. The practice of incentive pay needs to be replicated throughout the federal government in order to attract experts from the private sector. This perk also plays a key role in retaining cybersecurity talent. According to the Pew Research Center, millennials recently surpassed Generation X as the largest generation in the U.S. workforce. The *2017 $(ISC)^2$ Global Information Security Workforce Study* found that paying for professional memberships and training are key drivers in job satisfaction with this demographic.
- ***Prioritize investment in Acquisition, Legal and Human Resources (HR) Personnel.*** Acquisition, Legal and HR professionals are essential players within the federal cybersecurity ecosystem. They need to be educated on both the needs of the customer and the nuances of the cyber workforce in order to develop accurate Requests for Proposals (RFPs) and job descriptions that will result in quality hires and the procurement of secure products and systems.
- ***Prevent Getting Lost in Translation.*** The government needs effective communicators who can translate technical risk to business leaders in order to improve communications between cyber personnel and the boardroom. Effectiveness of the CISO role in the future will depend upon a "translation" layer of personnel that must be established and trained. The government realized this in changes made to OMB Circular A-123 which now calls for a Chief Risk Officer at each agency. Efforts to align technology risk with mission and business strategies should leverage this OMB initiative.
- ***Civil Service Reform.*** The civil service system is broken and does not meet the government's needs. In our best effort to attract and retain top cyber talent, we are

handicapped by the government's antiquated general schedule (GS) classification and pay system that makes it difficult to promote high-achievers and re-position non-achievers. One such reform effort should be considered – the "cyber national guard" concept – which would allow the federal government to repay student loans of STEM graduates who agree to work for a number of years in a federal agency before returning to the private sector. This will serve as a natural extension to the existing Scholarship for Service (SFS) program and will help to expand the broader workforce development initiative.

- ***Compliance Does Not Equal Security - Embrace Risk Management.*** According to NIST, the definition of resilience is "the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs." In the government's quest for cyber resiliency, a risk management perspective will be essential.
- ***A Standard Cyber Workforce Lexicon.*** In November 2016, NIST released draft NIST Special Publication 800-181 titled, "NICE Cybersecurity Workforce Framework (NCWF)," and is currently reviewing public comments. (ISC)² is working to align our certifications with this new framework which represents years of collaboration across government, industry and academia. According to NIST, the "NCWF provides a fundamental reference resource for describing and sharing information about cybersecurity work roles, the discrete tasks performed by staff within those roles, and the knowledge, skills, and abilities (KSAs) needed to complete the tasks successfully." Once finalized, this framework should provide an excellent resource for workforce development, planning, training and education.

(ISC)² also has a number of programs both internally and through our partners that can help address the workforce shortage. I will briefly mention two below.

1. **Associate of (ISC)².** The Associate of (ISC)² allows those just starting out in the information security workforce to demonstrate their competence in the field. Associates have passed a rigorous (ISC)² certification exam, proving their cybersecurity knowledge, and maintaining their continuing professional education (CPE) requirements while working toward completing the experience requirements to become fully certified. Exam costs here in the U.S. currently range from $250 to $599.
2. **Virginia Veteran Cyber Training Pilot.** This initiative is a unique cyber training collaboration between the Commonwealth of Virginia and private sector leaders, including Cisco, Amazon Web Services (AWS), (ISC)² and the Institute for Veterans and Military Families' Onward to Opportunity program (O2O). The initiative provides a free, cyber training program for veterans living in Virginia who are interested in careers in the cyber industry.

Through these recommendations and the programs we offer, (ISC)^2 hopes to establish an open avenue of communication with you, your staff and others in Congress as we all work towards strengthening cybersecurity throughout the federal government both now and in the future. We see this time of transition as an opportunity for our members to be a stabilizing force during an intrinsically uncertain process. (ISC)^2 would like to offer its ongoing support to you and the other organizations represented here today by providing resources, research and community.

Mr. HURD. Thank you, sir.

Mr. Marinos, you're now recognized for 5 minutes.

STATEMENT OF NICK MARINOS

Mr. MARINOS. Thank you, sir.

Chairman Hurd, Ranking Member Kelly, and members of the subcommittee, thank you for inviting GAO to testify on challenges facing the Federal IT and cybersecurity workforce.

For context, it's important to note that the Federal Government and the Nation's critical infrastructures continue to face an ever-increasing and evolving array of cyber threats. As the committee's aware, the GAO has designated this as a high-risk area for the government for 20 years now.

It's clear that having a qualified, well trained cybersecurity workforce is critical to mitigating these threats, and we also know that there is a persistent shortage in cyber talent affecting both the public and private sectors.

Today, I'd like to highlight three key challenges to building the government's cyber workforce. The first is workforce planning, the second is recruiting and retaining talent, and the third is navigating the government's hiring process.

As for workforce planning, the Federal Government hasn't always taken a strategic approach. We and others have reported over the last several years about difficulties agencies have had in assessing the gaps between what skills their workforce has today and where they need to be to address current and future threats.

Second, the Federal Government has had a hard time recruiting and retaining talent. In recent surveys we conducted of Federal chief information officers and chief information security officers this was consistently identified as a top challenge. In discussions with these officials we heard concerns over limitations that agencies had in offering competitive salaries and also difficulties in losing top government staff to higher-paying jobs outside government.

Third, we all recognize that the Federal hiring process can be lengthy and complex and doesn't always match candidates with open positions. We recently reported that agencies may not be leveraging the right hiring authorities when working to expedite the hiring process.

Collectively, the three challenges I just described are also reasons why GAO has kept strategic human capital management as another governmentwide high-risk area since 2001.

Now I'd like to mention a few of the ongoing efforts within the Federal Government aimed at tackling these issues.

As for the executive branch, in July of last year the Office of Management and Budget and the Office of Personnel Management jointly issued the Federal cybersecurity workforce strategy. This set goals and milestones for agencies to identify cybersecurity workforce needs, expand the workforce through education and training, recruit and hire highly skilled talent, and retain and develop the existing workforce. If implemented in full, the strategy could help executive branch agencies determine what critical skills they need and how to fill those gaps more quickly.

In addition, Congress has demonstrated its commitment to addressing cyber workforce challenges by holding agencies account-

able through recent legislation. These laws require Federal agencies to, for example, identify cybersecurity positions of critical need and mitigate shortages. Legislation also tasks GAO with monitoring agencies' progress in meeting these workforce planning requirements. And in fact, we've recently initiated that review in response to this requirement and expect to report back to Congress later this year.

There are also governmentwide efforts underway working to increase the supply of qualified cyber professionals. As several of the panelists have noted, the CyberCorps scholarship program provides tuition assistance to students who are studying cybersecurity at the now over 70 participating universities in exchange for commitment to Federal service.

In conclusion, recruiting, developing, and retaining a qualified and competent cybersecurity workforce remains a critical challenge to the Federal Government. If effectively implemented, recent efforts by the executive branch and by Congress could help in addressing these issues. We look forward to reporting back in the near future on whether progress has been made.

This completes my prepared remarks, and I look forward to your questions.

[Prepared statement of Mr. Marinos follows:]

United States Government Accountability Office
Testimony
Before the Subcommittee on Information Technology, Committee on Oversight and Government Reform, House of Representatives

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

CYBERSECURITY

Federal Efforts Are Under Way That May Address Workforce Challenges

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

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO Highlights

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

Why GAO Did This Study

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

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

What GAO Recommends

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

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

April 4, 2017

CYBERSECURITY

Federal Efforts Are Under Way That May Address Workforce Challenges

What GAO Found

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Background

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

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

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

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

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

Agencies Face Key Challenges in Ensuring an Effective Cybersecurity Workforce

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

Identifying and closing skill gaps

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

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

[3]The Partnership for Public Service and Booz Allen Hamilton, *Cyber-In-security: Strengthening the Federal Cybersecurity Workforce* (July 2009) and *Cyber In-Security II: Closing the Federal Talent Gap* (April 2015).

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

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

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

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

[4]See GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, GAO-12-8 (Washington, D.C.: Nov. 29, 2011) and *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

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

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

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

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

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

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

[8]GAO-17-8.

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

Recruiting and retaining qualified staff

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

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

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

[9]GAO-12-8.

- In August 2016, we reported the results of our review of the current authorities of agency chief information security officers (CISO).[10] Among other things, CISOs identified key challenges they faced in fulfilling their responsibilities. Several of these challenges related to the cybersecurity workforce, such as not having enough personnel to oversee the implementation of the number and scope of security requirements. In addition, CISOs stated that they were not able to offer salaries that were competitive with the private sector for candidates with high-demand technical skills. Furthermore, CISOs said that some security personnel lacked security skills or were not sufficiently trained.

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

Navigating the federal hiring process

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

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

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

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

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

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

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

- In August 2016, we issued a report on the extent to which federal hiring authorities were meeting agency needs.[16] Although competitive hiring[17] has been the traditional method of hiring, agencies can use additional hiring authorities to expedite the hiring process or achieve certain public policy goals. Among other things, we noted that agencies rely on a relatively small number of hiring authorities (as established by law, executive order, or regulation) to fill the vast majority of hires into the federal civil service. Further, while OPM collects a variety of data to assess the federal hiring process, neither it nor agencies used this information to assess the effectiveness of hiring authorities. Conducting such assessments would be a critical first step in making more strategic use of the available hiring

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

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

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

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

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

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

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

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

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

Multiple Executive Branch Initiatives Are Under Way to Address Workforce Challenges

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Recent Laws Address Cybersecurity Workforce Issues

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

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

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

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

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

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

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

- **The Homeland Security Cybersecurity Workforce Assessment Act (2014)** requires DHS to take certain actions related to cybersecurity workforce planning. Specifically, the Secretary of Homeland Security is to identify all positions in DHS that perform cybersecurity functions and identify cybersecurity work categories and specialty areas of critical need.[26]
- **The Federal Cybersecurity Workforce Assessment Act of 2015** assigns specific workforce planning-related actions to federal agencies.[27] These actions include
  - developing a coding structure to capture the work roles outlined in the revised national cybersecurity workforce framework (OPM, in coordination with NIST); [28]
  - establishing procedures for implementing the coding structure to identify all civilian cybersecurity positions (OPM, in coordination with DHS, NIST, and the Office of the Director of National Intelligence);
  - identifying all IT or cyber positions at agencies, and assigning the appropriate codes to each (federal agencies); and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contact and Staff Acknowledgments

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

Mr. HURD. Thank you, sir.

Ms. Plunkett, you are now recognized for 5 minutes.

STATEMENT OF DEBORA PLUNKETT

Ms. PLUNKETT. Chairman Hurd, Ranking Member Kelly, and distinguished members of the subcommittee, it is my pleasure to appear before you today as a member of the Strategic Advisory Board of the International Consortium of Minority Cybersecurity Professionals, a grassroots, not-for-profit organization established in 2014 which has contributed to efforts to address the great cybersecurity diversity divide. Ultimately, with scarce talent and high demand, it is even more critical to focus efforts on increasing capacity.

The cybersecurity workforce shortfall should be of much consternation given that cyber crime and information theft, to include cyber espionage, are among the most serious economic national security challenges that our country faces. In fact, as we speak, there are discussions in this Congress regarding the potential role that Russia may have played in our recent Presidential elections. There is an urgent need for more capacity to address this, as well as other current day cyber threats.

It has been reported that the underparticipation by large segments of our population represents a loss of opportunity for individuals, a loss of talent in the workforce, and a loss of creativity in shaping the future of cybersecurity. Not only is it a basic equity issue, but it threatens our global economic viability.

