

PREPARING THE PIPELINE: EXAMINING THE STATE OF AMERICA'S CYBER WORKFORCE

HEARING BEFORE THE COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES ONE HUNDRED NINETEENTH CONGRESS FIRST SESSION

FEBRUARY 5, 2025

Serial No. 119-2

Printed for the use of the Committee on Homeland Security



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

U.S. GOVERNMENT PUBLISHING OFFICE

60-649 PDF

WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas, <i>Vice Chair</i>	BENNIE G. THOMPSON, Mississippi, <i>Ranking Member</i>
CLAY HIGGINS, Louisiana	ERIC SWALWELL, California
MICHAEL GUEST, Mississippi	J. LUIS CORREA, California
CARLOS A. GIMENEZ, Florida	SHRI THANEDAR, Michigan
AUGUST PFLUGER, Texas	SETH MAGAZINER, Rhode Island
ANDREW R. GARBARINO, New York	DANIEL S. GOLDMAN, New York
MARJORIE TAYLOR GREENE, Georgia	DELIA C. RAMIREZ, Illinois
TONY GONZALES, Texas	TIMOTHY M. KENNEDY, New York
MORGAN LUTTRELL, Texas	LAMONICA MCIVER, New Jersey
DALE W. STRONG, Alabama	JULIE JOHNSON, Texas, <i>Vice Ranking Member</i>
JOSH BRECHEEN, Oklahoma	PABLO JOSÉ HERNÁNDEZ, Puerto Rico
ELIJAH CRANE, Arizona	NELLIE POU, New Jersey
ANDREW OGLES, Tennessee	SYLVESTER TURNER, Texas
SHERI BIGGS, South Carolina	VACANT
GABE EVANS, Colorado	VACANT
RYAN MACKENZIE, Pennsylvania	
BRAD KNOTT, North Carolina	

ERIC HEIGHBERGER, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

CONTENTS

	Page
STATEMENTS	
Honorable Mark E. Green, a Representative in Congress From the State of Tennessee, and Chairman, Committee on Homeland Security:	
Oral Statement	1
Prepared Statement	3
Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Oral Statement	11
Prepared Statement	14
WITNESSES	
Mr. David J. Russomanno, PhD, Executive Vice President of Academic Affairs and Provost, University of Memphis:	
Oral Statement	16
Prepared Statement	17
Mr. Robert Rashotte, Vice President, Global Training and Technical Field Enablement, Fortinet:	
Oral Statement	21
Prepared Statement	23
Mr. Chris Jones, President and Chief Executive Officer, Middle Tennessee Electric Membership Corporation:	
Oral Statement	28
Prepared Statement	29
Mr. Max Stier, President and Chief Executive Officer, Partnership for Public Service:	
Oral Statement	32
Prepared Statement	34
FOR THE RECORD	
Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Article by Cyberscoop.com	78
Letter to U.S. Office of Personnel Management	79
Letter to Office of Management and Budget	81
Honorable Elijah Crane, a Representative in Congress From the State of Arizona:	
Article From NextGov/FCW	57

PREPARING THE PIPELINE: EXAMINING THE STATE OF AMERICA'S CYBER WORKFORCE

Wednesday, February 5, 2025

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
WASHINGTON, DC.

The committee met, pursuant to notice, at 10:03 a.m., in room 310, Cannon House Office Building, Hon. Mark Green [Chairman of the committee] presiding.

Present: Representatives Green, McCaul, Higgins, Pfluger, Garbarino, Greene, Gonzales, Luttrell, Strong, Crane, Ogles, Biggs, Mackenzie, Knott, Thompson, Swalwell, Correa, Thanedar, Magaziner, Goldman, Ramirez, McIver, Johnson, Hernández, and Turner.

Chairman GREEN. The committee will come to order. Without objection, the Chair may declare the committee in recess at any point.

The purpose of this hearing is to examine the severity of America's cyber work force gap and assess how the shortage of skilled cyber professionals leaves our homeland vulnerable to evolving global threats in cyber space.

Specifically, we will delve into the challenges that the public and private sectors face in recruiting, training, and retaining skilled cyber talent. We will also discuss possible solutions to mitigate this shortfall.

I now recognize myself for an opening statement. Good morning, everyone. Today we are focused on the top cyber challenge we face and that is the cyber work force gap.

This issue has been a top priority for me and other Members of this committee since the last Congress, and I know it is for many of you in this room as well. There isn't a city or a State in this country not affected by this cyber work force gap.

Currently, our Nation lacks about 500,000 cyber professionals. That is a deficit of 1 million eyes and this means that many of our networks and critical infrastructure are going unwatched even while malicious nation-state actors like Volt and Salt Typhoon target them daily.

At a time when we need to go on the offensive we can barely play defense. We simply don't have enough people in the right jobs with the right skills to stay on top of the significant cyber challenges our homeland faces. We covered many of those threats in our first committee hearing 2 weeks ago and you can get a glimpse of the magnitude of these threats yourself. We captured them in the committee's cyber threat snapshot. You can see a little bit of that here.

Whether we are dealing with China, Russia, North Korea, Iran, or criminal actors, one thing is clear. Our vulnerabilities span from our heartland's hardware to our cities' software. Sometimes we are dealing with targeted attacks like ransomware and sometimes our vulnerabilities stem from poor cyber hygiene or economic models that do not prioritize cybersecurity.

But whatever the case, we need to do better and we need to do better now. Our Nation's security and prosperity depend upon a resilient cyber posture, something that can only be assured by adequately preparing our pipeline of cyber professionals.

Over the years, there have been many initiatives to address the cyber work force gap. Our witnesses here today have been at the forefront of some of those efforts. We applaud those efforts and hope they will continue.

However, it is clear we need a new but complementary approach, one that brings together the public and private sectors to fill gaps at all levels of Government and industry, one that creates quick pathways for individuals who want to pivot in their careers without having to complete a 4-year degree, one that provides hands-on experiences for cyber professionals and training and then supports them throughout their careers, one that cultivates a sense of community and service to the country like the ROTC program, one that's accessible to all Americans, and one that will finally change the decades-long narrative around the cyber work force gap.

I believe that bill is my bill, the Cyber PIVOTT Act. It directly addresses all of these issues in a meaningful way and that is why I reintroduced my bill today alongside Representatives Guest, Gimenez, Higgins, Strong, Biggs, Evans, Moolenaar, Ezell, and Rogers.

We've received significant support for the bill, including the American Association of Community Colleges. I want to thank our stakeholders and would like to submit the following statements for the record: Advocacy Blueprints; Business Software Alliance; Cyber Innovation Centers and their academic initiative cyber.org; Darktrace; Forescout Technologies; Foundation for Defense of Democracies; Information Technology Industry Council; the Internet Security Alliance, ISC2 or squared; Avanti; the McCrary Institute; Microsoft; National Rural Electric Coop Association; Palo Alto Networks; Peraton; the R Street Institute; SentinelOne; Special Competitive Studies; the U.S. Chamber of Commerce, and without objection, so ordered.

It is time to sign the Cyber PIVOTT Act into law, and I look forward to working across the aisle to ensure that we can do so in a bipartisan manner.

Last year we held a full committee hearing on the cybersecurity work force gap with Government witnesses. Today we will examine the perspective of the private sector. Thank you to our expert panel for joining us.

Your diverse experiences in academia, critical infrastructure, cybersecurity, and nonprofits will give us a holistic understanding of the complexities we face in bolstering our cyber work force and the strategies we must consider for reducing the work force gap once and for all. I look forward to this very important discussion.

[The statement of Chairman Green follows:]

STATEMENT OF CHAIRMAN MARK E. GREEN, MD

FEBRUARY 5, 2025

Good morning, everyone.

Today, we're focused on the top cyber challenge we face: the cyber workforce gap. This issue has been a top priority for me since last Congress, and I know it is for many of you as well. There isn't a city or a State in the country not affected by this cyber workforce gap.

Currently, our Nation lacks about 500,000 cyber professionals—that's a deficit of 1 million eyes. This means that many of our networks and critical infrastructure are going unwatched, even while malicious nation-state actors like Volt and Salt Typhoon target them daily.

At a time when we need to go on the offense, we can barely play defense. We simply don't have enough people in the right jobs with the right skills to stay on top of the significant cyber threats our homeland faces.

We covered many of those threats in our first committee hearing 2 weeks ago. And you can get a glimpse of the magnitude of these threats for yourself—we captured them in the committee's "Cyber Threat Snapshot".

Whether we're dealing with China, Russia, North Korea, Iran, or criminal actors, one thing is clear: our vulnerabilities span from our heartland's hardware to our cities' software.

Sometimes we are dealing with targeted attacks like ransomware. And sometimes our vulnerabilities stem from poor cyber hygiene or economic models that do not prioritize cybersecurity.

Whatever the case, we need to do better—now. Our Nation's security and prosperity depend upon a resilient cyber posture—something we can only assure by adequately preparing our pipeline of cyber professionals.

Over the years, there have been many initiatives to address the cyber workforce gap. Our witnesses here today have been at the forefront of some of those efforts. We applaud those efforts and hope they will continue.

However, it is clear we need a new but complementary approach:

One that brings together the public and private sectors to fill skill gaps at all levels of Government and industry.

One that creates quick pathways for individuals who want to pivot in their careers without having to complete a 4-year degree.

One that provides hands-on experiences for cyber professionals in training and then supports them throughout their careers.

One that cultivates a sense of community and service to country, like the ROTC.

One that is accessible to all Americans.

And one that will finally change the decades-long narrative around the cyber workforce gap.

I believe that my bill, the Cyber PIVOTT Act, directly addresses all of these issues in a meaningful way. That is why I re-introduced my bill today, alongside Reps. Guest, Gimenez, Higgins, Strong, Biggs, Evans, Moolenaar, Ezell, and Rogers.

We have received significant support for the bill, including from the American Association of Community Colleges. I want to thank our stakeholders and would like to submit the following statements for the record:

- Advocacy Blueprints
- Business Software Alliance (BSA)
- Cyber Innovation Center and their academic initiative, CYBER.ORG
- Darktrace
- Forescout Technologies
- Foundation for Defense of Democracies (RADM Mark Montgomery and Jiwon Ma)
- Information Technology Industry Council (ITI)
- The Internet Security Alliance (Larry Clinton)
- ISC2
- Ivanti
- The McCrary Institute (Frank Cilluffo)
- Microsoft
- National Rural Electric Coop Association (NRECA)
- Palo Alto Networks
- Peraton
- The R St Institute (Brandon Pugh)
- SentinelOne
- Special Competitive Studies Project
- The U.S. Chamber of Commerce

Without objection, so ordered.

It is time to sign the Cyber PIVOTT Act into law, and I look forward to working across the aisle to ensure we can do so in a bipartisan manner.

Last year, we held a full committee hearing on the cybersecurity workforce gap with Government witnesses. Today, we will examine the perspective of the private sector.

Thank you to our expert panel for joining us. Your diverse experiences in academia, critical infrastructure, cybersecurity, and non-profits will give us a holistic understanding of the complexities we face in bolstering our cyber workforce, and the strategies we must consider for reducing the workforce gap once and for all.

I look forward to this important discussion.

SUPPORT STATEMENTS SUBMITTED BY CHAIRMAN MARK E. GREEN

R STREET INSTITUTE

Chairman Mark Green's Cyber PIVOTT Act provides an innovative and meaningful way to address the cyber workforce shortage in the United States, which has been a challenge for many years. This shortage negatively impacts the cybersecurity posture of our Nation in the public and private sectors while the threat landscape continues to evolve. This legislation is designed to address these challenges in both the short and long term and recognizes that a 4-year degree is not the only path one can take to enter the cyber workforce. Given R Street's long-time commitment to studying and addressing the cyber workforce shortage, we are pleased to support the Cyber PIVOTT Act.

BRANDON PUGH,
Director and Senior Fellow,
Cybersecurity and Emerging Threats, R Street Institute.

ISC2

On behalf of ISC2 and its global community of nearly 275,000 certified members, and associates, we strongly support the PIVOTT Act. This legislation represents a crucial step toward strengthening the cybersecurity workforce and addressing the growing demands of an increasingly digital world. By recognizing certification as a viable and valuable pathway for professionals in the field, this legislation acknowledges that expertise in cybersecurity is not solely defined by traditional academic degrees, but by demonstrable skills and practical experience.

In today's ever-evolving cyber landscape, certifications provide a globally-recognized, standardized method of assessing an individual's technical proficiency and readiness for the challenges organizations face. The PIVOTT Act empowers individuals to validate their knowledge through legitimate industry certifications, giving them greater opportunities to advance their careers, contribute to organizational security, and ultimately help protect national critical infrastructure from cyber threats.

The PIVOTT Act is a critical investment in the future of cybersecurity, aligning with industry needs and providing a clear path for those passionate about living in a safe and secure world. This approach will enhance the resilience of both public and private sectors against emerging cyber threats.

FORESCOUT TECHNOLOGIES

"The cybersecurity workforce shortage in the United States leaves OT networks that underpin our critical infrastructure increasingly vulnerable to attack. The Cyber PIVOTT Act takes a crucial and necessary step toward addressing this challenge by expanding hands-on, skills-based training to develop a stronger pipeline of cybersecurity professionals. At Forescout, we believe that equipping the workforce with the expertise to protect the systems that power our economy is vital to strengthening our national resilience. We support the Cyber PIVOTT Act and urge swift passage to bolster cyber defenses where they matter most."

ALISON KING,
VP Government Affairs.

PALO ALTO NETWORKS

Palo Alto Networks applauds Chairman Green on the reintroduction of the Cyber PIVOTT Act. To build a cybersecurity workforce capable of tackling the evolving challenges of modern cyber threats, we must invest in engaging and skills-based cybersecurity workforce development practices that can attract untapped talent and expand pathways into cybersecurity roles, especially in the public sector. The bill's

recognition of the importance of collaboration between the Government, community colleges, and industry and the power of hands-on, skills-based exercises will help build a pipeline of skilled professionals capable of protecting our digital way of life.

DANIEL KROESE,

Vice President, Public Policy & Government Affairs at Palo Alto Networks.

IVANTI

Ivanti welcomes the introduction of Chairman Green's Cyber PIVOTT Act in the 119th Congress. At a time when highly-resourced nation-states are proliferating their cyber attacks against U.S. companies and critical infrastructure, one of the most urgent needs is to develop a well-trained, sophisticated cyber workforce within the U.S. Government to protect Government agencies and to assist private companies in preventing and responding to cyber attacks.

"As a software developer and vendor that works closely with U.S. Government, Ivanti has seen first-hand the need for the development of a skilled cyber workforce pipeline that can strengthen security for the U.S. Government and create a safer cyber environment for critical industries in the U.S. The Cyber PIVOTT Act is the right approach to developing this talent," said Brooke Johnson, senior vice president and chief legal counsel at Ivanti.

Ivanti applauds Chairman Green for his leadership on this issue, and we look forward to working with him and his office to enact this legislation.

BUSINESS SOFTWARE ALLIANCE (BSA)

"BSA appreciates Congressman Green's leadership in introducing the Cyber PIVOTT Act, which addresses the cyber workforce shortage that is occurring in the U.S. According to the Cybersecurity Supply and Demand Heat Map, there are currently over 450,000 cybersecurity job openings in the U.S. that could be addressed with meaningful legislation such as this.

"With the current workforce shortage, the U.S. is exposed to economic and national security risks. Creating a cyber pathway for those amid a career change or at the beginning of their careers increases the accessibility of cyber training by mobilizing American workers to fill the cyber workforce gap. BSA identified upskilling American workers and building a cyber workforce in its 2025 Cyber Legislative Agenda and the 2025 Global Cyber Agenda, one of the many ways that the U.S. Government can improve cybersecurity and resilience while engaging the U.S. workforce.

"The programs outlined in the bill will take the meaningful steps needed to address the critical cyber shortage and secure the U.S. Government with a beneficial partnership with the Cybersecurity and Infrastructure Agency. BSA is looking forward to working with Rep. Green to ensure that building a cyber workforce remains a priority for policy makers."

U.S. CHAMBER OF COMMERCE

"The U.S. Chamber of Commerce welcomes Rep. Mark Green's (R-TN) Cyber PIVOTT Act. Inspired by ROTC scholarship programs, this bill would help build up more talent to defend our networks against foreign threats and criminal organizations. Last year, the House Homeland Security Committee unanimously reported the Cyber PIVOTT Act. The Chamber urges Congress to swiftly pass this important legislation."

THE HON. RODNEY DAVIS,

Senior Vice President for Government Affairs, U.S. Chamber of Commerce.

INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI)

ITI is encouraged by the introduction of Chairman Green's Providing Individuals Various Opportunities for Technical Training to Build a Skills-Based Cyber Workforce Act (Cyber PIVOTT Act). With over 500,000 cybersecurity jobs open, and increasing cybersecurity attacks, it is imperative to bolster the Nation's cybersecurity workforce. The need for a skilled U.S. cybersecurity workforce is evident, and this bill would create opportunities for those to obtain the skills needed takes a crucial step in expanding the workforce pipeline. ITI applauds the Homeland Security Committee and Chairman Green's emphasis on finding a long-term solution to training and maintaining a qualified cybersecurity workforce.

MICROSOFT

"The Cyber PIVOTT Act takes important steps to bolster our Nation's cyber defense. By investing in education and technical training at America's community col-

leges, this legislation will help tap into a wider talent pool, cultivate a skilled workforce, and equip workers with the skills to combat new and evolving threats. Thank you to Chairman Green for his leadership on this issue,” said Fred Humphries, Corporate Vice President of U.S. Government Affairs at Microsoft.

ADVOCACY BLUEPRINTS

Nicole Tisdale, Founder and Principal

As the founder of Advocacy Blueprints, cybersecurity attorney, and a native of rural Mississippi, I strongly support Chairman Green’s Cyber PIVOTT Act, which addresses critical cybersecurity workforce needs in America, especially our rural communities. Our recent threat analysis found that when compared to urban cities, the 66.3 million Americans living in rural areas are facing the same escalating cyber threats to their hospitals, water systems, schools and critical infrastructure.

The Cyber PIVOTT Act takes a practical approach by creating accessible pathways through 2-year degrees and technical certifications at community colleges. We’re especially excited about the Act’s emphasis on Government service and practical training through internships to ensure these skills directly benefit rural communities through roles at local utilities, schools, emergency services, and critical infrastructure operators.

This model recognizes that rural communities need home-grown cyber talent who understand local systems and can protect essential services where they live.

We look forward to working with Chairman Green, additional Members of the House Committee on Homeland, the U.S. Senate, and stakeholders to advance this important workforce development initiative that strengthens our national security.

DARKTRACE

Marcus Fowler, CEO of Darktrace Federal, said: “At Darktrace, we see first-hand the urgent need for a stronger cybersecurity workforce. There are vast numbers of unfilled cybersecurity roles across the United States, leaving businesses and Government agencies vulnerable. The Cyber PIVOTT Act is a critical step toward closing this gap by creating smarter workforce development pathways, expanding access to hands-on training, and building a skills-based cybersecurity talent pipeline that meets the demands of today’s economy. To achieve this goal, we’ll also need to ensure security teams are trained on the most advanced tools, to ensure that technology fulfils its potential to augment the workforce and act as a true force multiplier. Darktrace believes that a smarter Federal cyber workforce policy when combined with greater adoption of AI-powered cybersecurity technologies, marks the best path forward toward meeting America’s skills and capabilities needs and building a more resilient national cyber defense.”

SPECIAL COMPETITIVE STUDIES PROJECT

The Cyber PIVOTT Act will strengthen America’s cybersecurity by expanding technical training and workforce development. Expanding access to cybersecurity education through community colleges and technical schools fills critical gaps and prepares the next generation of professionals to defend our Nation’s critical infrastructure. This bill is a strategic step toward a more secure and resilient digital future.

YLLI BAJRAKTARI,
CEO, SCSP-Action Program.

IBM

IBM commends Chairman Green for introducing the Cyber PIVOTT Act that would help more Americans seeking cybersecurity skilling pathways through programs at community colleges and technical schools through a new scholarship program. “IBM has long recognized the importance of closing the skills gap across technology, including cybersecurity, which is essential for AI innovation. Our company has a commitment to skill 30 million learners world-wide by 2030. As part of this work, recently we unveiled a new IBM SkillsBuild certificate in cybersecurity, which was piloted and designed with community colleges. We look forward to working with Congress to expand cybersecurity pathways and help more Americans pursue cybersecurity jobs.”

LYDIA LOGAN,
VP of Global Education and Workforce Development, IBM.

November 7, 2024.

The Honorable MARK GREEN, M.D.,
Chairman, House Committee on Homeland Security, H2-176 Ford House Office
Building, Washington, DC 20515.

The Honorable BENNIE G. THOMPSON,
Ranking Member, House Committee on Homeland Security, H2-117 Ford House Of-
fice Building, Washington, DC 20515.

CHAIRMAN GREEN AND RANKING MEMBER THOMPSON:

Thank you for your leadership on cybersecurity issues and commitment to protecting our Nation's critical infrastructure. I am writing today on behalf of the National Rural Electric Cooperative Association (NRECA) in support of H.R. 9770, the Cyber PIVOTT Act. This legislation will promote the development of a skilled cyber workers in rural America. NRECA applauds the strong bipartisan support for this bill as it passed the Homeland Security Committee.

NRECA is the national trade association representing nearly 900 not-for-profit electric cooperatives. America's electric cooperatives are owned by the people they serve and comprise a unique sector of the electric industry. From rapidly growing regions of the country to remote farming communities, electric cooperatives serve as engines of economic development for 42 million Americans across 56 percent of the Nation's landscape.

Electric utilities can be targets for cyber attacks because of their pivotal role in generating and distributing electricity to support our national security and our daily life. Defending our critical infrastructure requires a skilled workforce capable of implementing strong cybersecurity measures to safeguard against challenging and ever-evolving threats. In 2023, the National Institute of Standards and Technology reported that only 20 percent of business leaders at energy utilities felt confident they had the cyber talent they needed. The Cyber PIVOTT Act is a positive step toward filling our Nation's nearly 500,000 open cybersecurity jobs by developing a robust and skilled workforce ready to meet the challenges of the cyber landscape.

NRECA is particularly pleased with the inclusion of language that would extend cybersecurity internship opportunities to critical infrastructure in rural communities. While no sector or region is immune to the challenges of recruiting and retaining skilled cyber professionals, these challenges are exacerbated by the unique and inherent characteristics of rural areas. The Cyber PIVOTT Act will bridge the skills gap, enabling rural communities to strengthen their cyber defenses and secure their critical infrastructure.

The investments made by the Cyber PIVOTT Act in cybersecurity education and training are crucial to building a workforce capable of protecting our critical infrastructure. We appreciate the bipartisan support for addressing these issues and urge Congress to pass this legislation.

Sincerely,

JIM MATHESON.

INTERNET SECURITY ALLIANCE STATEMENT OF SUPPORT FOR THE PIVOTT ACT

The Internet Security Alliance (ISA) thanks and congratulates Chairman Mark Green on the introduction of the PIVOTT Act.

If enacted this bill would be the most impactful piece of cybersecurity legislation ever passed by the U.S. Congress.

It would be the most impactful because, for the first time, it addresses the USA's most basic cybersecurity need—the lack of an adequately trained cybersecurity workforce—at scale.

None of our country's cybersecurity programs can operate properly without an adequately-trained workforce. The technology can't work, the standards can't work, the frameworks can't work, the regulations can't work. Nothing can work effectively without an adequately trained workforce.