According to Frost & Sullivan's 2017 Global Information Security Workforce Study, there is a projected shortfall of 1.5 million people during the next 5 years. Today, however, women represent only 11 percent of the total cybersecurity workforce and the percentage representation of African Americans and Hispanics in cybersecurity has been reported at approximately 12 percent combined. This data takes on added meaning when we consider the projected growth of the U.S. minority population over the next few decades.

The cybersecurity workforce shortfall and the growing diversity gap in the United States also reflect the broader challenge that the U.S. faces in STEM programs in our schools. Until we can get more students matriculating with STEM-related degrees these shortfalls will persist. We must be laser focused on quality and retention in middle and high school STEM programs as these formative years determine the future talent pipeline for the cybersecurity workforce. Strategies and programs are needed to provide significantly more opportunities, to include an infusion of resources to support everything from curriculum and faculty development to tuition support.

We also need to develop programs that not only provide financial incentives, but that also provide the flexibility to move into and out of government and industry more seamlessly without the threat of a loss of forward career progression.

ICMCP has developed five key objectives to address the cybersecurity diversity divide that include increasing the number of scholarship, internship, and employment opportunities for minority STEM students and facilitating increased attraction, retention, and professional development and advancement.

Since 2016, ICMCP has awarded almost $200,000 for scholarships, certifications, and development, and placed dozens of aspirants into internships, cybersecurity positions, and/or with mentors.

Finally, we are very excited to have launched a Security Operations Center at an academic institution aimed at ensuring students graduate with hands-on skills to augment their classroom learning.

There are also several government-led initiatives, and I will just highlight one because others have already been mentioned. The CyberCorps Scholarship for Service program is a phenomenal program. There is legislation pending to increase funding and I would urge you to support it.

In conclusion, the efforts to date to address the cybersecurity workforce shortfalls are commendable, but clearly insufficient. More must be done and with the sense of urgency commensurate with our understanding of the capabilities and intentions of nation-states, as well as other bad actors.

Sadly, however, with over 200,000 unfilled jobs in cyber and with the dismal representation of women and minorities in the cybersecurity field, there is much more than can and must be done. Several studies have proven that diverse teams win, and specifically diversity has been shown to positively impact bottom line revenues.

The greatest tragedy could be our failure to recognize the potential for all Americans to contribute to this workforce deficit. The time is now to act decisively and courageously, to resource efforts, establish new initiatives, and closely track progress towards narrowing this gap.

Thank you for the opportunity to participate, and I look forward to your questions.

[Prepared statement of Ms. Plunkett follows:]

Written testimony of Debora Plunkett, Strategic Advisory Board Member of the International Consortium of Minority Cybersecurity Professionals, for the hearing of the Subcommittee on Information Technology of the Committee on Oversight and Government Reform titled "Reviewing Federal IT Workforce Challenges and Possible Solutions" Tuesday, April 4, 2017 2:00PM

Chairman Hurd, Ranking Member Kelly, and distinguished Members of the Subcommittee, I am pleased to appear today to discuss the challenges to developing, recruiting, and retaining the federal government's IT, and specifically cybersecurity, workforce with a specific focus on leveraging the capacity of diverse talent to meet these needs.

Our testimony today will highlight the challenges being faced across the public and private sectors in recruiting and retaining cybersecurity talent. These challenges are compounded for diverse populations, which face issues with career advancements for existing diverse practitioners and retention challenges that also exist in keeping diverse talent once they are recruited. We will also discuss the role and the progress that grassroots non-profits like the one I'm here representing today, the International Consortium of Minority Cybersecurity Professionals (ICMCP), have made in closing what we have called, "The Great Cybersecurity Diversity Divide." Ultimately, these challenges extend across government and private sector, with scarce talent and high demand, making it even more critical to focus efforts on increasing capacity. As noted in the Cybersecurity National Action Plan and 2017 Budget, the goal remains "...to identify, recruit, develop, retain, and expand the pipeline of the best, brightest, and most diverse cybersecurity talent for Federal service and for our Nation." As noted in the January 2017 report entitled "Diversity and Inclusion: Examining Workforce Concerns Within the Intelligence Community" commissioned by the Intelligence Community Equal Employment Opportunity and Diversity Office, "(t)he value of increasing diversity, especially in underrepresented segments such as minority groups, women and persons with disabilities, expands the talent base and more accurately reflects analytic capabilities necessary to evaluate and meet mission requirements." Additionally, a 2014 CIA Diversity in Leadership study commissioned by the Director of the CIA, noted that "...a lack of diversity of thought and experience was identified by congressional committees and independent commissions as contributing to past intelligence failures. That diversity is mission critical is no longer a debatable proposition – if it ever was."

The Realities of the Cyber Threat Landscape

There is no doubt that cyber threats today touch on virtually every aspect of the lives of our citizens. As a nation, we are faced with pervasive cyber threats and vulnerabilities. Malicious actors, including those at nation-state levels, are motivated by a variety of reasons that include espionage, political and ideological beliefs, theft and financial gain. Increasingly, State, Local, Tribal and Territorial (SLTT) networks are experiencing cyber activity at a sophistication level similar to that seen on National networks. These forces are not expected to decrease but rather will continue apace,

The Realities of the Cybersecurity Workforce Diversity

According to Frost & Sullivan's 2017 International Information Systems Security Certification Consortium (ISC2) Global Information Security Workforce Study (GISWS) of over 19,000 information security professionals globally, across 170 countries, women represent only 11% of the total cybersecurity workforce despite a projected workforce shortfall of 1.5 million people during the next five years due to a lack of trained professionals. The percentage representation of African Americans and Hispanics in cybersecurity has been reported at approximately 12% combined, for both these groups. This data takes on added meaning when we consider the projected growth in the U.S. minority population over the next few decades where the Hispanic population is expected to grow to 28.8% of the US population and the African American population is expected to climb to almost 20% according to Census data reflecting population growth from 2014 – 2060.

This workforce shortfall should be of much consternation given that cybercrime and information theft, to include cyber espionage, are some of the most serious economic and national security challenges that the country faces. In fact, as we speak, there are discussions in this Congress regarding the potential role that Russia may have played in our recent Presidential elections. There is an urgent need for more capacity to address this, as well as other current-day cyber threats. It has also been reported that the under-participation by large segments of our society represents a loss of opportunity for individuals, a loss of talent in the workforce, and a loss of creativity in shaping the future of cybersecurity. Not only is it a basic equity issue, but it threatens our global economic viability, and even our democracy, as a nation.

The Roots of the Cybersecurity Workforce Diversity Starts in our Middle Schools and High Schools

The workforce shortfall and the growing diversity gap in the cybersecurity industry in the United States also reflects the broader challenge that the USA faces in science, technology, engineering and mathematics , or STEM, programs in our schools. Until we can get more students matriculating with STEM-related degrees, these challenges faced within the cybersecurity industry and overall information technology industry will persist. According to the PEW Research 'Fact Tank' Report of International Students in Math and Science, American 15-year-olds were ranked 38th out of the 71 countries included in the report. The results were only slightly more encouraging for our 8-year-olds, who were ranked 11th out of the 38 countries included. As a country, we have to be laser-focused on quality and retention in middle and high school STEM programs, as these formative years determine the future talent pipeline for the cybersecurity workforce. Strategies and programs are needed to provide significantly more apprenticeship opportunities as well as opportunities in colleges and universities, to include an infusion of federal resources to support everything from curriculum and faculty development to tuition support.

Mr. Chairman, our STEM imperative cannot be more urgent for minority students. The mandate is clear when we consider the projected growth of minority populations according to the census data and the reported labor trends citing the fact that over 90% of all jobs by 2030 will require information technology skills.

The Imperatives for Grassroots Organizations like ICMCP

Toward leading tangible and meaningful societal change, the International Consortium of Minority Cybersecurity Professional (ICMCP) was created in 2014, achieving formal 501(c)(3) Public Charity Non-Profit from the Internal Revenue Service (IRS) in July 2014 and with the expressed purpose of "Bridging The Great Minority Cybersecurity Divide."

The ICMCP is tackling this "Divide" by creating academic scholarship opportunities to attract more females and students of color into the career field. For existing minority cybersecurity practitioners, ICMCP is deploying strategic mentoring programs geared towards fostering the career growth of junior and mid-level practitioners into becoming the next generation of executive decision-makers. Studies by various groups to include Diversity, Inc. and Working Mothers among others, have underscored the importance of mentoring, sponsorship and employee affinity groups as key strategic components of successful diversity and inclusion programs and employee retention initiatives.

ICMCP has developed five key objectives to address the cybersecurity diversity divide:

1. Increase the number of scholarship, internship and employment opportunities for minority STEM students pursuing cybersecurity related disciplines at both the undergraduate and post-graduate levels.

2. Facilitate the increased attraction, retention, professional development and career advancement of qualified, skilled entry-level to senior-level minority cybersecurity professionals.

3. Promote community awareness of the cybersecurity industry and the opportunities within, for minority cybersecurity professionals.

4. Serve as THE voice and destination for issues related to cybersecurity career and industry developments impacting minority cybersecurity professionals.

5. Establish online and offline channels and "virtual centers" to gather and disseminate relevant information for minority cybersecurity professionals.

Toward fulfilling these five key organizational objectives, last year ICMCP accomplished the following due to the generosity of our sponsors,

- Awarded 10 Academic Scholarships @ $5K each
- Awarded 5 Certification vouchers (average $3K)
- Awarded 1 Executive Development stipend ($16K)
- Placed 12 interns in cybersecurity positions
- Matched 17 Protégés to Mutually Matched Mentors
- Assisted and facilitated the job placements of over a dozen minority cybersecurity professionals at various levels in several industries
- Implemented the first operational Security Operations Center (SOC) at an academic institution toward ensuring students graduate with hands-on skills to augment their classroom learning.

So far in 2017, ICMCP has:

- Awarded over $100K in academic scholarships
- Awarded at least 10 certification vouchers (ISC2, CompTIA, SANS, ISACA, IAPP)
- Coordinated the placement of 6 interns and 3 job-seekers

We should also mention several ongoing and very noteworthy government-led initiatives, many with diversity underpinnings also tackling the "Great Minority Cybersecurity Divide" which include:

GenCyber
The National Security Agency's GenCyber program, co-sponsored by the National Science Foundation, sponsors cybersecurity summer camps for students and teachers at the K-12 level. The goals of the GenCyber program are to help increase in diversity in the cybersecurity career field, help students understand correct and safe on-line behavior and to improve the teaching methods for delivering cybersecurity content in the K-12 curricula. This year the program sponsored 130 GenCyber camps and reached nearly 5,000 students and 1,000 teachers across the nation.

The Consortium Enabling Cybersecurity Opportunities and Research (CECOR)
The Consortium Enabling Cybersecurity Opportunities and Research (CECOR) funded by the Department of Energy is a collaborative effort among thirteen colleges and universities and two national laboratories to develop a K-12 pipeline for the cybersecurity workforce.

CyberCorps Scholarship for Service (SFS) Program
SFS is a program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. This program provides scholarships that may fully fund the typical costs incurred by full-time students while attending a participating institution, including tuition and education and related fees. The scholarships are funded through grants awarded by the National Science Foundation.

But this is clearly not enough. To make significant progress in developing and employing the cybersecurity capacity our nation needs, we need to be filling over 200,000 cybersecurity jobs annually according to the Frost and Sullivan ISC2 GISWS Report and to make these opportunities available to diverse candidates.

Diversity is the Strategic Imperative
Mr. Chairman, several studies have proven that diverse teams win and specifically in the private sector, diversity has been shown to positively impact bottom line revenues. In fact, recent reports are showing that every incremental percentage point in African American and Hispanic representation at NASDAQ-listed tech companies is linked with a three-percentage-point increase in revenues. If the racial/ethnic diversity of tech companies' workforces reflected that of the engineering talent pool, the sector at large could generate a 20 – 22 percent increase in revenue—an additional $300 – $370Bn each year. Companies with above-median Hispanic representation (currently standing at roughly 5 – 6 percent of the technical workforce) are linked with annual revenues that are 40 percent higher than companies that fall below the median in Hispanic representation.6 The links between African American representation and revenues were also positive, yet did not show statistical significance.

There is also a linkage between racial/ethnic diversity and operating margins - every one percentage point increase in racial/ethnic diversity at a tech company is linked with 0.3 – 0.4 percentage point increase in operating margins. Extrapolating to the tech sector achieving levels of racial/ethnic diversity that reflect the talent marketplace would be linked with $6 – 7Bn in additional operating earnings industry-wide, or roughly a 2 – 3 percent increase in total industry earnings.

These links between diversity and financial performance are not unique to the tech industry—a range of studies conducted in other industries support them. For instance, research published in the American Sociological Review found that firms with high levels of racial/ethnic diversity have more than 98 percent higher sales revenue, serve over 54 percent more customers, are roughly 33 percent more likely to have above-average market share, and are nearly 30 percent.

Our analysis is supported from the commercial sector, by the well-known consulting firm of McKinsey & Company which conducted a 2015 study of 366 public companies across a range of industries in the United Kingdom, Canada, the United States, and Latin America. The resulting analysis of the 366 companies revealed a statistically significant connection between diversity and financial performance. The companies with the highest gender diversity were 15 percent more likely to have financial returns that were above their national industry median, and the companies with the highest racial/ethnic diversity were 35 percent more likely to have financial returns above their national industry median. The correlation does not prove that greater gender and ethnic diversity in corporate leadership automatically translates into more profit—but rather indicates that companies that commit to diverse leadership are more successful

Conclusion

In closing Mr. Chairman, there are several good efforts underway to address cybersecurity capacity writ large, some of which also tackle the problem we have titled the "The Great Minority Cybersecurity Divide". Progress is being made but more must be done, and with a sense of urgency commensurate with our understanding of the capabilities and intentions of nation states as well as other bad actors. Sadly however, with over 200,000 unfilled jobs in cyber each year, with the average representation of women in the cybersecurity industry averaging barely 10% for the past few years, and analogous to the combined representation of African Americans and Hispanics with one or two percentage points, there is much more that can be done and that must be done when we consider the projected minority population growth and trends in the labor market.

Thank you for the opportunity to testify, and we look forward to your questions.

Mr. HURD. Thank you, Ms. Plunkett.

And before I recognize Robin Kelly for her opening questions, I ask unanimous consent that a statement from UC Berkeley on the cybersecurity workforce talent be entered into the record. Without objection, so ordered.

Mr. HURD. I would now like to recognize Ranking Member Kelly for 5 minutes.

Ms. KELLY. Thank you. And thanks to the witnesses.

Events of the past few years have made clear how vitally necessary it is to protect our public and private institutions from cyber threats. Attacks against critical infrastructure, such as electric grids and nuclear facilities around the world, prove that highly skilled and determined enemies are attacking real targets all the time, and we need talented people to defend against these attacks. It is alarming that as our critical need to seriously build and develop a world-leading cyber workforce grows, we face a shortage of the very people that we need to accomplish this work.

And I guess to all of you first, whoever wants to answer, why don't you think, especially from the young folks, that we have more interest, when you think about all the games and this, that, and the other, why do you think from younger people that this is not one of their, I guess, aspirations, to get into this market? And we're talking about cyber, but as I speak to my manufacturers even about advanced manufacturing, they need technology. They are suffering also. So it's tech in general.

Ms. HYMAN. I'm happy to reply in brief.

So CompTIA has a philanthropic arm, it is called Creating IT Futures, and they recently did some research with the group IDEO, out of Chicago actually, looking at this exact issue, because we are very focused on trying to get younger people into the tech pipeline.

A lot of it has do with exposure to mentors, believe it or not, that have good jobs that are interesting to them and that they can share that sense of excitement with young people. I know that sounds sort of simplistic, but in fact research bears it out.

Recently, we launched something called the NextUp program through our philanthropic arm. The idea is to try and match young people grades 6 through 10 with mentors throughout the tech community so that they're disabused of the idea that a tech career is some guy in a hoodie in a basement, but it is actually a very multifaceted, colorful career opportunity. And we are doing this by partnering with other groups. So we just gave, I believe, $150,000 to Tech-Girls, for a program in Chicago, in fact, to try and bring together those mentorship opportunities.

So that's one piece of the puzzle, but in fact, in our view, a very important one.

Ms. KELLY. Thank you.

Mr. COOPER. Let me add a perspective, kind of from inside government, although everybody knows I'm retired and not officially inside government. But I want to combine a lot of what Ms. Plunkett said along with what Ms. Hyman just said.

I think a significant part of the problem that directly addresses how come more younger folks don't come into this field, particularly in government, because we in government don't do a good job of making it attractive.

Let me use an example from when I was in the private sector with Eli Lilly. We had a very, very formal program that placed recruiting teams on a regular basis with the Historically Black Universities and Colleges. It was extremely successful. There were three or four team members who remained in place, a lot of them were alumni of these organizations, joint with other Lilly managers and senior people, that visited campuses on an ongoing basis to identify early rising talent, the best students coming out.

Lilly then did a number of things, but they had an 80 percent hire rate of those students identified through that program and about a 60 percent career retention rate of those people. It included scholarships and things like that.

So I think a whole lot of it—there is nothing like that that I'm aware of in government. I didn't do it, shame on me, when I was in government. But we've got to make folks more aware of the opportunities, particularly in cyber, in the Federal enterprise.

Ms. KELLY. Yes.

Mr. WADDELL. I just wanted to piggyback on Elizabeth's comments from CompTIA. I absolutely agree with what she said.

At (ISC)2 we are actually trying to get them a little bit earlier. We have actually partnered with Garfield, believe it or not, to address the 1 through 6 grade level. And it is really just going into schools and having a dialogue with these kids, because a lot of times they have this impression of the hacker in the hoodie and the cyber job that is really all about just being behind the keyboard.

But cybersecurity has so many different roles to play, and we found that through this program just by simply inducing videos and comic books about just basic internet safety it starts the dialogue.

I've been in schools in Prince William and Fairfax County and I've talked to these kids. And they come up and they say, "Wow, what do you do for a living? I want to do that. How do I get involved?"

So just by using that character Garfield, believe it or not, it really starts that conversation.

Ms. KELLY. I'm so glad to hear the comments that all of you had, because I think it is so important to start young and to go into the schools. Because in my district, which is urban, suburban, and rural, so the thing that I have to deal with that everyone talks about Chicago. But there is a—I'm glad you do—but there is the south suburbs, I have a rural part of my district, and they tend to lose out because they are kind of competing with the big city, and they don't have the transportation and those kind of things.

But I do think, like you said, people don't even think about doing these things and we have to put it on their minds. And then some of my school districts, they don't even—I just helped get one area of my district the internet so they could go on the world wide web. So, I mean, they don't even have that, your phone or your GPS doesn't work. Now it does, but it didn't work.

So we really do need to have that personal relationship and whatever your companies can do would be fantastic.

I'm over time.

Mr. HURD. Mr. Raskin from Maryland is recognized.

Mr. RASKIN. Thank you very much, Mr. Chairman.

And thanks to all the witnesses for your excellent testimony.

I'm someone who is quite perturbed and disturbed about the Russian cyber hacking and sabotage of the 2016 election. And the best that I can tell is that Vladimir Putin figured that he was no military match for the United States, but he could launch something like a Manhattan Project for cyber attacks and then figure out a way to unleash mayhem in the U.S., Brexit, France, Italy, all over the world. And so it seems to me you guys are on the front lines of the real defense of America against the big threats today.

But I wonder if you think that the allocation of our resources corresponds to the reality of the threats against us. President Trump has suggested slashing $56 billion from the domestic budget from NIH and from Peace Corps and from HUD and Community Development Block Grants, which I think is independently a misallocation of our priorities.

But put that $56 billion directly into the Pentagon and I'm wondering if you think if the money is spent the way we have traditionally spent it that addresses the threats that are really facing the country or if we have to think of the defense budget as something that puts cybersecurity right at the heart of it now.

So I don't know if anybody wanted to volunteer to take that one. Mr. Cooper.

Mr. COOPER. I'll take a shot at it. I can kind of talk—I can color outside the lines a little bit as opposed to joining you in previous hearings.

First of all, I think that the approach we're taking to hiring cyber talent is well intended but it gets in the way of actually filling an awful lot of these vacancies across the Federal enterprise and retaining that talent. Specifically, here is what I'm talking about. And please don't hear this as criticism, it is not intended this way, it is feedback.

Appropriations bills require CIOs to spend that taxpayer dollars that have been approved within, in my example most recently, the Department of Commerce. What if I could pool some of that money with fellow CIOs most in need in the Cabinet departments and with the Department of Defense to do a couple things?

First of all, why not use pooled hiring? Why do I have to end up competing with other CIOs? DHS is more sexy, DOD attracts a heck of a lot more people than the Department of Commerce, speaking very candidly. It is not a negative, it is just reality. But if we could team up and if we could kind of have a recruiting team, you guys figure out where it might be placed, possibly GSA, possibly OPM, possibly DHS, or possibly DHS, DOD combined, but let them do all the hiring for these folks.

Go after the skill sets we need, and that's where these folks can give you a lot of detail about the different scope and breadth and depth of hiring what talent is required. But I couldn't find forensic analysts. I just couldn't compete. There was no way in hell.

Mr. RASKIN. But let me come back to something——

Mr. COOPER. And then take those people and deploy them to the highest risk.

Mr. RASKIN. Gotcha. As the departments request their help on particular things or creating interagency initiatives for cybersecurity.

So let me come back to something that you actually started with, which was the hiring freeze. To what extent does this blanket categorical hiring freeze in fact undermine the ability to hire and to get in the people we need in the cybersecurity field, maybe on an emergency basis?

Mr. COOPER. Well, my answer is simple. Right now, it's having a pretty significant adverse impact.

Mr. RASKIN. Others want to weigh in?

Mr. Waddell.

Mr. WADDELL. I would say that the impact is not only on the agencies themselves because of the open positions, but the impact on the cyber workforce that's already there. So now you're asking the cyber workforce that's doing their 9 to 5 job to now pick up other duties and skills just to help cover it. So I think we also need to think about the current folks that are there. This shortage is really draining the resources of those people.

I like to use the sports analogy. I think we have too many coaches and not enough players, and in order to play defense, we need more players. So we need that pathway to help get these folks in without the threat of sequestration and hiring freezes and the like.

Mr. RASKIN. And as you sweat the people who are there harder, it drives them out and then you can't fill their positions.

Mr. WADDELL. Right, exactly.

Mr. RASKIN. So you're in a destructive downward cycle there.

Mr. Chairman, thank you very much.

And I appreciate your testimony.

Mr. HURD. Mr. Krishnamoorthi, you're recognized for 5 minutes.

Mr. KRISHNAMOORTHI. Thank you, Mr. Chairman.

First of all, thank you all for coming today. I really appreciate Congressman Raskin's line of questions. I'd like to build a little bit on what I've heard so far.