Currently we have a workforce shortage of between 500,000 and 750,000 people—an estimated 35,000 people short in the Federal Government alone—and the gap is growing at up to 10 percent a year.

When fully operational, the PIVOTT Act will be the first legislation that addresses this fundamental issue from its appropriate national perspective and at 10,000 new recruits a year, at a scale that will begin to make a dent in this gap.

The PIVOTT Act addresses a core problem with traditional cyber workforce programs by focusing on recruiting previously under-targeted groups such as certification programs and community colleges by expanding the traditional military academy model of providing free security training in return for Government service. In

doing so PIVOTT recognizes that cybersecurity is a matter of critical national and homeland security equivalent to traditional military defense.

The graduates of the PIVOTT program will also become available to the badly underfunded cybersecurity programs in State and local governments, which, due to their interconnections with the Federal Government currently represent a major—and currently unsecured—vulnerability to our national cyber systems.

PIVOTT is also a cost-effective approach to the cyber workforce problem since the PIVOTT graduates will be able to replace the high-priced independent contractors the Government currently needs to hire from the open market at vastly inflated costs.

PIVOTT will be the ISA's No. 1 legislative priority in the Congress, and we urge all entities who care about our Nation's cybersecurity to join in aggressively supporting PIVOTT's passage in the House, Senate, and eventually receive President Trump's signature.

LETTER FROM SCOTT COOPER, VICE PRESIDENT, GOVERNMENT RELATIONS, PERATON CORPORATION

February 3, 2025.

Chairman MARK GREEN, (R-TN),
House Homeland Security Committee, U.S. House of Representatives, Ford House Office Building, Washington, DC 20515.

RE: Letter of Support for the Cyber PIVOTT Act

DEAR CHAIRMAN GREEN:

We write to express our strong support for your cyber workforce bill, the Providing Individuals Various Opportunities for Technical Training (PIVOTT) to Build a Skills-based Cyber Workforce Act of 2025. We look forward to the House acting on the Cyber PIVOTT Act in the near term so that we focus on building a robust and resilient cyber workforce to confront the cyber threats that our country faces.

The cyber threats to our country have only increased over the last few years, particularly to the U.S. critical infrastructure and civilian networks. On January 22, 2025, the Committee held a hearing entitled, "Unconstrained Actors: Assessing Global Cyber Threats to the Homeland" to examine the threats we face, which highlighted the need to build a robust cyber workforce. As you said in the hearing, "the American economy, our government and the military depend upon the resilience of our networks and our infrastructure. It's past time for us to get a step ahead of the typhoons, a list of actors that seem to grow every day." You continued saying, "to do this, we need prepared cyber professionals." To that end, we appreciate that you have made it a top priority to enact the Cyber PIVOTT Act to grow the cyber workforce.

The Cyber PIVOTT Act provides access to cyber training and education with a scholarship program for 2-year degrees at community colleges and technical skills in exchange for Government service. This program will encourage technical training, and education needed to ensure the Government has the cyber workforce necessary to defend the homeland.

As a Federal contractor and a company with more than 3,000 military veterans, we at Peraton recognize the importance of ensuring the U.S. Government has the best and brightest cyber workforce on duty to defend the homeland against increasing cyber threats.

Peraton is a national security company that drives missions of consequence spanning the globe and partners regularly with the U.S. Government to fulfill its cybersecurity mission. We are the world's leading mission capability integrator and transformative enterprise IT provider, delivering trusted, highly differentiated solutions and technologies that protect our Nation and allies from threats across the digital and physical domains.

We strongly support the Cyber PIVOTT Act and look forward to continuing to partner with you to build a robust, capable, and resilient cyber workforce ready to confront the cyber threats of today.

Sincerely,

SCOTT COOPER,
Vice President, Government Relations.

STATEMENT OF RADM (RET.) MARK MONTGOMERY AND JIWON MA, FOUNDATION FOR
DEFENSE OF DEMOCRACIES

FEBRUARY 5, 2025

THE PIVOTT ACT IS PIVOTAL TO SECURING THE FUTURE OF THE FEDERAL CYBER
WORKFORCE

Last week, a number of experts testified to the significant threat that the United States faces in cyber space, especially from the aggressive and malicious cyber behavior of the Chinese Communist Party. Addressing this cyber threat will require efforts across all the dimensions of cybersecurity, including technology, policy, and processes, and—most importantly—personnel. The committee’s decision to next look at the cyber workforce issue is an astute one, as this is the dimension that can most rapidly and effectively address the shortfalls in Federal, State, and local government cybersecurity efforts.

We are confident that the committee will read and hear a number of good ideas in the upcoming hearing, but Congress already holds the most important tools needed to move forward—legislation that was introduced in the 118th Congress and that needs to be passed in the 119th Congress. Specifically, the Providing Individuals Various Opportunities for Technical Training to Build a Skills-Based Cyber Workforce (PIVOTT) Act provides an excellent vehicle to identify, recruit, and train the next generation of the cyber workforce by utilizing proven techniques and leveraging existing Governmental programs to identify supporting institutions. Similarly, the Federal Cyber Workforce Training Act provides a blueprint of how to properly onboard and continue to develop the graduates of the PIVOTT Act programs as they enter the Federal cyber workforce. Passing both of these provisions would make 2025 a banner year for the cyber workforce.

WORKFORCE CHALLENGES AT THE FEDERAL, STATE, AND LOCAL LEVELS

The United States is grappling with a shortage of cybersecurity professionals, with estimates placing the cyber workforce gap at over 500,000 unfilled positions nationwide. This deficit has a cascading impact on the public sector, where Federal, State, and local government agencies struggle to compete with private-sector compensation and streamlined hiring processes.

These vacant cybersecurity roles weaken the Federal Government’s ability to defend against national security threats. State and local governments face an equally acute challenge, operating with an unsustainable defense model constrained by budget shortfalls and limited cybersecurity personnel. Many local governments have just a handful of dedicated staff protecting multiple disparate systems, leaving locally-operated critical infrastructures such as water utilities, transportation systems, and energy facilities vulnerable to ransomware attacks and cyber intrusions.

Outdated hiring frameworks further compound the issue. Federal agencies continue to prioritize 4-year degrees, overlooking highly-skilled professionals with in-demand industry certifications and real-world expertise that do not fit traditional academic criteria for hiring.

ON-GOING FEDERAL EFFORTS

Over the past 2 decades, the Federal Government has implemented initiatives across multiple agencies to expand and sustain its cybersecurity workforce, including flagship programs like CyberCorps: Scholarship for Service and the Cyber Excepted Service at the Department of Defense.

For 25 years, the CyberCorps: Scholarship for Service, modeled after ROTC programs, has placed graduates into Federal cybersecurity roles by offering scholarships in exchange for Government service. The program now places approximately 450 graduates annually into Federal cybersecurity positions. Similarly, for nearly a decade, the Defense Department’s Cyber Excepted Service has attracted and retained more than 15,000 defense civilian employees with cyber skills, providing the Department with critical workforce agility. The program continues to grow, offering enhanced hiring flexibility for cyber and IT personnel, strengthening the U.S. military’s readiness and ability to win wars.

While these programs have successfully grown Federal cybersecurity talent over the years, they remain limited in accessibility for individuals who pursue non-traditional degree pathways. Without additional Federal initiatives to diversify recruitment and hiring efforts, cyber roles will remain unfilled.

OPPORTUNITIES FOR CONGRESS

Addressing this crisis requires bold workforce reforms, and the 119th Congress has a unique opportunity to expand the reach of successful programs. Introduced by Chairman Green, the PIVOTT Act is intended to recruit into Government highly-skilled individuals trained through vocational schools, community colleges, and industry certification programs. Like CyberCorps, the PIVOTT program would provide scholarships, training, and internships to students at community colleges and technical schools in exchange for a 2-year service commitment to Federal, State, or local government. The PIVOTT Act therefore provides a scalability and speed currently lacking in Federal programs. This new program would provide expanded opportunities for motivated Americans to acquire a great skill, secure a great job, and serve a great country.

Additionally, Congress must focus on the retention of the Federal workforce by establishing a complementary initiative that improves on-boarding and incentives for newly-hired and existing Federal cybersecurity employees. The Federal Workforce Development Institute, which is the centerpiece of the Federal Cyber Workforce Training Act, would help modernize hiring by streamlining processes, improving initial training and orientation for junior employees, and expanding training pathways to better compete with the private sector. By improving initial onboarding, the Federal Government can get a head start on an improved development and retention process.

Cyber threats have proven to be persistent risks, disrupting the essential systems Americans rely on every day. With a strong foundation, individuals who are properly trained, on-boarded, and empowered to serve their country will play a vital role in reinforcing public trust in our Government and go on to strengthen national defense against cyber threats throughout their careers.

CONCLUSION

A healthy and robust cyber workforce is the backbone of U.S. national security. As cyber threats evolve, so must our strategy to defend against them. Opportunities through the PIVOTT Act and the Federal Cyber Workforce Training Act are not just workforce solutions—they are strategic investments in protecting America’s critical infrastructure and Government systems. Without a steady influx of talented individuals serving our country, adversaries will continue to exploit vulnerabilities in Federal networks. Developing and sustaining a strong talent pipeline of cybersecurity professionals are critical to ensuring the Nation has the capacity to detect, prevent, and respond to evolving cyber threats before they cause irreparable harm.

LETTER FROM KEVIN NOLTEN, PRESIDENT, CYBER INNOVATION CENTER

February 4, 2025.

The Honorable Chairman MARK E. GREEN, MD,
Committee on Homeland Security, H2-176 Ford House Office Building, Washington, DC 20515.

DEAR CHAIRMAN GREEN: On behalf of the Cyber Innovation Center (CIC) and our academic initiative, CYBER.ORG, I am writing to express our support of the “Providing Individuals Various Opportunities for Technical Training to Build a Skills-Based Cyber Workforce Act of 2024” or the “Cyber PIVOTT Act.”

Based in northwest Louisiana, the CIC is a 501(c)(3) nonprofit, economic, and workforce development organization that provides communities and schools in all 50 States with cybersecurity curricula and content, technology resources, and training that supports over 38,000 educators and 5.3 million students.

Additionally, CYBER.ORG is the current recipient of the Cybersecurity and Infrastructure Security Agency’s Cybersecurity Education and Training Assistance Program (CETAP), a competitively-awarded, multi-year grant focused on building a workforce pipeline to address our national cybersecurity workforce shortage.

We believe the Cyber PIVOTT Act will provide valuable incentives, resources, and opportunities to students pursuing cybersecurity education and training, encouraging more individuals to serve our Federal, State, local, Tribal, and territorial governments in cyber or cyber-relevant roles. Filling these critical cybersecurity workforce gaps will enable our Nation to defend its critical infrastructure and ensure our national and economic security. For these reasons, we are pleased to support the Cyber PIVOTT Act.

Sincerely,

KEVIN NOLTEN,
President, Cyber Innovation Center.

LETTER FROM FRANK CILLUFFO, DIRECTOR, MCCRARY INSTITUTE FOR CYBER AND
CRITICAL INFRASTRUCTURE SECURITY

Tuesday, February 4, 2025.

*Committee on Homeland Security, H2-176 Ford House Office Building, U.S. House
of Representatives, Washington, DC 20515.*

CHAIRMAN GREEN, RANKING MEMBER THOMPSON, AND MEMBERS OF THE COMMITTEE: As the committee embarks on its important legislative and oversight work in the 119th Congress, my colleagues at the McCrary Institute and I look forward to engaging on a bipartisan basis with you all to advance our shared objectives of securing U.S. critical infrastructure from a severe and persistent cyber threat environment. In the 118th Congress, I testified before the Subcommittee on Cybersecurity and Critical Infrastructure Protection about the importance of ensuring the resiliency of critical infrastructure sectors. Investing in the current and future cyber workforce, as this bill does, is a vital component of building and maintaining such resiliency.