You know, Chairman Hurd has put forth some really good ideas about increasing collaboration between the public and private sectors. Ms. Depew, you have called for an expansion of the CyberCorps program and I wanted to ask you a couple of questions about that. One is that my understanding is that—is the CyberCorps program limited to folks with a 4-year degree?

Ms. DEPEW. I believe at this time it is focused on juniors and seniors in a 4-year cybersecurity-focused degree.

Mr. KRISHNAMOORTHI. Okay. What do you think about potentially opening it up to folks in community colleges who might specialize in a cybersecurity degree? I'm just concerned that perhaps we're limiting our supply of people for these open positions by basically excluding people who might specialize in a 2-year degree, but possess the requisite skills to do the job. I mean, what are your comments on that?

Ms. DEPEW. Oh, absolutely. We highly recommend that it be expanded to include community colleges. There are a breadth of skills necessary to effectively run a Security Operations Center and some of those skills can absolutely be obtained via certifications, 2-year degrees. It's not just about 4-year or advanced degrees to develop those skills and that talent.

Mr. KRISHNAMOORTHI. I see a lot of heads nodding in agreement, including Mr. Waddell from—what an interesting name, I think ISC, in parens, squared.

Mr. WADDELL. (ISC)2, yes.

Mr. KRISHNAMOORTHI. Okay. That seems like a very mathematical name there. So please, what are your thoughts?

Mr. WADDELL. I couldn't agree more. I think that—and I think limiting it to just the STEM folks, I think, leaves a lot of the liberal arts and the communication pieces of the cybersecurity job. Look no further than the OPM breach, where I think there was just a communication gap between the folks that were on the keyboards, and the folks kind of at the top. But the folks at the top didn't understand what was the risk of not patching these systems. What was the risk of these vulnerabilities? And that message just did not get filtered up for whatever reason. So, absolutely, couldn't agree more.

We could—not all positions require a college degree. It's a great thing to have, but you can certainly tap into high school, a 2-year college and have training and certifications to help augment and validate those skills.

Mr. KRISHNAMOORTHI. Go ahead, Ms. Hyman.

Ms. HYMAN. Yes. I just want to reiterate everything that's been said. We share (ISC)2's position as being a certifying body. And we've been working for a long time with the government to try and suggest that this is a very good government way of spending money is to make sure that if you're going to have training, you need to have some way to validate what that training was about. And so even if you don't have a 2- or 4-year college degree, there are certifications that an individual can take to get them into the beginning of the cybersecurity career. And on top of it, I would point out there's something called the Government Employ Training Act, GETA, which obviously says that it's okay for money to be spent for training, but it doesn't explicitly say that it should be used for testing. And so when we go to talk to various agencies, we learn that, well, they are not specifically authorized to use that funding for the purpose of testing. Therefore, we're not validating the skills that we've spent government money on to make sure an individual understands what their cybersecurity responsibilities are.

So I would commend all of to you address GETA and try to make that a more explicit piece within that particular piece of law.

Mr. KRISHNAMOORTHI. That's a great point.

I think, Chairman Hurd, perhaps we should take a look at that.

I just believe very strongly in vocational, technical education, community college education being kind of potentially the pathway forward in filling a lot of these open technical positions in our country. And so, I think we're—this year we're going to be reauthorizing the Carl D. Perkins Career and Technical Education Act in the Education and the Workforce Committee. I think this is something, perhaps, we should look at there as well.

Ms. Depew, what is the current investment into the CyberCorps program?

Ms. DEPEW. I believe it was $45 million 2 years ago, $50 million last year, and it's proposed at $70 million this year.

Mr. KRISHNAMOORTHI. I mean, what's your thought? Is that sufficient to address the shortages that we're seeing in the workforce?

Ms. DEPEW. So $40 million funds about 1,500 scholarships. If there's a 10,000-person deficit, that puts a small dent, but not a significant enough one. So I do think we do need to investigate at a heavier level. And that could be a combination of both a traditional program or expanding to community colleges.

Mr. KRISHNAMOORTHI. Great.

Final question, what level of funding do you think is required?

Ms. DEPEW. I think on the order of $180 million would be necessary to put a sufficient dent in the problem.

Mr. KRISHNAMOORTHI. Okay. Thank you very much.

Thank you, Chairman.

Mr. HURD. I want to recognize myself for my line of questionings.

First question goes to you, Mr. Marinos and Mr. Cooper. Why is it hard for a CIO to tell me how many positions they don't have—that they haven't been able to hire for?

Mr. MARINOS. So, I think, like I mentioned in my statement, I see three issues, but I'll probably focus less on the recruiting and retention, which others have mentioned. So the first one is on strategic planning. It has been a high-risk area since 2001 for a reason. Part of the difficulty with cybersecurity in particular is that, obviously, with the threat constantly changing, so are the needs themselves as well. So——

Mr. HURD. I get that. But why can't they tell me what they need today? Right? Let's start with today——

Mr. MARINOS. Sure.

Mr. HURD. —and the difficulty. I would think that I should be able to go to any agency head and call them on the phone, and they should be able to produce how many positions that they have billets for that are unfilled. Is that a—is that a—is that a yeoman's work to pull that number out of there?

Mr. MARINOS. So, I think they are working off of an old system. I throw it out there. We've got three job series that are set up to classify IT and cybersecurity. In that old system, it doesn't really provide you much granularity. So let's say you want to know how many people do I need in my SOC? How many people do I need on incident response? Well, if you're looking to hire up, or you're looking to express to the committee, to Congress, exactly what you need, you don't have a lot to work off of.

More recently, NIST has put out an updated framework, which is supposed to give agencies that ability. I would point out, though, that it's a long-term goal, even with the law that was mentioned earlier, Federal Cybersecurity Workforce Assessment Act, tasked agencies with getting there by 2019. So I think it's a real concern that I would share with you, Chairman, that I think, ultimately, asking the question up front as to what are agencies doing now to shore themselves up is of major concern.

Mr. HURD. Good copy.

Mr. Cooper.

Mr. COOPER. I'm going to give you a little bit more direct answer.

I think it varies a little bit by agency, and quite frankly, it varies by CIO. I believe you know, I could give you the answer to your

question. I still can, even though I'm not there. And I think you will find——

Mr. HURD. What was the number when you were there?

Mr. COOPER. The total—in my particular office, when I walked in the door, I learn a little bit of research, there were 16 cyber-specific vacancies. Okay? Three years later, there are 10; but there were another 10 that were not funded. So 20 is the need. 10 is officially what the number is that I shared with you this morning.

Mr. HURD. Got you.

Mr. COOPER. Additionally, across the entire Department, so all 12 bureaus, that number increased, particularly—remember, we're coming up on the 2020 decennial Census, so it's a big driver. But that number increased to about 97 across the entire Department.

Mr. HURD. And, Ms. Depew, you said a number has been used multiple times. 10,000 is what we think the estimation is in the Federal Government of IT professionals. Is that correct?

Ms. DEPEW. Yes, that's the number we referenced, yes.

Mr. HURD. Mr. Marinos, would you agree with that estimate?

Mr. MARINOS. No. Though I would point out that there have been varying estimates out there. I would say that last year, there was a goal, I think, around about 7,000, and as of January, when OMB provided its report to Congress on FISMA compliance, it did report that it met that goal.

Mr. HURD. So if we're looking to fill a gap, start saying, Hey, we need to get near 10K, 10,000 people, that's good enough for—because if we try to produce something that only produces 10, you know, graduates that can go into jobs, that's not going to make a dent. So we need—the magnitude that we're talking about is—is around 10,000.

Next question: So—and, Mr. Cooper, I'm going to start with you. Ms. Hyman, I love your perspective. And, Mr. Waddell, and if anybody else has perspectives, just please raise your hand, and I'll ask you that—this idea of rotational IT workforce, and you alluded to it in your opening remarks, what kinds of jobs could they be working on, and how would you—how—what are the hurdles that we're going to have in making sure CIO has the authority to task this rotational workforce? Right?

Because when I think of rotational, it's you have three people for 10 days working on a project, or you can have one person for 10 days, and you are able to plan in advance, and maybe you get three people to do that. So a project that takes 30 man-days can be filled by three people.

What are some of those kinds of projects? And as a former CIO, would you have wanted to use—would you want to have that kind of capability?

Mr. COOPER. All right. Let me first clarify. I may have accidentally confused members of the subcommittee or even maybe colleagues on the panel. I apologize if I did that. Let me clarify.

When I use the term "rotational," here's what I'm actually talking about. I'm talking about a longer period of time, 6 months to up to 2 years. That's what I mean when I say "rotational."

Contrast that, or compare it with the cyber National Guard or the concept of shorter periods of time, both are valuable. Which—which would you prefer me to address?

Mr. HURD. The shorter period.

Mr. COOPER. All right. Okay. The shorter period. The types of positions that would be very, very valuable for skilled people—and there are a whole lot of these folks who are in the contractor workforce that support most of the CIO offices across the Federal agencies, take something as simple as deploying testing and deploying vendor security patches. That's—that's something that skilled people and people who are trained through some of these programs at a 2-year level, by the way—I fully agree. This could be done by community college graduates. It would be a tremendous opportunity to build a workforce to do that. That's something that people can step in and add real value for however much time they are able to do that.

So, literally, that could be 3 days, 2 weeks. If I've got somebody skilled, I will take them. And I will take as many as those people as I can get, as long as I have some way to know that they're skilled, and that's where I fully support all of the colleagues sitting to your right around rigorous certification. That's terribly, terribly important. Because, otherwise, I don't know these people, and I don't know whether their skills are right. You give me as many of those people short term, I will take them all.

Ms. HYMAN. Yes. Great question. And I agree in terms of the short-term purposes. I think maybe in—I'm going to defer to some of the true experts on the panel, but also looking at some of the cybersecurity—excuse me—logs on a continual basis, so long as you have an opportunity—if you are there for 2 or 3 days, and you're looking at some of the patterns there, there's some sort of system to capture that. I don't know if that's possible short term. But I was thinking about that. Because that is introductory industry analyst type position.

The other thing, frankly, is using some of these people to train your remaining noncybersecurity workforce. The amount of human error that contributes to cybersecurity breaches, it's usually about 50 percent or higher. And so you could, on a very short-term purpose, use some of these individuals to deliver, you know, quick training for the regular workforce along those lines.

Mr. HURD. So, as Mr. Waddell says, harden the workforce.

Ms. Depew, do you have any comments?

Ms. DEPEW. Two thoughts that come on top of head—on top of mind are specific coding projects. We always have a multitude of ideas that we would like to flesh out. So if somebody had advanced coding skills, there are contained projects we could do on a short-term basis that I think would be really valuable. Another thing I would love to do is put folks with government experience in front of some of our products and tell us what we need to improve and why they don't work as effectively as we need to in your infrastructure. So that would be very advantageous to us as well.

Mr. WADDELL. Two things jump out at me for the short-time assignments. One is like a site assessment. When I was a contractor with the DOD, I was on a 2-week rotation with the Army where we went to MetCom and the military entrance processes command and tested all the sites. That was a 2-week rotation. We went in. We red-teamed. We threw everything we could against that site, interviewed the people, did a bunch of pin tests, and then cranked

out a report and left. I think that's probably a really good one for that short-term assignment.

The second one was also a breach response forensics, say, for example, you know, some agency organization got hacked, and they needed to do forensics on a hard drive, maybe come in and just do a real quick recovery of that and then rotate to the next breach.

Mr. HURD. Ms. Plunkett.

Ms. PLUNKETT. So I'd agree with everything that has been said. Areas like research and development, developing mitigations, product testing, and some level of forensics, I think would be ripe. The other areas that would be more difficult would be real-time response, because you want to have some a priority understanding of the network. It's not impossible, particularly if you have someone that's rotating in on a regular basis to the same place. But if it really is a ready reserve where they would go anywhere, it would be difficult to send someone in just to address a threat when they don't know the infrastructure and they are not up on the current vulnerabilities.

Mr. HURD. So, Mr. Marinos, what are the difficulties going to be if let's—you know, we have these different kinds of work requirements that a short-term rotational workforce could address. Help me think in advance of, you know, the problems that we're going to see in trying to introduce that into the Federal Government? Is that a fair question, these incidents?

Mr. MARINOS. Absolutely. I think the quickest answer is coordination. So—I hate to tell you. You know, and you all are champions of empowering the CIOs who are doing work for you and enforcing FITARA, we're looking at that area very carefully. When you think about that, you are thinking a lot about CIO and CFO working hand in hand to procurement, working with the CIO. Here, you've got a whole different story. You've got the chief human capital office working with the CIO and the chief information security officer at individual agencies having to work together. So, you know, I just kind of throw that out as a potential paying point in terms of the coordination.

If you're thinking about where this fits within the Federal Government too, thinking about what DHS' mandate is, the National Cybersecurity Communications Integration Center is increasing in its—you know, its level of assistance to other agencies. That might be a location to consider in terms of whether they are going to need assistance to be able to help other agencies out.

But I would go back to what Mr. Cooper has expressed at previous hearings as well, which is that if the CIO is not actively engaged, then the help may not be going to the right places.

Mr. HURD. Let's do a quick lightning round. Okay? We'll just go down the panel. Where should this cyber National Guard sit? And "I don't know" is a valid question.

Mr. Cooper.

Mr. COOPER. Okay. So the truth is——

Mr. HURD. Lightening round.

Mr. COOPER. The truth is I don't know, but I would argue DHS plus OPM plus DOD.

Ms. HYMAN. I don't know, but I would add that there should be information back from the Federal cybersecurity workforce assess-

ment process so that you could figure out where gaps are and what agencies really need to be invested.

Ms. DEPEW. I don't have an answer for the National Guard, but for the expansion of the scholarship program, we do think that the NSF is an appropriate place, because it's nonregulatory and it has great respect with the private sector.

Mr. HURD. Got you.

Mr. WADDELL. I would say a mix of DHS and DOD.

Mr. MARINOS. I'll add in—I think it's really important for the Office of Management and Budget. We had the Federal CIO in the previous administration. I think it's important for there to be a proactive involvement from that office.

Mr. HURD. Okay. Ms. Plunkett.

Ms. PLUNKETT. I'd say in a place where there's a real-time current cybersecurity mission, it can't be just a place to deploy, because that won't—they won't have the right understanding of the types of skills that are needed for a specific situation. It's got to be in a place where there's active cybersecurity mission going on.

Mr. HURD. Next question, lightening round. I'm going to start with you, Ms. Plunkett. I'm going to go down this way. Expand the cyber—so CyberCorps—CyberCorps is only 4-year institutions.

Is that correct, Ms. Depew?

Ms. DEPEW. That is my understanding.

Mr. HURD. Okay. So is it focused on getting scholarships to high school kids that go to college forgive debts? And I would say not college—when I say "college," I mean 2- or 4-year institutions. So is it to forgive debt or is it people that have already gone to school, or do we focus on trying to give scholarships to high school kids who go to school, or something else?

Ms. PLUNKETT. I think it's all of the above. And in addition, we need to invest in those high school students while they're in high school. We need to look at investigating in areas like——

Mr. HURD. What gives us the quickest result?

Ms. PLUNKETT. To address the immediate need, it's likely more for scholarship for service, to get folks who are at the end of their degree program through more quick—through debt forgiven, get them into the workplace.

Mr. HURD. Good copy.

Mr. MARINOS. So as the one current government guy here, I can say from GAO's perspective, we've recruited, and we still have CyberCorps folks there after decades. So I think there's an importance at the undergraduate and graduate level, but I think it couldn't hurt if there was an extension of that.

Mr. WADDELL. I quickest I would consider cohort programs that retrain folks that are already in another vertical and retrain them quickly through a 16-week program and get them in entry level. That's the quickest.

Ms. DEPEW. I agree the quickest is to leverage what exists now and potentially pump up more existing scholarship programs. But if you are going to systemically fix the problem, you have to start deeper in the pipeline and do something with middle school and high school students.

Ms. HYMAN. Same thing, but I would also say, upscaling is crucial. And to take that existing workforce pipeline and provide not

only, again, certifications, but identify a career path for these individuals to continue within government service with opportunities for training, education, and progression.

Mr. COOPER. Most immediate impact and easiest to implement right away, 2-year community college-based degrees plus a year's of service Federal obligation. The other stuff I agree with, but the most impactful right now, people trained out of 2-year colleges hit the ground right now, but they require an obligation on years of service.

Mr. HURD. Ms. Kelly, you're now recognized.

Ms. KELLY. I have to ask this question, since it's Women's Equal Pay Day. When you talk about recruitment and retention, what have you seen as far as a difference in pay between men and women? Because from something I read, I saw there was like a 15- to $16,000 difference.

Mr. COOPER. I can address that directly. There was a disparity. I took a look at it. I tried to do something as best I could, but—but I didn't tackle it directly male, female. I did it on an equity-based basis around roles, and that was more palatable to my HR counterparts.

Ms. HYMAN. We don't have the data specifically on that question, but I will say, obviously, women are underrepresented in the tech fields. And I think we have to pay attention to getting more women in so that we can also drive up salaries.

Ms. KELLY. Right. Because they are underrepresented, that might be one of the reasons why they are not going to get equal pay.

Then the other question is, I know we're talking about how to get young people involved. But when people are laid off from a career they've had, some people—you know, we always say, we should put them back into training and skills and blah, blah, blah. And some people would say, oh, people that get laid off in their 40s or 50s, they don't want to go back in and learn something.

Have you found that, or do you have many people that you work with, Mr. Waddell, Ms. Hyman, that are older, but younger than me?

Ms. HYMAN. Yes. Talking a little bit about our philanthropic arm, they also have developed something called the IT–Ready program, and it looks at folks that have been displaced, put out of work, as well as younger people in underrepresented populations.

I don't have specific numbers for you, but what I can say is that these types of programs, it's not just a simple matter of retraining somebody.

The—when we take somebody on for the IT–Ready program, we've assessed them, whether there's an aptitude for technology. There's a good 8 weeks to 10 weeks of training. There's support services that go with it. How do you interview for your job? And then we place them into an internship or apprenticeship, so that there's an opportunity then to turn that into a full-time job.

We've had, I believe, over 85 percent success rate with this program, but the issue is scaling it up. We probably have about 800 people annually. You know, we have a lot of work to do.

Mr. WADDELL. Yes. I just wanted to give you some facts, some figures, from our 2017 report specifically about the wage gap.

The wage gap of women at the director level and above has narrowed from salaries reported in 2015; however, women are still paid 3 percent less than men in equivalent roles. At the manager level, the gap has remained relatively the same, with women earning 4 percent less than men. The gap at the nonmanagerial level has widen to 6 percent from 4 percent in 2015.

Ms. PLUNKETT. You know, what we found is that we actually have been successful at retraining folks who are either laid off, or are looking for a career change. And the answer has been a combination of, certainly, academic training, but then, exposure to operational cybersecurity capabilities as we might find in the ESOC or the SOC or the ICMCP has been piloting, where they've had some hands-on experience in an academic experience. So that when they go into the workplace, they've touched the code; they've touched the machines; they have touched in, an operational kind of way, systems, so they can hit the ground running.

Mr. HURD. Mr. Raskin is now recognized.

Mr. RASKIN. Mr. Chairman, thank you. Just one final question. If Members of Congress, like members of this panel, wanted to do a job fair or a higher education fair, college fair, career opportunities fair, who is the best person to contact about creating a cybersecurity careers presence there? Do you guys do that?

Mr. WADDELL. Yes. We do. I think all of us on here do some sort of job fair. I'll just give you an interesting, very quick story. I offered a table at our career fair to DHS, US–CERT a couple of years ago, and the deputy director at the time, Brad Nix, said, I'd love to come, but by the time we get there, all the positions—all the folks would be gone, and we wouldn't have an opportunity to capture them, because it just takes them so long to get them into the system. Average is at about 6 months. So I don't know if the problem is the career fair themselves. It's just—we need to streamline the onboarding and hiring process to get those folks in quickly—quicker.

Mr. RASKIN. Yes, Ms. Plunkett.

Ms. PLUNKETT. Can I just add, the process by which we actually match aspirants or candidates with good jobs is an area that could use some help. And, certainly, ICMCP would be absolutely willing to participate in a job fair. We have lots of young people coming to us looking for those opportunities.

Mr. RASKIN. That's great. Well, I'll definitely take your information. And I don't know whether you are deterred by the hiring freeze in terms of doing this, but I suppose it makes sense in any event to go forward and do it.

Mr. HURD. Well, I'd like to notify my colleague, in places like DOD, the IT professionals are considered must-haves, and so the hiring freeze is not impacting them.

Mr. RASKIN. Okay.

Mr. HURD. And many of the other Federal agencies could have that same interpretation.

Mr. RASKIN. Thank you, Mr. Chairman.

Mr. HURD. Ms. Hyman, can your cybersecurity career path positions descriptions, could they be used as the foundation for Mr. Cooper's idea of working with the Federal CIO counsel and OPM on having pre-approved positions?

Ms. HYMAN. Yes. So what we've done with our certifications is that we've mapped them to the National Initiative for Cybersecurity Education, which looks at knowledge, skills, and abilities across different uses for cybersecurity. And the 8140 program, the successor to the DOD 8570 program, which is their information assurance requirements, they're actually going to be mapping many of their requirements to the 81—to the NICE initiatives. So what you're starting to see is, across different government agencies, sort of a similar lexicon about what cybersecurity knowledge, skills, and abilities are. And we're not the only certifying body that has mapped our certifications to NICE.

Mr. HURD. Good copy.

Mr. Cooper, 18F and USDS, can their business model be used to address some of these—how would I best say it?

Mr. COOPER. Some the shortcomings?

Mr. HURD. —some of the shortcomings, yes.

Mr. COOPER. Yes, I actually believe it could.

I think they've done a lot of learning from their first approach, or first foray, through U.S. Digital Services, I think it has been a positive learning. I would support that, and I think that you could probably pull that group together with a Federal CIO when named, and the Federal CIO counsel appropriate interaction with the HR community. But, yes, I do think that could work.

Mr. HURD. Ms. Depew, the Cyber—I don't know why I can't remember that—CyberCorps program, my understanding is that the funds go to the universities, and the universities are the ones that are the selecting individuals to potentially receive that. Is that a correct understanding of the program?

Ms. DEPEW. I would—yes.

Mr. HURD. So my question is—and is that restricting us by having just those participant—the schools that are participating in that, and the only other option would be, you have some entity in the Federal Government that administers these programs, which I'm always circumspect about whether we can pull off something like that in order to have kids apply and go to the school of their choice—their choosing. Am I—am I thinking about this problem the right way?

Ms. DEPEW. I think that's fair. I would have to—I'm curious how they choose which schools if the schools opt in or if they were targeted. I was looking through the list myself, looking for which schools were near some of our campuses, because it would be nice to be able to offer some local teachers. And I didn't see a multitude in the States and cities where our campuses were, which is another reason a community college-based program would open that aperture and have more availability to a broader——

Mr. HURD. Got you.