Our Nation's adversaries, particularly the People's Republic of China (PRC), Russia, Iran, and North Korea, continue to pose a major threat to U.S. critical infrastructure and the American way of life. PRC-backed adversaries like Salt Typhoon, Volt Typhoon, and Flax Typhoon, have infiltrated OT and IT systems across several sectors including telecommunications, energy, Government, high education, transportation, and health care. In order to combat current and future threats to our critical infrastructure, the Federal Government must invest in the development of our cyber workforce via our educational institutions, as outlined in this legislation.

I was pleased to see the Cyber PIVOTT Act pass the committee with an overwhelmingly bipartisan vote in the 118th Congress. The truth is we need everyone rallying to our cyber defense, from K-12 schools to technical and trade institutions and 4-year colleges and universities. This updated version of the bill will allow universities like Auburn to potentially advance the goals of the legislation, just as we have from previous cybersecurity legislation coming out of this committee, such as the State and Local Cybersecurity Improvement Act, which is currently supporting McCrary's work to stand up the Alabama Cybersecurity Intelligence Center (ACIC) with the Alabama Office of Information Technology. Now, more than ever, it is a national security imperative that Congress provide CISA with the resources and authorities needed to secure critical infrastructure sectors from cyber threats, and this legislation aligns with that imperative.

I thank Chairman Green for his leadership on this legislation, and urge the committee to, once again, pass this bill in a bipartisan manner.

Sincerely,

FRANK CILLUFFO,
Director.

Chairman GREEN. I now recognize the gentleman from Mississippi, our Ranking Member Mr. Thompson for his opening statement.

Mr. THOMPSON. Thank you. Thank you very much, Mr. Chairman. Good morning.

I would like to thank our witnesses for agreeing to testify today. I appreciate your expertise and your input is valuable to the committee's work on cyber work force policy.

Just over 2 weeks ago, President Trump was sworn into office. Nearly every day since then there's been a White House directive undermining the Federal Government's ability to serve the American people. There is confusion about which Federal grant funds President Trump froze last week and whether the funds are still frozen. The administration refuses to give Americans a straight answer about that.

Disaster victims recovering from hurricanes in North Carolina and Florida and wildfires in California are wondering whether FEMA will still be standing after the President made clear he would like to shut down the agency.

Now an unelected millionaire from South Carolina—South Africa, Trump's co-president Elon Musk, has gotten into Federal net-

works and is assessing American's sensitive personal data. God only knows what he's doing with Americans' data or what he plans—his plans are for our information.

He is inside the Treasury Department system where he is not only assessing information but has the ability to change it. These systems have American's Social Security numbers and payment information.

Trump gave Musk control of our Nation's checkbook of a bank account funded by American's hard-earned tax dollars. We don't know what he is doing with any of it.

His DOGE team also allegedly bought a commercial server, set it up in the Office of Personnel Management, and began assessing intimate details about American's personal lives from home addresses to medical histories.

Musk is demanding access to the information systems across the Federal Government to collect even more data about millions of Americans for reasons that are yet unclear. These actions violate a host of Federal laws and policies intended to ensure data privacy and security and protect Federal networks, leading one security expert to describe DOGE access to Federal data as an absolute nightmare.

Nevertheless, neither the White House nor my Republican colleagues in Congress have shown any inclination to force Elon Musk and his DOGE underlings to follow the law, adhere to security practices, or justify their unprecedented access to Government systems and American's data access to Government.

It is not clear who is, in fact, running the country because it seems the President is either unable or unwilling to control Musk. Either way, Americans will be paying the price.

To be honest, Mr. Chairman, it is also not clear why the committee would hold a hearing on cyber work force at this time. Make no mistake. Addressing cyber work force challenges is a critical security priority but holding a hearing on cyber work force while letting Elon Musk root around in Government systems is like worrying someone might break in through the back door of your home while swinging the front door wide open.

I am afraid the committee is failing to address this urgent security issue and our adversaries like China, Russia, and Iran are watching the administration do nothing.

Having said that, I would be remiss if I did not point out that one of the biggest obstacles to growing a robust cyber work force are the Trump-Musk policies.

As I speak, the Federal work force is in a tailspin. All of us are hearing from Federal employees not knowing should they stay or should they go. There is no policies that has been outlined as to why I am receiving this e-mail telling me that I am somehow not useful or valued.

I can understand where CISA and other agencies fall in this tailspin. President Trump's nominee to head the Office of Management and Budget has said, and I quote, "We want the bureaucrats to be traumatically affected. When they wake up in the morning we want them to not want to go to work because they are increasingly viewed as villains. We want to put them in trauma."

Hiring freezes are delaying the onboarding and recruitment of top cyber talent. Secretary Noem, who with little explanation, has said she wants to shrink CISA. Deferred resignations, offers the administration has no authority to issue, accompanied by insults about productivity and warnings of layoffs sent a clear message that the administration does not value its work force. It is not loyal to it and does not prioritize developing expertise within Government. In short, the work force is expendable.

Moreover, the President is openly hostile to a diverse work force that reflects the American people. In just 2 weeks, he has directed Federal departments and agencies to strip references to diversity from their website and blame diversity for a national tragedy.

Mr. Chairman, I appreciate your commitment to addressing the cyber work force challenge by expanding Scholarships for Service for Community College, but under these circumstances who would want to commit to working for the Government?

Until the administration begins to treat its work force with more respect and turn a page on his cruel and dismissive attitude toward diversity, I cannot support new efforts to tie tuition assistance to employment with the Federal Government or to an employer the administration must approve.

Despite what the President might think, cyber jobs are black jobs, Asian jobs, Hispanic jobs, and jobs for women. I wish I were more hopeful that the committee would work to correct course on the Trump-Musk policies that are causing chaos and undermining security.

Toward that end, today I will introduce two resolutions of inquiry to ensure that the committee has the information necessary to evaluate whether Donald Trump and Elon Musk have adequately considered the security implications of their terrible policies.

The first resolution of inquiry directs the Secretary to provide the committee documents related to security assessments associated with efforts to freeze payment of critical homeland security programs that, among other things, support cyber work force training and cybersecurity efforts at the State and local level.

The second resolution of inquiry directs the Secretary to provide the committee documents related to the impact of the hiring freeze on the cyber work force, as well as any of the security policies related to providing DOGE access to DHS information systems and data.

Additionally, today committed Democrats are sending a letter to OPM requesting information about the impact of President Trump's hiring freeze and deferred resignation offers on the cyber work force in a letter to OMB raising our grave concerns about Elon Musk's unfettered access to Federal networks and American's data.

This information is necessary to the committee's oversight obligation and Democrats will not stand by while the Trump-Musk administration rips off the American people.

With that, I again thank the witnesses for participating in today's hearing, and I yield back the balance of my time.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

FEBRUARY 4, 2025

Just over 2 weeks ago, President Trump was sworn into office. Nearly every day since then, there has been a White House directive undermining the Federal Government's ability to serve the American people.

There is confusion about which Federal grant funds President Trump froze last week, and whether the funds are still frozen. The administration refuses to give Americans a straight answer about that. Disaster victims recovering from hurricanes in North Carolina and Florida and wildfires in California are wondering whether FEMA will still be standing after the President has made clear he would like to shut down the agency.

And now, an unelected billionaire from South Africa, Trump's co-president Elon Musk, has gotten into Federal networks and is accessing Americans' sensitive personal data. God only knows what he is doing with Americans' data or what his plans are for our information.

He is inside the Treasury Department's systems where he is not only accessing information but has the ability to change it. These systems have Americans' Social Security numbers and payment information. Trump gave Musk control of our Nation's checkbook, of a bank account funded by Americans' hard-earned tax dollars. We don't know what he's doing with any of it.

His DOGE team also allegedly bought a commercial server, set it up at the Office of Personnel Management, and began accessing intimate details about Americans' personal lives—from home addresses to medical histories. Musk is demanding access to information systems across the Federal Government to collect even more data about millions of Americans for reasons that are unclear.

These actions violate a host of Federal laws and policies intended to ensure data privacy and security and protect Federal networks, leading one security expert to describe DOGE's access to Federal data as "an absolute nightmare."

Nevertheless, neither the White House nor my Republican colleagues in Congress have shown any inclination to force Elon Musk and his DOGE underlings to follow the law, adhere to security practices, or justify their unprecedented access to systems and Americans' data across the Government. It is not clear who is, in fact, running the country. Because it seems the President is either unable or unwilling to control Musk. Either way, Americans will be paying the price.

To be honest, it's also not clear why the committee would hold a hearing on cyber workforce at this time. Make no mistake, addressing cyber workforce challenges is a critical security priority. But holding a hearing on cyber workforce while letting Elon Musk root around in Government systems is like worrying someone might break in through the back door of your home while swinging your front door wide open.

I am afraid the committee is failing to address this urgent security issue, and our adversaries—like China, Russia, and Iran—are watching the administration do nothing. Having said that, I would be remiss if I did not point out that one of the biggest obstacles to growing a robust cyber workforce are the Trump-Musk policies. As I speak, the Federal workforce is in tailspin.

President Trump's nominee to lead the Office of Management and Budget has said: "We want the bureaucrats to be traumatically affected. When they wake up in the morning, we want them to not want to go to work because they are increasingly viewed as the villains . . . We want to put them in trauma."

Hiring freezes are delaying the on-boarding and recruitment of top cyber talent. Secretary Noem, with little explanation, has said she wants to shrink CISA.

Deferred resignation offers the administration has no authority to issue, accompanied by insults about productivity and warnings of layoffs sends a clear message that the administration does not value its workforce, is not loyal to it, and does not prioritize developing expertise within Government. In short, the workforce is expendable.

Moreover, the President is openly hostile to a diverse workforce that reflects the American people. In just 2 weeks, he has directed Federal departments and agencies to strip references to diversity from their websites and blamed diversity for a national tragedy.

Mr. Chairman, I appreciate your commitment to addressing the cyber workforce challenge by expanding scholarships for service for community college, but under these circumstances, who would want to commit to working for the Government?

Until the administration begins to treat its workforce with more respect and turn the page on its cruel and dismissive attitude toward diversity, I cannot support new efforts to tie tuition assistance to employment with the Federal Government or an

employer the administration must approve. Despite what the President might think, cyber jobs are Black jobs—and Asian jobs, and Hispanic jobs, and jobs for women.

I wish I were more hopeful that the committee will work to correct course on the Trump-Musk policies that are causing chaos and undermining security.

Toward that end, today I will introduce two Resolutions of Inquiry to ensure that the committee has the information necessary to evaluate whether Donald Trump and Elon Musk have adequately considered the security implications of their terrible policies.

The first Resolution of Inquiry directs the Secretary to provide the committee documents related to security assessments associated with efforts to freeze payments of critical homeland security programs that, among many other things, support cyber workforce training and cybersecurity efforts at the State and local level.

The second Resolution of Inquiry directs the Secretary to provide the committee documents related to the impact of the hiring freeze on the cyber workforce as well as any of the security policies related to providing DOGE access to DHS information systems and data.

Additionally, today committee Democrats are sending a letter to OPM requesting information about the impact of President Trump's hiring freeze and deferred resignation offers on the cyber workforce and a letter to OMB raising our grave concerns about Elon Musk's unfettered access to Federal networks and Americans' data.

This information is necessary to the committee's oversight obligations, and Democrats will not stand by idly while the Trump-Musk administration rips off the American people.

Chairman GREEN. The gentleman yields.

Other Members of the committee are reminded that opening statements may be submitted for the record.

I am pleased to have a distinguished panel of witnesses before us today, and I ask that our witnesses please rise and raise their right hand. Do you solemnly swear that the testimony you will give before the Committee on Homeland Security of the U.S. House of Representatives will be the truth, the whole truth, and nothing but the truth, so help you God?

Let the record reflect that the witnesses have answered in the affirmative. Thank you. You may be seated.

[Witnesses sworn.]

Chairman GREEN. I would now like to formally introduce our witnesses. Dr. David Russomanno currently serves as the executive vice president for academic affairs and is the provost at the University of Memphis. Prior to his current role, he served for 13 years as dean of the Purdue School of Engineering and Technology and as professor of electrical and computer engineering at the collaborative campus of Indiana University and Purdue University.

Throughout his career Dr. Russomanno has spearheaded the growth of numerous initiatives to improve the recruitment, retention, and overall success of STEM students.

Mr. Robert Rashotte. Mr. Robert Rashotte serves as vice president of global training and technical field enablement at Fortinet where he is responsible for creating award-winning training and education programs for cybersecurity. He also previously served as the director of world-wide education services at that organization.

Before joining Fortinet, he served as the director of Global Training and Enablement at Trend Micro, director of the Canadian Standards Association Learning Institute, and senior manager of training and certification programs at Entrust.

Mr. Chris Jones. Mr. Jones serves as the president and chief executive officer of Middle Tennessee Electric, an electric cooperative where he spent the past 26 years. Mr. Jones also serves as a board

member for United Communications, the Tennessee Electric Cooperative Association, and the Tennessee Chamber.

He previously served as chair of the Chamber of Commerce in both Rutherford and Williamson Counties as an advisory member of the Tennessee Nuclear Energy Advisory Council.

Mr. Max Stier. Mr. Stier serves as president and chief executive officer of the Partnership for Public Service. He previously worked in all 3 branches of government.

Prior to his current role, he served as deputy general counsel for litigation at the Department of Housing and Urban Development. Mr. Stier also previously served as a clerk for the U.S. Supreme Court and U.S. Court of Appeals for the Second Circuit. In addition, he previously worked as special litigation counsel at the Department of Justice and as a staff member in the office of a United States representative.

I thank the witnesses for being here today, and I now recognize Mr. Russomanno for 5 minutes to summarize his opening statement.

STATEMENT OF DAVID J. RUSSOMANNO, PH.D, EXECUTIVE VICE PRESIDENT OF ACADEMIC AFFAIRS AND PROVOST, UNIVERSITY OF MEMPHIS

Mr. RUSSOMANNO. Chairman Green, Ranking Member Thompson, and distinguished Members of the committee thank you for the opportunity to appear before you today. I express my gratitude to Chairman Green for your overall leadership on cybersecurity work force and for introducing the Cyber PIVOTT Act.

My name is David Russomanno. I'm a computer engineer by training and have the privilege of serving as provost at the University of Memphis. The University of Memphis is a Carnegie R1 university, which is a designation meaning we are a high-performing, comprehensive research university.

I have devoted a significant portion of my career as an engineering professor, department chair, and dean of engineering and technology to advance STEM education focused on initiatives to grow the student pipeline and produce successful student outcomes aligned with work force needs.

For example, I have served as principal or co-principal investigator on National Science Foundation-administered scholarships for STEM and CyberCorps Scholarship for Service projects.

Rightly so, prior testimony to this committee has focused on cyber threats to our Nation presented by a variety of threat actors. A parallel threat is the loss of human intellectual capital that could be marshalled toward strengthening our cybersecurity work force.

The Cyber PIVOTT Act is an important contribution toward mitigating these threats by expanding support for students, including those pursuing education and training at 2-year community colleges and technical schools. To my knowledge, these institutions are currently only eligible as sub-awardees of the partnering 4-year CyberCorps institutions.

There are significant challenges to forming comprehensive cybersecurity readiness, including data that shows many colleges are struggling to align education with work force needs. For example, a recent American Society for Engineering Education publication

referenced a *Forbes* article by Perna in which he states, “Historically, institutions of higher learning have been slow to pivot their offerings to meet current work force needs. The inertia is real.”

The article also cites a survey in which 85 percent of recent college graduate respondents state “I wish my college had better prepared me for the workplace.”

In high-demand areas, most notably and critically in cybersecurity, the private sector may prefer to recruit experienced employees from other companies rather than creating entry-level positions and hiring new graduates of post-secondary institutions.

Such an approach alone contributes to an unsustainable race for talent rather than developing highly-collaborative partnerships with educational institutions and the public sector to grow the talent pipeline at scale and in a sustainable manner. A race-for-talent scenario may also have unintended consequence of presenting significant barriers to entry to the cybersecurity profession.

A service commitment proportional to student sponsorship, as incorporated into CyberCorps and the PIVOTT Act, serves as an important model for the private sector. The Federal Government is encouraged to incentivize such a private-sector service commitment, especially given the dependence of the United States, including the U.S. military, on private-sector infrastructure maintained with insufficient levels of cyber resilience, as noted by Rear Admiral Montgomery in his recent testimony to this committee.

When private companies invest in collaborative education programs they help the skills gap, easing the financial burden on taxpayers. Consideration of the Cyber PIVOTT Act also highlights the urgency for 4-year institutions, including comprehensive R1 institutions to develop and align a portion of their STEM baccalaureate degree portfolio to facilitate smooth pathways from applied technology programs.

Per a report from the Education Commission of the States, 31 States have policies for transferring lower division core courses and a State-wide guaranteed transfer of an associate degree.

However, in many instances, these articulations may exclude or not optimally articulate courses, knowledge, and skills acquired through applied technology programs creating a barrier to baccalaureate degree completion, which is a focus of the Polytechnic Initiative at the University of Memphis and is described in my written remarks.

Thank you again for the opportunity to have this conversation today.

[The prepared statement of Dr. Russomanno follows:]

PREPARED STATEMENT OF DAVID J. RUSSOMANNO

FEBRUARY 5, 2025

INTRODUCTION

Chairman Green, Ranking Member Thompson, and distinguished Members of the committee, thank you for the opportunity to appear before you today. I express my gratitude to Chairman Green for your overall leadership on cybersecurity workforce priorities and for introducing the Cyber PIVOTT Act.

My name is David Russomanno. I am an electrical and computer engineer by training and have the honor of serving as executive vice president for academic affairs and provost at the University of Memphis. The University of Memphis is a Carnegie R1 university, which is a prestigious designation meaning we are a high-

performing, comprehensive research institution. Before becoming an academic more than 30 years ago, I worked as an engineer for corporations in the defense, automotive, and computer sectors.

I have conducted fundamental research with support from various sponsors, including the National Science Foundation (NSF), Army Research Laboratory (ARL), State and local governments, and the private sector to advance the state-of-the-art in some areas and apply the state-of-the-art in other areas. Most importantly, I have devoted a significant portion of my career as an engineering professor, department chair, and dean of engineering and technology, before assuming my role as provost, to advance Science, Technology, Engineering, and Mathematics (STEM) education focused on initiatives to grow the student pipeline and produce successful student outcomes aligned with workforce needs. For example, I have served as principal investigator or co-principal investigator on NSF-administered Scholarships for STEM (S-STEM)¹ and CyberCorps Scholarship for Service (SFS) Defending America's Cyberspace² projects.

Per the U.S. Department of Commerce, about 500,000 cybersecurity positions are open. Those vacancies place our Nation's digital infrastructure, intellectual property, and privacy at significant risk from threat actors who are looking to exploit our vulnerabilities.

The Cyber PIVOTT Act is an important contribution toward addressing this deficiency.

In addition, we at the University of Memphis are implementing an additional and needed contribution so that 4-year universities are doing even more by strengthening pathways from applied technology programs, including applied cybersecurity, to appropriate baccalaureate programs.

BACKGROUND

Rightly so, prior testimony to this and other Congressional committees has focused on various cyber threats to the United States presented by a variety of threat actors, including nation-states, criminal organizations, and individuals. A parallel threat, which has been noted in prior hearings, is the loss of human intellectual capital that could be marshalled toward strengthening our cybersecurity infrastructure. I am pleased that this 119th Congress is considering steps to address this threat through the Cyber PIVOTT Act, which will expand support for education and training programs at community colleges and technical schools. These institutions, to the best of my knowledge, are eligible only as sub-awardees of the partnering 4-year CyberCorps (SFS) institutions. Therefore, the Cyber PIVOTT Act will broaden and strengthen the workforce and contribute toward forming a panoply of cybersecurity readiness at scale desperately needed by our Nation.

CHALLENGES

There are significant challenges to forming that comprehensive cybersecurity readiness to which I just referred, with many opportunities for post-secondary education, as well as the public and private sector to work collaboratively to address the challenges.

Higher Education

As summarized last week in the American Society for Engineering Education's (ASEE) First Bell publication,³ data shows that many colleges are struggling to align education with workforce needs. As referenced by ASEE First Bell and described in Forbes by Perna:⁴ "Historically, institutions of higher learning have been slow to pivot their offerings to meet current workforce needs. The inertia is real. The problem is, Gen Z is smart enough to know it." I add that with respect to our cybersecurity readiness, adversaries are smart enough to know it too.

Although the focus of the Perna article is Artificial Intelligence (AI), many of the highlighted issues are relevant to the applied cybersecurity workforce. For example, Perna cites a survey conducted by Hult International Business School in which 85

¹NSF Scholarships in Science, Technology, Engineering, and Mathematics Program (S-STEM): <https://new.nsf.gov/funding/opportunities/s-stem-nsf-scholarships-science-technology-engineering-mathematics> (link active as of February 1, 2025).

²NSF CyberCorps Scholarship for Service (SFS): <https://new.nsf.gov/funding/opportunities/sfs-cybercorps-scholarship-service> (link active as of February 1, 2025).

³ASEE First Bell: <https://www.asee.org/publications/NEWSLETTERS/First-Bell> (link active as of February 1, 2025).

⁴M.C. Perna, "New Data Reveals Just How Deep The College Crisis Goes," *Forbes*, January 28, 2025: <https://www.forbes.com/sites/markperna/2025/01/28/new-data-reveals-the-depth-of-college-crisis/> (link active as of February 1, 2025).

percent of recent college graduates who participated in the survey agreed with the statement:⁴ “I wish my college had better prepared me for the workplace.” The Perna article goes on to state:⁴ “The call here is simply for the higher education system to better align with what today’s students and employers need—before it’s too late.”

The Perna article could understandably be interpreted as the higher education system is solely responsible for preparing its graduates to meet workforce needs. However, in high-demand areas, most notably and critically in cybersecurity, the private sector may prefer to recruit experienced employees from other companies rather than creating entry-level positions and hiring new graduates. Such an approach contributes toward an unsustainable “race for talent” rather than developing deep and sustained partnerships with educational institutions and the public sector to grow the talent pipeline at scale and in a sustainable manner. Such a “race for talent” scenario may also have the unintended consequence of presenting significant barriers to entry to the profession for new graduates who may have interest but limited experience in cybersecurity.

Examples of sustained private sector and higher education best practices include “invested” program advisory boards that provide input to academic programs to guide their educational objectives, curriculum, and student learning outcomes. The advisory input is then supplemented with ample opportunities for students to augment their program of study with compensated and meaningful experiential learning opportunities, including internships sponsored by advisory board members, to become better-prepared applicants upon graduation.

A service commitment proportionate to student sponsorship as incorporated into CyberCorps (SFS) and the Cyber PIVOTT Act should serve as an important model for the private sector to strengthen its commitment toward contributing to a sustainable cybersecurity workforce at scale. Opportunities for incentivizing such a private-sector commitment at the Federal and State levels are encouraged, especially given the dependencies of the United States, including the U.S. military, on private-sector infrastructure maintained with insufficient levels of cyber resilience as noted by Rear Admiral (Ret.) Montgomery in his recent testimony to this committee.⁵

By focusing on retaining cybersecurity professionals, the Federal Government can avoid the high costs of continually recruiting and training new employees. Cybersecurity experts in critical infrastructure roles are costly to train, and turnover disrupts operations while forcing taxpayers to bear the expense of new hiring and training processes.