Mr. Cooper.

Mr. COOPER. One quick thought, which honestly just occurred to me listening to our conversation, it might be interesting to talk to the military academies about adding kind of a cyber curriculum. They have the basics, but with a goal of actually training cyber officers who don't necessarily go through direct military. They are in the military, but they come back to, you know, not just DOD, civilian agencies as well, might be an interesting thing to explore.

Mr. HURD. 10 seconds, final question. Everybody gets 10 seconds, final statement: What should we be walking away here or something that we haven't—we haven't discussed or you haven't been able to bring up?

Ms. Plunkett, I'm going to start with you.

Ms. PLUNKETT. I'd say let's not—I recommend you not focus on what's working. Scholarship for service is working. Needs more resources. Focus on capacity at lower levels, middle school, high school. Focus on 2-year colleges. Focus on SOC experiences where folks can get operational experiences and then jump right into the workforce.

Mr. HURD. 10 seconds.

Mr. MARINOS. I think your continued focus of oversight is really important here. We can't afford to wait, and I'm concerned about the longer term focus of where our initiatives are going.

Mr. HURD. Thank you.

Mr. WADDELL. Scale up fine pockets of excellence of things that are working such as the cyber pay incentive program at DHS, MPPD that has been shown to attract and retain talent.

Ms. DEPEW. The threat landscape is always changing. It's not like certain degrees where they fix routine process, so you need to consider that when you're recruiting your diverse workforce and training them for how to think not what the differing knowledge is.

Ms. HYMAN. It might also be useful to take a look at the current National Guard personnel that are actually certified in cybersecurity capabilities just to get a sense of what that rotational workforce might look like.

Mr. COOPER. Set up a new program along the line of what we talked about for veterans and unemployed workers, jointly funded, public-private partnership, graduates of 2-year, 4-year program, whatever, rigorous certification. Companies that hire these people receive additional acquisition points in competitive procurements, based upon the number of people they are hiring out of this program and competitive solicitations.

Mr. HURD. I'd like to thank our witnesses for taking the time to appear before us today.

I ask unanimous consent that members have 5 legislative days to submit questions for the record.

Without objection, so ordered.

And if there's no further business, without objection, this subcommittee stands adjourned.

[Whereupon, at 3:55 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Written Testimony of
Steven Weber, Faculty Director, UC Berkeley Center for Long-Term Cybersecurity
Jesse Goldhammer, Associate Dean, UC Berkeley School of Information
and Betsy Cooper, Executive Director, UC Berkeley Center for Long-Term Cybersecurity

Before the
Subcommittee on Information Technology,
Committee on Oversight and Government Reform,
U.S. House of Representative

April 4, 2017

We are pleased to contribute written testimony to the Committee regarding the cybersecurity workforce talent gap, particularly with regard to the committee's interest in public and private skills shortages, and the prospects for an industry-government rotational workforce. As representatives of one of three national cybersecurity centers founded through the Hewlett Foundation Cyber Initiative—and the only one at a Tier One public research university—we are deeply concerned about the shortage of cybersecurity professionals to fill available jobs. UC Berkeley will contribute to narrowing the human capital gap as we plan to launch in 2018 an online cybersecurity masters' degree program that will be available to students across the country.[1]

At the same time, we believe that the committee should focus its attention not just on the numbers that describe the cybersecurity labor market gap, but on the specific reasons why skills are lacking and jobs remain unfilled. We believe that one significant reason the federal government is struggling to fill its cybersecurity workforce is that there are few opportunities for private-sector technologists to work for the government without having to relocate to Washington, DC to take a permanent government job. Put simply, the dynamic flows of knowledge and talent that energize the Silicon Valley technology and human capital ecosystem are not mobilized to the benefit of government cybersecurity needs. In the below testimony, we outline the skills shortage issue and propose a solution —a Silicon-Valley based Cyber Workforce Incubator—that can address this urgent challenge.

Importantly, we do not believe that this organization should be based in a federal agency, nor should it be solely funded by federal dollars. An independent 501(c)(3) in the model of In-Q-Tel, and funded jointly by the government and private sector, will best reduce the friction that discourages private-sector technologists from working on government problems, and often prevents West Coast talent from working in East Coast government agencies.

The Nature of the Cybersecurity Skills Shortage Problem

Cybersecurity is arguably the fastest-growing and most important subfield of information technology. Yet the dramatic rise in the importance of cybersecurity has been accompanied by a severe shortage of trained professionals. In the private sector, "[t]he demand for the [cyber security] workforce

[1] For more information, see cybersecurity.berkeley.edu.

is expected to rise to 6 million (globally) by 2019, with projected shortfall of 1.5 million."[2] Already, more than 209,000 cybersecurity jobs in the United States are unfilled; demand is expected to grow by 53 percent through 2018."[3] Cisco estimates there are more than one million unfilled cybersecurity jobs worldwide,[4] while the UK House of Lords estimates two million.[5]

The United States cybersecurity infrastructure has also struggled to recruit private-sector talent into the federal government. The Department of Defense aimed to find 6,200 operators to fill CYBERCOM's 133 Cyber Mission Force teams by 2018, with an interim goal of reaching "initial operating capacity" by the end of 2016.[6] In 2015, Admiral Mike Rogers said that CYBERCOM was "already hard pressed" to find qualified candidates to fill its 133 Cyber Mission Force teams.[7] As of January 2017, there are reportedly 123 teams, with only 27 operating at full capacity.[8] These problems are not limited to the military; even prior to the recently implemented hiring freeze in the federal government, more than 1,000 federal cybersecurity jobs were unfilled.[9]

The prototypical way of explaining this cybersecurity labor market shortage is to describe it as a "market failure" into which the government should intervene. But we believe that treating the entire cybersecurity market as a unilateral entity that is "failing", or to assume that one policy solution could resolve this problem, would be a mistake. Instead, there are likely multiple markets for cybersecurity professionals, and/or multiple challenges or failures to be faced, requiring separate solutions.

We focus here on one particular market problem: today, when the US Government wishes to solve digital national security problems, it almost exclusively draws upon East Coast-based government employees or contractors. With rare exception, the West Coast's private-sector cybersecurity technologists, who often have precisely the skills most needed in the federal government, have displayed little interest in working for the national security community. While senior cybersecurity leaders recognize the need for this talent, many structural, bureaucratic, and cultural factors have contributed to the acute government labor shortage, including:

---

[2] Steve Morgan, "One Million Cybersecurity Job Openings In 2016." *Forbes* (Jan. 2, 2016) (quoting Michael Brown, CEO of Symantec), https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#3bd0a4b827ea.

[3] Setalvad, Ariha. "Demand to Fill Cybersecurity Jobs Booming." Peninsula Press (March 31, 2015), http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/.

[4] Cisco. *Mitigating the Cybersecurity Skills Shortage* (2015), http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf.

[5] Morgan, Lewis, "Global shortage of two million cyber security professionals by 2017," IT Governance (Oct. 30, 2014), http://www.itgovernance.co.uk/blog/global-shortage-of-two-million-cyber-security-professionals-by-2017/.

[6] United States. Department of Defense. "The Department of Defense Cyber Strategy." April 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[7] Rogers, Mike. "A Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities." March 4, 2015. http://docs.house.gov/meetings/AS/AS26/20150304/103093/HHRG-114-AS26-Wstate-RogersM-20150304.pdf

[8] Maucione, Scott. "CYBERCOM's New Buying Power Now Closer to Reality." *Federal News Radio,* January 2017. http://federalnewsradio.com/acquisition/2017/01/cybercoms-new-buying-power-now-closer-reality/

[9] Sternstein, Aliya. "Trump's hiring freeze blunts rush to recruit cybersecurity talent." *Christian Science Monitor Passcode,* January 25, 2017, http://www.csmonitor.com/World/Passcode/2017/0125/Trump-s-hiring-freeze-blunts-rush-to-recruit-cybersecurity-talent.

- Demand for cybersecurity professionals that is expanding rapidly across sectors, leaving the federal government in competition with the private sector for top talent;
- A cultural disconnect between 'West Coast' and 'East Coast' work styles, which is partially the result of lengthy, bureaucratic decisionmaking that can delay testing and implementation of new technology solutions, as well as poor work environments in aging government buildings;
- Organizational tensions between government and private sector work structures, including lengthy, cumbersome security clearance processes that often cause applicants to lose interest in government jobs before their application process is completed, and security policies that can unnecessarily isolate employees from their social and professional networks;
- Geographic and career rigidities within the federal government, including risk averse government managers, and relocation requirements from preferred technology hubs like Boston, Austin, and, most importantly, Silicon Valley to the greater Washington, DC area; and
- The inability to easily transition between government and private-sector roles, particularly since it may be difficult to stay current on the latest private-sector technological developments while working in government.

While the US Government is already seeking to remedy these organizational challenges on a piecemeal basis, it takes significant time and effort to change large organizations. To make cybersecurity agencies hospitable to highly innovative, private-sector technologists would require senior US Government leaders to make significant and simultaneous structural changes to HR and security policies, professional incentives, work environments, and management techniques. Such changes would almost certainly be disruptive to the existing workforce and would likely be met with resistance from current government employees, rendering the changes ineffective.

Moreover, even if the US Government *could* find ways to convince sufficient numbers of West Coast professionals to relocate to Washington, we do not believe this would be advisable because the quality of that talent depends precisely on its intimate, ongoing connection to the entrepreneurial ecosystem present in Silicon Valley. This ecosystem, which is most fertile in Silicon Valley but also present in other entrepreneurial hubs, develops talent through:

- A culture of relentless experimentation and the nimbleness to shift resources away from "dead ends" with relatively little friction;
- A relatively open labor market where people circulate and re-mix expertise by moving around through different companies;
- A large and dynamic professional community that shares common values, and that is continuously re-infused with research and thought leadership by two of the world's top universities; and
- Powerful economic incentives that encourage the rapid commercialization of emerging technologies.

Especially in the short to medium term, this system simply cannot be replicated inside government. As a result, it is important for the federal government to find a way to access cybersecurity talent within the Silicon Valley ecosystem, and not remove talent from it.

A New Model for an Industry-Government Rotational Workforce: The Cyber Workforce Incubator

We have so far argued that West Coast cybersecurity professionals do not want to work for the federal government under current conditions. But this is not the same as saying that West Coast cybersecurity professionals do not want 'government jobs' per se. We believe that, if such professionals were given the ability to work on national security challenges without degrading their cutting-edge technical skills or requiring them to give up their livelihoods, work cultures, and social networks—and to leverage that experience to advance their career—many would jump at the opportunity.

Other proposed industry-government rotational workforce solutions—such as a Cyber Reserve Force or temporary appointments within the US Digital Service—are not well equipped to provide this type of work experience. While a traditional rotational program would reduce one barrier to entry—enabling short-term private-sector engagement with interesting US Government problems—it would not attract those deterred by the cultural differences, geographic distance, or career rigidities within the federal government.