Additionally, when private companies invest in collaborative training programs, they help bridge the skills gap, easing the financial burden on the Federal Government by sharing the responsibility for workforce development.

Traditional Pathways to and Barriers Preventing Joining the Cybersecurity Workforce

Although many comprehensive universities across the United States offer a 4-year program of study in cybersecurity and closely-related fields, there are often barriers for student entry into such programs. For example, rigorous computer science and engineering programs, which incorporate cybersecurity education into their curricula, require extensive mathematics and basic sciences preparation, such as including Calculus in the first year of a 4-year program of study. These programs are based on foundational knowledge acquired through courses with substantial prerequisite chains. First-principle-based programs are critically important to our Nation to prepare students to advance the state-of-the-art in a variety of fields. However, these types of programs may not always be the most appropriate educational pathway for students interested in applying the state-of-the-art versus acquiring foundational knowledge at the baccalaureate level, which may be required for graduate programs in computer science and engineering focused on research to advance the state-of-the-art.

Moreover, the time required to earn a 4-year degree, particularly for students who may be working during their program of study, may also present a hurdle that is too high.

Therefore, the opportunity to earn cybersecurity credentials through community colleges and technical schools will present an attractive option to both traditional students and those who may be considering career change. The Cyber PIVOTT Act

⁵RADM (Ret.) Montgomery, “Unconstrained Actors: Accessing Global Cyber Threats to the Homeland,” A House Committee on Homeland Security hearing, January 22, 2025, <https://homeland.house.gov/wp-content/uploads/2025/01/2025-01-22-FC-HRG-Testimony.pdf> (link active as of February 1, 2025)

is appropriately focused on community colleges and technical schools as a component for increasing the cybersecurity workforce at scale.

Given the appropriate focus of the Cyber PIVOTT Act on community colleges and technical schools, it is important for 4-year institutions, including comprehensive R1 institutions, to strengthen pathways from applied technology programs, including applied cybersecurity, to appropriate baccalaureate programs.

A vitally important aspect of the Cyber PIVOTT Act is the DELAYED SERVICE clause in which students who immediately after completion of their community college or technical school program enroll in a 4-year program may delay their service obligation until after receiving the 4-year degree. This clause will be an attractive incentive for many students as they are considering career goals. I encourage that both the public and private sectors be incentivized in some appropriate manner to consider continued support of Cyber PIVOTT Act recipients to pursue a 4-year degree at a later stage of their career if students do not pursue a 4-year degree immediately after completing their community college or technical school program.

By partnering with universities, community colleges, and technical schools, the Federal Government can create tailored cybersecurity programs that build upon students' prior learning experiences such as military service and technical certifications. This collaborative approach allows the Government to leverage existing skills and expertise without having to start from scratch, ultimately maximizing the return on its investment in workforce development.

Although significant progress has been made in many States with articulation agreements from community colleges to 4-year universities, especially for general education courses, arguably the same progress has not been made with respect to articulation agreements with programs offered by technology schools.

Per a report by the Education Commission of the States, at least 31 States have policies requiring a transferable core of lower-division courses and State-wide guaranteed transfer of an associate degree.⁶ However, my experience is that these articulations primarily focus on a general education core, which is a component of most associate of science (AS) and associate of arts (AA) degrees or very similar programs, and may exclude or not optimally articulate courses, knowledge, and skills acquired through associate of applied science (AAS) programs creating a barrier to baccalaureate degree completion. For example, within the State of Tennessee, there are limited articulation agreements between programs offered by Tennessee Colleges of Applied Technology (referred to as TCATs) to baccalaureate programs offered by 4-year universities.

However, progress is being made, especially with articulations from AAS to Bachelor of Applied Science (BAS) programs. The University of Memphis (UofM) is striving to be a national leader to accelerate the AAS-to-BAS transfer pathway through The Polytechnic @ UofM initiative.

SUPPORTING WORKFORCE GROWTH AT SCALE

The Polytechnic Model

A polytechnic⁷ may be regarded as an educational institution or unit within an institution that primarily focuses on applied sciences, applied technology, and career pathways.

Although polytechnic has several definitions and a variety of implementations, some recurring themes are as follows:

- Offer real-world experiences and industry partnerships
- Provide hands-on training with emphasis on practice and applying the state-of-the-art versus advancing it
- Serve as a complement to first-principle-based curricula (e.g., traditional computer science and engineering programs) in which the fundamental concepts or assumptions on which a theory, system, or method is based⁸ are foundational to progression in the curriculum.

To attain their ideal definition, polytechnic programs must align with workforce needs and demonstrate the ability to pivot to meet rapidly changing knowledge and skillset demands by the workforce (arguably requiring a more rapid feedback loop with respect to assessing student and workforce needs for continuous improvement than programs that have strong foundations in first principles).

⁶Education Commission of the States: "50-State Comparison: Transfer and Articulation Policies—Education Commission of the States," <https://www.ecs.org/50-State-comparison-transfer-and-articulation/> (link active as of February 1, 2025).

⁷"Polytechnic," Merriam-Webster.com Dictionary, Merriam-Webster, <https://www.merriam-webster.com/dictionary/polytechnic> (link active as of February 1, 2025).

⁸"First Principles," Oxford Learner's Dictionary, https://www.oxfordlearnersdictionaries.com/us/definition/american_english/first-principles (link active as of February 1, 2025).

While dean of the Purdue School of Engineering and Technology at Indiana University—Purdue University Indianapolis (now part of Purdue in Indianapolis), I enthusiastically supported the development of an application-oriented Bachelor of Science degree in Cybersecurity and a Master of Science degree in Cybersecurity and Trusted Systems.

Distinguishing features of these programs included: (i) minimization of extensive course prerequisite chains; (ii) team-based and project-based courses and labs; (iii) “invested” advisory boards as previously mentioned; (iv) significant student participation in experiential learning opportunities, including paid internships; and (v) flexibility in accommodating transfer from 2-year institutions for the BS program and accommodating a variety of undergraduate BS degrees in preparation for admission to the MS program. Moreover, both the BS and MS programs incorporated student participation in NSF CyberCorps (SFS), which served as a model to enhance partnerships with the programs’ advisory board and other entities from the private sector.

Now as Provost at the University of Memphis, with strong support from the President of the University and our Board of Trustees, we are launching The Polytechnic @ UofM as an important component of the UofM’s Ascend strategic plan⁹ to better prepare our students for workforce needs with emphasis on a successful outcome for every student.

The Polytechnic @ UofM will serve as the organizational sub-unit within our Herff College of Engineering to host several existing applied technology programs, as well as to launch new applied technology programs to rapidly respond to workforce needs.

Implementation includes a Bachelor of Applied Science (with concentrations such as Applied Cybersecurity, Applied AI, and Advanced Manufacturing Supervision) to expand support for student matriculation pathways from the following: (i) Tennessee Colleges of Applied Technology; (ii) Community Colleges with associate of applied science programs; (iii) private-sector training and certification programs; (iv) credit for prior learning, including experience gained through military service; and (v) other applied technology and vocational institutions across the United States, all of which are well-positioned to benefit from the Cyber PIVOTT Act and to contribute to building a cybersecurity workforce at scale.

CONCLUSION

I am honored to testify today in strong support of the Cyber PIVOTT Act under consideration by the 119th Congress as it will broaden and strengthen the workforce toward forming the panoply of cybersecurity readiness at scale desperately needed by our Nation. Moreover, consideration of the Cyber PIVOTT Act highlights the urgency for 4-year institutions to develop and align a portion of their STEM academic portfolio to provide a seamless pathway to baccalaureate programs for students pursuing applied technology programs, including applied cybersecurity, from community colleges and technical schools.

The Polytechnic @ UofM is an important new initiative leveraging partnerships within the State of Tennessee and beyond to contribute toward a national model for addressing workforce needs in applied technology areas and as an important complement to first-principle-based baccalaureate and graduate programs in computer science, engineering, and closely related fields of study.

Chairman GREEN. Thank you, Dr. Russomanno.

I now recognize Mr. Rashotte, and am I pronouncing your name correctly—

Mr. RASHOTTE. Yes.

Chairman GREEN [continuing]. Perfect—for 5 minutes to summarize his opening statement.

STATEMENT OF ROBERT RASHOTTE, VICE PRESIDENT, GLOBAL TRAINING AND TECHNICAL FIELD ENABLEMENT, FORTINET

Mr. RASHOTTE. Chairman Green, Ranking Member Thompson, and distinguished Members of the committee, my name is Rob

⁹Office of the President of the University of Memphis, Ascend strategic plan 2023–2028, <https://www.memphis.edu/president/strategic-plan/index.php> (link active as of February 1, 2025).

Rashotte and I serve as vice president of Fortinet's training institute. I've spent my career focusing on empowering others with the skills to successfully enter and advance within the cybersecurity work force. I appreciate the opportunity to testify before you today on the state of America's cyber work force.

Fortinet is a U.S. company that is one of the largest cybersecurity companies in the world. While we manufacture over half of the firewalls sold world-wide, our portfolio extends across nearly 60 different integrated cybersecurity and networking solutions. This reflects our commitment to innovation as cyber threats continue to evolve.

In addition, Fortinet operates an award-winning training institute focusing on making training, cybersecurity training, available to everyone. We believe teamwork across the public and private sector is critical to ensure strong national cyber resilience.

A robust and skilled work force is foundational to this resilience, making today's discussion both about jobs and our national security.

The demand for cybersecurity professionals continues to outpace supply with over 500,000 unfilled positions in the United States. We annually conduct a skills gap survey surveying IT and cybersecurity decision makers with our findings compiled into an annual cybersecurity skills gap report.

Our latest research found that 75 percent of U.S. organizations believe that the work force gap is escalating cyber threats and nearly 90 percent have experienced a breach they attribute in part to lack of cyber skills. While companies are working to recruit and retain talent, more than half struggle to find qualified professionals.

The cybersecurity work force gap has been exacerbated by several interconnected challenges, the most significant challenge being the persistent reliance on traditional 4-year degrees as a primary requirement for most roles. We've observed a growing number of technical schools, colleges, and universities launching 2-year degree programs that effectively prepare students for a range of cybersecurity roles.

Waiting until high school or college, however, to influence career decisions is often too late. Just as kids talk to their parents about becoming doctors or firefighters, we need to ensure that cyber threat hunter, for example, becomes part of that conversation.

To help create that spark, Fortinet has developed cybersecurity awareness training for K to 12 schools nationwide and has made it available at no cost. The curricula introduces cybersecurity concepts as early as kindergarten. Today, the program operates in 43 States by engaging students, teachers, and parents who are sparking interest in cybersecurity careers early.

We must also do more to attract existing underutilized talent pools. A key example is military veterans moving into civilian roles. Many veterans possess highly relevant skills that are invaluable to cybersecurity.

Our veteran partner organizations, though, often note that their members lack awareness or the confidence in how their military experience translates into cybersecurity careers. We must unlock this wealth of talent that is both capable and well-suited for the field.

We must also focus on reskilling and upskilling. Cyber professionals often face high stress and burnout and many organizations lack clear career progression paths. Strengthening training, mentorship, and career mobility will help grow a sustainable work force.

Industry, academia, and Government are making progress but we must scale our efforts. If enforced, the proposed Cyber PIVOTT Act would have a positive impact across both the public and private sector with its emphasis on cybersecurity scholarships for students in partnership with technical schools, colleges, and universities, as well as developing internships and Federal job opportunities for graduates.

In conclusion, I'm confident that with the right tools, incentives, and partnerships we can ensure the cyber work force pipeline is strengthened and that today's work force gap becomes yesterday's issue. To achieve this we need bold, consistent action that can scale, ranging from early training of our children on cyber awareness through to technical career training and efforts like the PIVOTT Act.

Thank you for the opportunity to be part of today's discussion and I look forward to your questions.

[The prepared statement of Mr. Rashotte follows:]

PREPARED STATEMENT OF ROBERT RASHOTTE

FEBRUARY 5, 2025

Chairman Green, Ranking Member Thompson, and distinguished Members of the committee, I appreciate the opportunity to testify before you today on "the state of America's cyber workforce". My name is Rob Rashotte and I serve as vice president of the Training Institute at Fortinet.

Fortinet¹ is a U.S. company that is one of the largest cybersecurity companies in the world. While we manufacture over half of the firewalls sold world-wide, our portfolio extends across nearly 60 different integrated cybersecurity and networking solutions and services, reflecting our commitment to innovation as information technology (IT) and cyber threats continue to evolve. In addition to our products and services, Fortinet operates a robust cybersecurity training institute² focused on helping to address the significant global cyber workforce and skill gaps and preparing the next generation of cybersecurity professionals. Our ultimate goal is to enable a more digitally secure society.

We believe teamwork is key to best defend against cyber threats. To that end, Fortinet is part of numerous collaborative activities between industry and the U.S. Government, ranging from participation in the IT sector's coordinating council to collaboration on technology development through NIST's National Cybersecurity Excellence Partnership³ and coordinated cyber threat analysis and response via the Joint Cyber Defense Collaborative⁴ (JCDC) run by the Cybersecurity and Infrastructure Security Agency (CISA). Reflecting the fact that cyber crime does not stop at country borders, Fortinet also participates in global initiatives such as the World Economic Forum Centre for Cybersecurity⁵ and the Cyber Threat Alliance.⁶

Our commitment to collaboration is also reflected in our training initiatives, where we've established meaningful partnerships with leading tech-focused non-profits across the globe to expand the talent pool and awareness of jobs in the field. We established a Veterans Program Advisory Council, comprised of veteran non-profit representation from across the Five Eyes, given the strong correlation between skills gained by veterans during their time in service to the needs of the

¹<https://www.fortinet.com/corporate/about-us/about-us>.

²<https://training.fortinet.com>.

³<https://www.nccoe.nist.gov/news-insights/ncep-mechanism-partnering-nccoe>.

⁴<https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative>.

⁵<https://centres.weforum.org/centre-for-cybersecurity>.

⁶<https://www.cyberthreatalliance.org/>.

cyber workforce. This council helps us gain deeper insights into the needs of the veteran community and enables us to continually evolve our programs to better serve them. These collaborations are essential to broadening our impact and ensuring we attract enough talent to close the industry gap. The individuals we support will enter the cyber field across a variety of industries, like the energy or education sectors, working to safeguard corporate networks and critical infrastructures—ultimately ensuring a more secure and resilient Nation. Our training could be utilized by all organizations represented here today. No one is immune and cybersecurity is all our responsibility.

STATE OF THE CYBER WORKFORCE

As the cybersecurity landscape becomes increasingly complex, the demand for skilled professionals continues to grow with more than 500,000 cybersecurity professionals required to address the workforce gap within the United States.⁷ As part of our training initiatives, we place a strong emphasis on direct engagement with key stakeholders. Each year, we conduct a skills gap report, surveying 1,850 IT and cybersecurity decision makers across 29 countries, with the United States contributing a significant 300 respondents. The findings are compiled into our annual Cybersecurity Skills Gap Global Research Report, now in its fourth year of publication. Our latest 2024 report revealed that 70 percent of global organizations believe the shortage of skilled cybersecurity professionals is escalating security risks. That statistic rises to 75 percent for U.S. respondents.⁸

In the past year, nearly 90 percent of organizational leaders said their enterprise experienced a breach that they can partially attribute to a lack of cyber skills. Despite many organizations adopting creative strategies to recruit, hire, and retain qualified cybersecurity professionals to fill positions, 51 percent of leaders say the talent pools for their needed skill sets are generally lean. These on-going recruitment challenges represent a significant and dangerous supply problem for the industry, with 54 percent of enterprises noting that they continue to struggle to recruit cybersecurity talent.

While there are numerous hurdles associated with recruitment and hiring, leaders also noted that the retention of skilled cybersecurity practitioners is also a challenge. Half of respondents said that offering employees sufficient training and upskilling opportunities was the biggest hurdle to keeping qualified practitioners on staff.

BARRIERS TO ENTRY

The cybersecurity workforce gap has been exacerbated by several interconnected challenges ranging from lack of standardization and awareness of cybersecurity roles to competition for skilled professionals in adjacent fields. Among the most significant challenges, however, are the barriers to entry for both newcomers to the field and existing professionals seeking career advancement. Based on our research and insights from numerous partnerships, the most pressing and wide-spread issue in this regard is access to education and training. While financial constraints are often a factor for those looking to start a career in the field, a major obstacle remains the persistent reliance of companies and Government agencies on traditional 4-year degrees as a primary requirement for cybersecurity roles. This outdated requirement should no longer serve as a default filtering mechanism in the hiring process.

Through our collaborations with hundreds of academic institutions, we have observed a growing number of technical schools, colleges, and universities launching 2-year degree programs that effectively prepare students for a range of cybersecurity roles. Additionally, many industry stakeholders have made significant strides in providing high-quality cybersecurity industry training at little or no cost to aspiring professionals. Since the beginning of 2020, Fortinet has been offering its entire catalog of self-paced cybersecurity certification training free of charge to all individuals looking to enter the field or advance their careers. Other organizations, both within and beyond the cybersecurity sector, have taken similar steps to expand access to industry-recognized training.

While not a substitute for formal academic education, industry training and certification play a crucial role in equipping new entrants with the practical knowledge and hands-on skills-based experience that isn't always available through traditional

⁷ <https://homeland.house.gov/2024/09/24/chairman-green-introduces-cyber-pivott-act-to-tackle-government-cyber-workforce-shortage-create-pathways-for-10000-new-professionals/>.

⁸ <https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf>.

degree programs. Our top level of certified professionals, who have earned the title of Fortinet Certified Experts (FCX), tell us repeatedly that their expertise was mostly obtained through hands-on experience. To address the cybersecurity workforce gap effectively, we all need to remove as many barriers to education as possible, while hiring organizations must recognize and embrace alternative pathways to competency and expertise.

THE NEEDED “SPARK”: AWARENESS OF CYBERSECURITY AS A CAREER

Cybersecurity has evolved from an obscure technical concept to become part of our household vocabulary, often happening for all the wrong reasons. However, we must seize this newfound visibility and use it as an opportunity to inspire young students to pursue careers in cybersecurity. Just as children come home from school and talk to their parents about becoming a doctor, firefighter, or police officer, we must challenge ourselves to make “Cyber Threat Hunter” a part of that conversation. In many instances, waiting until high school or college to influence career decisions is too late.

This goal is not only achievable but already yielding results. We have seen first-hand the impact of early engagement through our extensive work with K–12 schools across the United States. In 2022 Fortinet participated in the White House’s National Cyber Workforce and Education Summit. This initiative brought together Government and private industry leaders to discuss how we could collectively address the pressing issue of workforce development in cybersecurity. We were grateful for this opportunity to participate, as it challenged us to rethink the approach and responsibility of the Fortinet Training Institute.

In response, our experienced team of cybersecurity curriculum content developers began adapting our enterprise security awareness and training service for the education sector with a focus on equipping K–12 staff and faculty with the knowledge to become more cyber aware. We offered this training at no cost to school districts and private schools across the United States, and the feedback was overwhelmingly positive.

To demonstrate the selfless nature of the educators in this country, many asked if we could also develop a curriculum to teach cybersecurity directly to K–12 students. Recognizing the urgent need for this type of education, we once again were tasked with evolving our role and responsibility at the Fortinet Training Institute. We immediately hired a dedicated team of K–12 curriculum developers—former educators—who now focus exclusively on creating age-appropriate cybersecurity content for students, teachers, and parents while leveraging the expertise of the cybersecurity professionals in our organization.

Our programs now introduce cybersecurity concepts as early as kindergarten and evolve into more career-oriented content as students progress through later grades. To date, this program is active in 43 States, and has issued more than 700,000 licenses to our content. Taking a holistic approach—engaging students, teachers, parents, and staff—is critical to fostering a cybersecurity-aware culture and sparking interest in cyber careers at an early age.

We are seeing many States across the United States take a leadership role in this as well. States, such as Nevada, Nebraska, North Carolina, Rhode Island, South Carolina and Tennessee, are bringing cyber education to younger students by requiring a credit in computer science to be eligible for high school graduation. Tennessee has taken it a step further by including a credit in cybersecurity as an alternative to the requirement. We believe these efforts are highly appropriate and necessary to expand awareness, and hope additional States take similar action.

Beyond inspiring the next generation, we must also do more to attract existing underutilized talent pools, particularly individuals transitioning into new careers. A key example is military veterans moving into civilian roles. Many veterans possess highly relevant skills—including situational awareness, leading in a crisis, and the ability to perform under pressure—that are invaluable in cybersecurity. While technical skills can be taught, these innate attributes are critical in many cyber roles. However, our partner organizations that support veterans, such as VetSec Inc. and Hire Heroes USA, frequently report that their members lack awareness or confidence in how their military experience translates into cybersecurity careers. Addressing this gap is essential to unlocking a wealth of talent that is both capable and well-suited for the field.

LACK OF CLARITY ON CAREER PATHS AND ROLES

While some traditional cybersecurity roles—primarily technical roles—are relatively well-defined, the field has evolved to encompass a vast and increasingly complex range of roles and required skill sets. This rapid evolution has led to significant

ambiguity, making it challenging for individuals seeking education and training to navigate their path into a cybersecurity career.

Organizations such as NIST and the National Initiative for Cybersecurity Education (NICE) have made great strides in developing cybersecurity career pathways. As cybersecurity roles evolve at a rapid pace, these efforts must continue and evolve to ensure these frameworks remain current and, more importantly, that they serve as a benchmark for standardizing cybersecurity roles across Government and industry.

Clearly-defined career pathways are not only essential for individuals entering the field but also for current professionals looking to advance. Establishing standardized career pathways is crucial in efficiently upskilling the existing workforce and creating a pipeline of experienced professionals for senior and leadership roles as part of long-term succession planning. By creating greater clarity and consistency in cybersecurity career paths, we can better equip both new entrants and seasoned professionals to meet the growing demands of the industry. At Fortinet, we have seen increasing interest over the last few years in courses in security operations (SecOps) and cloud-based security architecture. In response, we updated our entire certification program in 2023 to meet the needs of the rapidly-evolving threat landscape and job market needs.

RECRUITMENT AND RETENTION

Recruiting and retaining cybersecurity professionals remain significant challenges in addressing the cyber workforce shortage. Unlike well-established fields such as accounting—where hiring for a CPA, for example, follows a clear and standardized process—cybersecurity is still a relatively young profession with roles and responsibilities that are constantly changing. This on-going evolution makes the recruitment process uniquely difficult.

Many recruiters struggle to develop accurate job descriptions or identify the appropriate skills needed for cybersecurity roles. As a result, they often rely on arbitrary requirements, such as mandating a traditional 4-year degree, which unnecessarily excludes a large pool of highly-qualified candidates. This underscores the critical importance of efforts by organizations like NIST and the NICE⁹ initiative, which is making significant strides in standardizing cybersecurity roles and career pathways. Establishing clearer role definitions and hiring frameworks will be essential in improving both recruitment and retention across the industry.

Retention efforts are just as critical as recruitment in addressing the cybersecurity workforce gap. Attracting new talent is only part of the solution—organizations must also focus on keeping skilled professionals engaged, motivated, and growing within their careers. High turnover rates not only exacerbate the workforce gap but also lead to knowledge loss, increased training costs, and disruptions in cybersecurity operations, all of which can weaken an organization's security posture.

Moreover, cybersecurity professionals often face high levels of stress, burnout, and job dissatisfaction due to long hours, intense workloads, and the ever-evolving threat landscape. Without clear career pathways, opportunities for advancement, and continuous upskilling, many professionals may leave for better-defined roles in other industries.