We have released a white paper, "Cyber Workforce Incubator," (available at https://cltc.berkeley.edu/, and attached as an appendix), describing an institution that we think could better attract the West Coast's best technologists to work for the US Government. Through a careful application and vetting process, , the CWI would choose promising private-sector candidates for a one- or two-year workforce development program. Participants would undergo a rapid security clearance process before joining specialized teams that have needed technology skills; collaborate with defense, intelligence, and homeland security partners; and work on discrete projects that achieve defined mission objectives. CWI would replicate the environment, culture, and pace of West Coast startups, dramatically increasing the benefits and reducing the costs for private-sector technology talent to engage in national service. CWI would also provide state-of-the-art training and mentorship to participants, who will complete the program with new and more refined skills that will ultimately benefit federal, non-profit, or corporate employers. Incubator participant stipends would combine federal dollars and corporate donations, ensuring that private-sector organizations share some of the costs of training talent from which they will benefit

By giving technologists and government workers the opportunity to work side by side on unique government problems through short deployments, an incubator will fill a unique workforce niche that government agencies cannot solve themselves or through conventional contractor relationships with academics or private-sector companies. By overcoming a manageable number of geographic and bureaucratic hurdles, such an incubator can help the US government to solve some of its toughest technical innovation challenges, recruit top talent, build a strong reputation, and lay the groundwork for long-term, private-sector cyber technology innovation partnership that will benefit the nation for generations.

We do not believe such an organization should be housed in a federal agency. Instead, following the model of In-Q-Tel and its relationship to CIA, the CWI should be an independent 501(c)(3) nonprofit that is anchored to a particular agency—likely the Department of Defense, CYBERCOM, or NSA—but also serves the needs of other sister agencies. In-Q-Tel, which operates as a venture capital resource to promote technology development for the intelligence community, functions differently than a government agency because of its independent status. In-Q-Tel has successfully identified promising early-stage technologies for the intelligence community because it stands between the public and private

sectors, and so can understand the needs of the intelligence community and translate those needs to start-ups. A cybersecurity incubator could similarly identify promising solutions to difficult problems through its ability to liaise between the public and private sector. This structure would also make it possible for the incubator to work on problems that sit under different authorities (e.g., Title 10 and Title 50).

We believe that joint federal and private-sector funding is the best model for setting up a Cyber Workforce Incubator. Because the CWI experience will provide its participants with marketable skills, the private sector should share the burden in supporting participant stipends and direct operating costs. At the same time, federal investment is necessary to set up the organization, and to demonstrate ongoing US Government support for the initiative. Federal expenses will likely be more significant in the first few years of operation, and will decrease as CWI develops the expertise, relationships, and reputation required to consistently raise private funds.

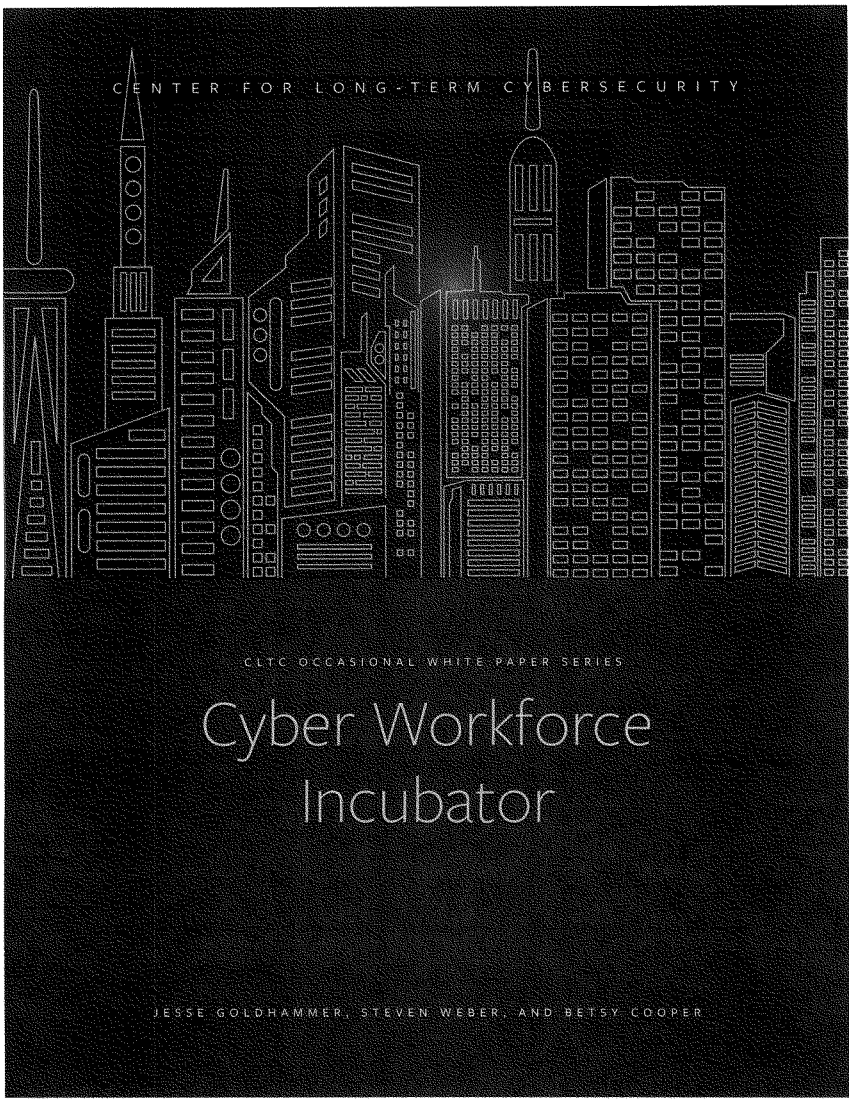
Conclusion

Today, the nation's most talented cyber technologists face a stark choice between private- and public-sector employment. This choice does not serve the nation well, and the costs to national security are mounting as technology evolves and the gap between the private- and public-sector workplace experiences widens. CWI provides the US government with a low-risk, high-impact, and organizationally proven way to leverage top talent without also needing to massively restructure its own work environment, incentives, and systems. We urge the Committee to consider this model as a way to begin closing this particular aspect of the cybersecurity workforce talent gap.

About the Authors

Steve Weber is Faculty Director of the UC Berkeley Center for Long-Term Cybersecurity, as well as a Professor in the School of Information. Jesse Goldhammer is Senior Advisor to the Center, as well as Associate Dean for Business Development and Strategic Planning at the UC Berkeley School of Information. Betsy Cooper is the Executive Director of the Center.

The Center for Long-Term Cybersecurity is a research and collaboration hub housed within the University of California, Berkeley School of Information (I School). Funded through a generous seed grant from the William and Flora Hewlett Foundation, the CLTC has a mission to design solutions to cybersecurity issues that arise wherever humans and digital systems interact, based on a long-term vision of the internet and its future. Working with researchers from UC Berkeley and outside organizations, we are building a diverse community of partners to advance concepts, technologies, and recommendations that will help governments, corporations, and individuals better prepare for the challenges of cybersecurity throughout the 21st century. We focus our work on three streams of activity: Research, Education, and Engagement.


CENTER FOR LONG-TERM CYBERSECURITY
CLTC OCCASIONAL WHITE PAPER SERIES
Cyber Workforce Incubator
JESSE GOLDHAMMER, STEVEN WEBER, AND BETSY COOPER

Summary

The United States urgently needs highly innovative, technically trained personnel for cyber defense and security to protect critical infrastructure and assure vital military and civilian missions. The Defense, Intelligence, and Homeland Security communities struggle to acquire, train, and retain sufficient numbers of cutting-edge technologists who can help the government innovate faster and more effectively than our adversaries, specifically in the domain of cybersecurity.

Cyber defense and security require a highly skilled, deeply technical workforce that has experience with the latest hardware and software as well as the know-how and mindset to solve a wide range of complex, ambiguous problems. Women and men across the West Coast have these capabilities because they live and work in a regionally distinctive innovation ecosystem that enables them to constantly upgrade their knowledge and experience. Today, however, they have no viable, short-term professional opportunities to place their talents in the service of US national security. Moreover, even when the government can attract these workers, those who choose to stay often struggle to keep abreast of fast-moving technology developments in the private sector, which is the center of cyber innovation. This places our government in a position of structural disadvantage. We propose here an approach to overcome and reverse that.

A new, nimble, and innovative not-for-profit Cyber Workforce Incubator would allow the West Coast's best technologists to work on national security challenges without degrading their cutting-edge technical skills or requiring them to give up their livelihoods, work cultures, or social networks. By giving technologists and government workers the opportunity to work side by side on unique government problems through short deployments, an incubator will fill a unique workforce niche that government agencies cannot solve themselves or through conventional contractor relationships with academics or private-sector companies. By overcoming a manageable number of geographic and bureaucratic hurdles, such an incubator can help the US government to solve some of its toughest technical innovation challenges, recruit top talent, build a strong reputation, and lay the groundwork for long-term, private-sector cyber technology innovation partnership that will benefit the nation for generations.

Introduction

Today, the private sector dominates technology innovation in cybersecurity and data science. Thanks to the rapid growth of private-sector technology companies, large segments of the nation's best technology talent are building commercial products and services in established companies and startups, especially on the West Coast. As primary drivers of global technology innovation, these companies are combining speed, agility, ingenuity, creativity, and the profit motive to fundamentally change how humans and machines interact everywhere on the planet. The men and women who work in these companies are driving the future of technology and in the process profoundly shaping how and where the work of cyber innovation takes place.

The United States does not currently have an agile way to leverage the talent of these cybersecurity operators to solve tough, often classified, government cybersecurity problems. As a result, the government is also falling behind in its efforts to create a more resilient federal cybersecurity infrastructure. A not-for-profit Cybersecurity Workforce Incubator (CWI) will help address this problem by providing a low-risk, high-impact, and organizationally proven way to get top West Coast technologists focused on critical mission work. Such an organization would also serve as a unique example of government workforce innovation, as it will draw features from private-sector startups — such as team-building, a risk mindset, and innovation culture — and put them in the service of the government.[1]



The Cybersecurity Workforce Gap

The United States cybersecurity infrastructure — particularly US Cyber Command (CYBERCOM), the Military cybersecurity components, and the Department of Homeland Security (DHS) — struggle to recruit private-sector talent into the federal government. The Department of Defense (DOD) has aimed to find 6,200 operators to fill CYBERCOM's 133 Cyber Mission Force teams by 2018, with an interim goal of reaching "initial operating capacity" by the end of 2016.[2] In 2015, Admiral Mike Rogers said that CYBERCOM was "already hard pressed" to find qualified candidates to fill its 133 Cyber Mission Force teams.[3] As of January 2017, CYBERCOM is reported to have 123 teams, with only 27 operating at full capacity.[4] These capacity problems are not limited to the military; before the Trump Administration implemented a hiring freeze on the federal government, more than 1,000 federal cybersecurity jobs remained unfilled.[5]

In 2013, the DOD released its Cyberspace Workforce Strategy, which recognized that the Department faces "fierce competition" in the labor market and must position itself as an "employer of choice" using a variety of tactics. One strategy the report recommended is to create more transition opportunities "between and within military and civilian service."[6] However, this strategy focused on retaining existing service members, rather than engaging the private-sector talent pool.

One reason that the federal government has struggled to recruit top cybersecurity talent is the East Coast-West Coast divide. Today, when the US Government wishes to solve classified national security problems, it almost exclusively draws upon East Coast-based government employees or contractors. With rare exceptions, the West Coast's private-sector cybersecurity technologists have displayed little interest in working for the national security community. While senior cybersecurity leaders recognize the need for this talent, many bureaucratic and cultural factors mute and dull the call to service, including:

- Lengthy, cumbersome clearance processes that often cause applicants to lose interest;
- Risk-averse government managers who sacrifice innovation to professional advancement;
- The cost and burden of relocating from preferred geographic technology hubs like Boston, Austin and, most importantly, Silicon Valley to the Greater Washington, DC area;
- Security policies that can unnecessarily isolate employees from their social and professional networks;

- Lengthy, bureaucratic decisionmaking that can delay testing and implementation of new technology solutions;
- HR policies and institutions that undermine short-term, meaningful work; and
- Poor work environments in aging government buildings.

While the US Government is already seeking to remedy these organizational challenges on a piecemeal basis, it takes significant time and effort to change large organizations. To make cybersecurity agencies hospitable to highly innovative, private-sector technologists would require senior government leaders to make significant and simultaneous structural changes to HR and security policies, professional incentives, work environments, and management techniques. Such changes would almost certainly be disruptive to the existing workforce and would likely be met with resistance from current government employees, rendering the changes ineffective.

Solution: A Cyber Workforce Incubator

To harness West Coast cyber technology talent and tap directly into the innovation ecosystem in which it grows, the US Government would benefit from a not-for-profit [501(c)(3)], San Francisco Bay Area-based Cyber Workforce Incubator that provides West Coast technologists with the unique ability to work with select personnel on important, classified national security challenges.

HOW IT WOULD WORK

Through a careful application and vetting process, the CWI would choose promising private-sector candidates for a one- or two-year workforce development program. Participants would undergo a rapid security clearance process before joining specialized teams that have needed technology skills; collaborate with defense, intelligence, and homeland security partners; and work on discrete projects that achieve defined mission objectives. CWI would replicate the environment, culture, and pace of West Coast startups, dramatically increasing the benefits and reducing the costs for private-sector technology talent to engage in national service. CWI

would also provide state-of-the-art training and mentorship to participants, who will complete the program with new and more refined skills that will ultimately benefit federal, non-profit, or corporate employers. Incubator participant stipends would combine federal dollars and corporate donations, ensuring that private-sector organizations share some of the costs of training talent from which they will benefit.

By removing the need for the government to make difficult and highly disruptive internal changes to attract top technical talent, CWI would help reduce the friction that prevents skilled private-sector technologists from working on mission-critical challenges. Several underlying assumptions make CWI uniquely attractive:

1. Participants will not have to relocate;
2. Their work is by definition temporary; and
3. Equipped with a new set of skills, they will return after one or two years to the private sector, where they can continue to work on innovative technologies that will help the US Government in the long run.

Once fully set up, CWI would be housed in its own physical location with both unclassified and classified (SCIF) workspaces. CWI would need authority and support to conduct fast-track clearance reviews—modeled on the Intelligence Community's ability to provide rapid, temporary clearances to VIPs for forums like the Enduring Security Framework—so that CWI's technologists can get a high-level clearance in a matter of 6-12 months.[7] CWI would select incubator participants well before the start of the program to ensure they are able to complete their full clearance process.

By serving the defense, intelligence, and homeland security partners through this new model for public-private engagement, CWI would provide the following significant benefits:

Relationship To Existing Programs

Although CWI is fundamentally a workforce development innovation, it is not a high-risk endeavor because it borrows from techniques and approaches that are already proven by other organizations that work closely with US cybersecurity communities, including:

DARPA
The DARPA innovation model features project managers who come from industry and academia for short periods of time to work on hard, future-oriented technical challenges. When a new manager at DARPA receives an identification badge on Day 1, it also prominently features their last day of work two years later. The message is clear: innovation requires a period of intense focus and appropriate risk, not years of incremental change. Key Lesson: Borrowing from the DARPA model, CWI will offer temporary one- or two-year positions to highly talented individuals who wish to work on cybersecurity technology challenges for a set time period.

IN-Q-TEL
This not-for-profit venture capital firm has successfully identified promising early-stage technologies for the intelligence community because it stands between the public and private
continued on page 6

Relationship to Existing Programs
continued from page 5

sectors, allowing it to understand what the intelligence community actually needs and translate those needs to start-up companies in clear language. In-Q-Tel solves an important technology innovation supply-chain problem that acquisitions officers cannot fix themselves.
Key Lesson: Following the In-Q-Tel model, CWI will be a not-for-profit that will be funded both through the US Government and partnerships with corporations looking for CWI graduates. CWI will also build long-term relationships with government officials who need assistance solving time-sensitive, mission-critical technology challenges.

Y COMBINATOR
A funder and seed accelerator, Y Combinator provides the infrastructure, training, and resources necessary for young talent to set up their own technology companies. This firm's approach illustrates a powerful model for addressing the challenge of scouting and developing top technology talent.
Key Lesson: Using Y Combinator's example, CWI will foster team-based work, mentor-mentee relationships, and talent development, so that CWI "graduates" return to the workforce with a sophisticated set of marketable skills and experiences.

- Tiger teams capable of working on mission-critical, classified technology challenges;
- Technologists who are able to bring cutting-edge hardware and software solutions to intractable national security technical challenges and who can remain technically current during their CWI service;
- An elite group of private-sector technologists who may wish to work for the government for longer periods of time;
- An engine for improving the US Government's relationships and brand within Silicon Valley and other technology hubs;
- Knowledge and skill transfer from CWI participants to US government personnel, and vice versa;
- An intermediary organization that helps the US Government to better engage with West Coast start-ups and technology companies;
- A reputation for applying ingenious solutions to intractable workforce challenges that are endemic to the military and to civilian government operations;
- Hundreds of innovators and entrepreneurs who will "graduate" from CWI and go on to build hardware and software that benefit the Department of Defense and secure the nation; and
- A workforce innovation that complements and reinforces other types of technology outreach efforts, such as In-Q-Tel and DIUx.

RELATIONSHIP TO OTHER INITIATIVES

To our knowledge, there are no existing workforce programs that systematically allow the government to leverage top private-sector cybersecurity talent to work directly on actual national security challenges without also forcing those individuals to leave the West Coast and take 'permanent' government, military, or contractor jobs.

Consequently, CWI complements, but does not replicate, several existing efforts to drive workforce improvements in the US Government. For example, the Cyber Mission Force will come online in the medium term and will provide the DOD with cutting-edge

cyber operators from within the four military services. The US Digital Service, soon to be followed by the recently initiated Defense Digital Service, is already demonstrating promise as it matches private-sector technical talent to the general IT needs (e.g., website design) for US agencies. 18F, a federal digital consultancy run out of the General Services Administration (GSA), has already demonstrated value by building modern digital services for federal agencies; 18F successfully operates on a contracting model that allows technologists to work on government projects from offices across the country.[8] DIUx, a DOD initiative that helps bridge the military with the private sector, and In-Q-Tel, a venture capital firm focused on identifying and investing in technologies that will benefit US national security, are well placed to identify and invest in technology for the defense and intelligence communities, respectively.[9]

CWI also complements, but does not replace or overlap traditional military, intelligence, and homeland security agency procurement of academic and private-sector company services. Academics provide deep expertise to the government, but they rarely work on mission-critical projects because they usually lack appropriate clearances, work according to a slower tempo, and must balance their work for the government with other university priorities. Private-sector contractors provide the government with a diversity of unclassified and classified technical services, including some that are core to mission. In many cases, the individuals performing these services are former military or intelligence agency individuals who have spent their whole careers as private-sector government contractors. These employees are often quite effective at solving known technical problems that can be described in a statement of work, but struggle to help the government apply cutting-edge cybersecurity knowledge to ambiguous problems that are hard to disaggregate and even harder to solve. Furthermore, contractors will always have incentives to solve technical problems in ways that generate more government contracting work for their companies.

Relationship to Existing Programs
continued from page 6

UNITED STATES DIGITAL SERVICE (USDS)

The US Digital Service and Innovation Fellowships bring technological talent to the government. Currently in its second year, USDS has been tremendously successful at addressing conventional government IT problems, such as open government, record keeping, website design, and workforce efficiency.

Key Lesson: CWI can learn from the US Digital Service's ability to quickly assemble private-sector technologists into teams that are able to effectively solve complex, unclassified technology challenges.

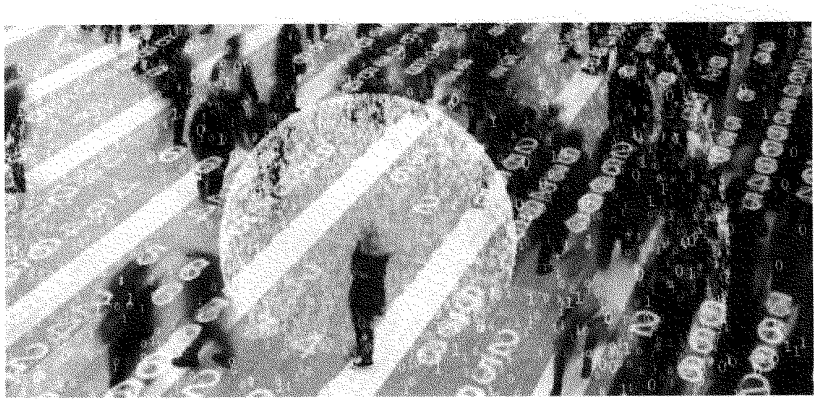
DIUx

DIUx operates in and around major technology hubs and works to identify and pilot cutting-edge technologies that meet government mission needs. Today, DIUx is focused on building relationships with technology companies, funding pilots, and facilitating the procurement of promising, quickly deployable technologies.

Key Lesson: CWI can leverage the relationships that DIUx is building with technology companies, providing them with a new way to develop and retain their talent. CWI might also benefit from DIUx's physical space at Moffett Field.

Conclusion

Today, the nation's most talented cyber technologists face a stark choice between private- and public-sector employment. This choice does not serve the nation well, and the costs to national security are mounting as technology accelerates and the gap between the private- and public-sector experiences widens. CWI provides the US Government with a low-risk, high-impact, and organizationally proven way to leverage top talent without also needing to massively restructure its own work environment, incentives, and systems. Today, some of world's greatest technological talent resides within the West Coast's private-sector innovation ecosystem. CWI will, for the first time, make this talent available to address classified challenges while also conferring long-term strategic benefits to the US Government.



1 This paper focuses primarily on the role a cybersecurity incubator could play in assisting the Department of Defense, Department of Homeland Security, and related intelligence agencies in solving key cybersecurity problems. We encourage the adaption of this policy concept to other agencies' needs — for cybersecurity and beyond.
2 United States. Department of Defense. "The Department of Defense Cyber Strategy." April 2015.
https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
3 Rogers, Mike. "A Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, Before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities." 4 March 2015.
http://docs.house.gov/meetings/AS/AS26/20150304/103093/HHRG-114-AS26-Wstate-RogersM-20150304.pdf
4 Maucione, Scott. "CYBERCOM's New Buying Power Now Closer to Reality." Federal News Radio, 23 January 2017.
http://federalnewsradio.com/acquisition/2017/01/cybercoms-new-buying-power-now-closer-reality/
5 Sternstein, Aliya. "Trump's hiring freeze blunts rush to recruit cybersecurity talent." Christian Science Monitor Passcode, 25 January 2017. http://www.csmonitor.com/World/Passcode/2017/0125/Trump-s-hiring-freeze-blunts-rush-to-recruit-cybersecurity-talent
6 United States. Department of Defense. "Cyberspace Workforce Strategy." 3 December 2013.
http://dodciCWIo.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed(final).pdf
7 The National Guard may also be able to facilitate fast-track clearance reviews through its use of the Defense Support of Civil Authorities (DSCA).
8 News Staff. "What is 18F?" Government Technology, 8 August 2016. http://www.govtech.com/What-is-18F.html
9 Other current efforts, such as the DOD's Force of the Future or the Loaned Executive Program at DHS, may also be instructive.