Investing in retention strategies, such as competitive compensation and professional development, ensures that organizations maintain a strong, experienced cybersecurity workforce.

Ultimately, addressing retention challenges is key to building a sustainable and resilient cybersecurity talent pipeline.

ON-GOING PROGRESS TO ADDRESS THE CYBER WORKFORCE GAP

While there is work to be done to develop the future cybersecurity workforce, it's encouraging that there are significant efforts already under way across industry, academia, and Government to address this challenge. Many industry-leading organizations are working to meet the challenge head on. Fortinet, for example, has committed to training 1 million people over a 5-year period (2021–2026) through our Fortinet Training Institute. We are slightly ahead of our goal with more than 630,000 trained as of Dec. 31, 2024.¹⁰ By providing free, self-paced cybersecurity training and working with academic institutions, non-profits, global organizations

⁹ <https://www.nist.gov/itl/applied-cybersecurity/nice/about>.

¹⁰ <https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2024/fortinet-announces-progress-towards-mission-to-tackle-cybersecurity-skills-shortage>.

and Government agencies, Fortinet is helping to equip individuals with the skills needed to enter and advance in the field.

Additionally, through our many academic partnerships, Fortinet has seen several innovative post-secondary institutions recognize the importance of alternative education pathways. Some of our academic partners, such as Northeast State Community College in Tennessee, Sinclair Community College in Ohio, and Mohave Community College in Arizona have introduced 2-year cybersecurity degree programs that provide students with skills-based, relevant knowledge and hands-on training and industry certifications. These programs are effectively preparing students for entry-level cybersecurity roles. Effective degree programs, along with Government-backed workforce initiatives, apprenticeship programs, and veteran transition efforts, are making cybersecurity careers more accessible to a broader talent pool. While these initiatives represent meaningful progress, continued investment and collaboration will be essential to closing the cybersecurity workforce gap at scale.

WHAT MORE CAN BE DONE?

Despite on-going efforts to close the cybersecurity workforce gap, more comprehensive solutions are needed to address systemic challenges. First, organizations and policy makers must expand and embrace alternative pathways into cybersecurity roles beyond traditional 4-year degrees. Increased investment in shorter degree programs, vocational training, industry-recognized certifications, and apprenticeship programs can help individuals enter the field quickly and transition from adjacent fields into cybersecurity. Additionally, upskilling and reskilling of existing employees must be prioritized. This is necessary in order to provide clear career progression opportunities to retain critical talent and ensure robust succession planning.

Stronger partnerships between industry, academia, and Government agencies can also enhance workforce development. Businesses should collaborate with educational institutions to ensure curricula align with real-world cybersecurity needs. Governments should continue to provide incentives for companies and academic institutions that invest in cybersecurity training, education, and workforce development. These public-private partnerships can help to ensure portability of experienced cybersecurity professionals between Government and private-sector roles and help to bridge the workforce gap at scale.

The work of this committee is also key to expanding awareness of cyber roles in the workforce and closing the cyber workforce gap. If enacted, the proposed Cyber PIVOTT Act would have a positive impact across both the public and private sector with its emphasis on cybersecurity scholarships for students in partnership with community colleges and technical schools, as well as developing internships and Federal job opportunities for graduates of this program.

Finally, the cybersecurity profession must improve awareness and branding. Many potential candidates are unaware of the range of cybersecurity careers available. Public awareness campaigns, starting at the high-school level, can help attract more individuals to the field, ensuring a sustainable and resilient workforce for the future.

CONCLUSION

Our digital ecosystem is constantly under attack by hackers, cyber criminals and nation-state actors. Teamwork across the public and private sector is crucial to ensure strong national cyber resilience. A robust and skilled workforce is foundational to this resilience—making today's discussion both about jobs and our national security.

I have spent my career focusing on empowering others with the skills to successfully enter or advance within the cybersecurity workforce. I am confident that with the right tools, incentives, and partnerships we can ensure the cyber workforce pipeline is strengthened and that today's skills gap becomes yesterday's issue. To achieve this, we need bold and consistent action that can scale—ranging from early training of our children on cyber awareness through to technical training on secure coding practices. Efforts like the Cyber PIVOTT Act are critical examples of how private and public-sector collaboration can ensure this workforce pipeline is strengthened.

Thank you for the opportunity to be part of this hearing and I stand ready to assist the committee on this important topic. I look forward to today's discussion and I welcome your questions.

Chairman GREEN. Thank you, Mr. Rashotte.

I now recognize Mr. Jones for 5 minutes to summarize his opening statement.

STATEMENT OF CHRIS JONES, PRESIDENT AND CHIEF EXECUTIVE OFFICER, MIDDLE TENNESSEE ELECTRIC MEMBERSHIP CORPORATION

Mr. JONES. Chairman Green, Ranking Member Thompson, and distinguished Members of this committee, thank you for the opportunity to testify before you today. My name is Chris Jones and I serve as president and CEO of Middle Tennessee electric.

I am testifying to provide my perspective as an electric co-op leader but also to represent the National Rural Electric Cooperative Association and the 900 electric cooperatives across the country. In all these respects, it is quite an honor to be before you today.

MTE is the largest electric cooperative in the TVA region and the second-largest in the United States, serving more than 750,000 Tennesseans. Our service territory includes 15,000 miles of distribution lines across 11 Middle Tennessee counties.

NRECA is the national trade association representing 900 electric cooperatives. Electric co-ops are not-for-profit electric providers and are focused on delivering affordable, reliable, and secure electricity to more than 42 million Americans in 48 States. We are unique in the electric sector in that we operate without profit incentives and are owned and governed by the very people we serve.

Electric co-ops were created with the mission to address the distinct challenges associated with providing electric service to rural communities, which typically have lower population densities, are more residential, and less affluent than the industry average. This means cooperatives are constantly asked to do more with less and they deliver.

Electric co-ops are owners and operators of some of the Nation's most critical infrastructure, including providing power to more than 150 military facilities and installations in the United States. We also serve as economic drivers and life lines for critical industries and services in our communities like hospitals, schools, emergency services, energy, and food and agricultural production.

Protecting America's electric grid from cyber and physical threats is a top priority for our electric co-ops and the communities they serve. Accomplishing this important task as at-cost entities presents its own set of challenges.

The same circumstances that made it difficult to invest in electrifying rural America nearly 100 years ago, including being isolated from larger customer bases and diverse talent pools available in urban areas, persist in some places today.

I address these issues in more detail in my written testimony, but electric cooperatives struggle for cyber professionals against more competitive salaries and benefits offered by larger urban-based firms. It is also often difficult to attract skilled talent to rural areas because of a perceived lack of professional development or career progression opportunities.

However, electric co-ops are identifying innovative ways to overcome these obstacles through partnerships and smart investments.

I would be remiss if I did not take this opportunity to thank Chairman Green for his leadership with the Cyber PIVOTT Act to help tackle some of these issues. Electric cooperatives were pleased with the inclusion of language that would extend cybersecurity in-

ternship opportunities to critical infrastructure in rural communities.

Creating a talent pipeline that includes pathways into rural areas will foster a local, skilled cybersecurity work force to safeguard critical infrastructure in these regions.

We have a saying that if you have met one electric co-op then you have met exactly one electric co-op. We come in all different shapes and sizes. But many of our challenges share similar themes.

MTE is fortunate to not have to wrestle with some of the more intense challenges of the rural cybersecurity work force issue. However, with my 26 years working for the cooperative I have seen the lengths MTE has had to go to tackle those issues and can share many challenges that are impacting other co-ops across the broader community.

Thank you for this opportunity. I hope to be helpful, and I look forward to responding to any questions.

[The prepared statement of Mr. Jones follows:]

PREPARED STATEMENT OF CHRIS JONES

WEDNESDAY, FEBRUARY 5, 2025

INTRODUCTION

Chairman Green, Ranking Member Thompson, and Members of this committee: Thank you for the opportunity to testify before you today. My name is Chris Jones, and I serve as president and CEO of Middle Tennessee Electric (MTE). I am testifying today to provide my own insights as a co-op leader, but also representing the National Rural Electric Cooperative Association (NRECA) and nearly 900 electric cooperatives across the country.

MTE is the largest electric cooperative in the Tennessee Valley Authority (TVA) region and the second-largest in the United States, serving more than 750,000 Tennesseans. Our service territory includes 15,000 miles of distribution lines over 2,200 square miles—or more than double the landmass of Rhode Island—across 11 Middle Tennessee counties, primarily Rutherford, Cannon, Williamson, and Wilson. MTE employs around 540 people in 6 local offices and its Murfreesboro headquarters.

NRECA is the national trade association representing nearly 900 rural electric cooperatives across the country. Electric co-ops are not-for-profit, at-cost electric utility providers focused on delivering affordable, reliable, and secure electricity to over 42 million Americans in 48 States. We are unique in the electric utility sector in that we are private-sector, operate without profit incentives, and are owned and governed by the people we serve.

Electric co-ops were created with a mission to address the distinct challenges associated with providing electric service to rural communities, which typically have lower population densities, are more residential, and less affluent than the industry average. This means that cooperatives are constantly asked to do more with less, and they deliver. Cooperative members give their utilities the highest customer satisfaction scores, on average, in the electric sector.

Electric co-ops are owners and operators of some of our Nation's most critical infrastructure, such as power plants, electrical substations, and transmission and distribution lines. This also includes infrastructure to generate or provide power for more than 150 military facilities and installations across the United States. We also serve as economic drivers and lifelines for critical industries and services in rural communities, including hospitals, schools, emergency services, and food and agriculture production.

Protecting America's electric grid from cyber and physical threats is a top priority for the Nation's electric cooperatives. Accomplishing this important task presents its own set of challenges. The same circumstances that made it difficult to invest in electrifying rural America nearly a hundred years ago, including being isolated from the larger customer bases and diverse talent pools available in urban areas, persist today. These challenges add difficulty in investing in the people, processes, and technologies needed to secure the grid in rural communities.

We have a saying in our industry: If you have met one electric co-op, then you have met exactly one electric co-op. The nearly 900 electric co-ops across the country

all come in different shapes and sizes. Although MTE does not fit the profile of the typical electric cooperative, all our challenges share similar themes. MTE is fortunate to not have to wrestle with some of the more intense challenges of the rural cyber workforce issue. However, with my over 2 decades of experience working for the cooperative, I have seen how MTE has tackled those issues and can share how co-ops are impacted across the broader community.

I will share some of the challenges electric co-ops face in securing the grid, specifically in recruiting, retaining, and developing cybersecurity professionals. I also will highlight how electric cooperatives are overcoming these challenges through the help of resources developed by NRECA and the smart investment of Federal dollars.

THREAT LANDSCAPE

Cyber threats jeopardize electric reliability and pose a significant risk to the Nation's safety, security, and economic well-being.

The cybersecurity threat landscape for electric utilities is increasingly complex and perilous. Electric utilities are prime targets for cyber attacks due to their pivotal role in both national security and daily life. Threat actors, ranging from state-sponsored groups to cyber criminals, exploit vulnerabilities for geopolitical or monetary gains. These attacks have the potential to disrupt the power supply, causing wide-spread outages and economic damage. The rise of sophisticated malware, ransomware, and phishing attacks further exacerbates the risk.

Additionally, smart grids, distributed energy resources (DER), and internet of things (IoT) devices—while improving efficiency—introduce new targets. Defending our infrastructure against new challenges and evolving cybersecurity threats requires strong cybersecurity measures, continuous monitoring, proactive threat intelligence, and a skilled workforce capable of safeguarding these critical assets against increasingly sophisticated attacks.

WORKFORCE CHALLENGE

As cyber threats grow more complex and prevalent, particularly those targeting critical infrastructure like electric utilities, the demand for cybersecurity professionals will continue to grow. In 2023, the National Institute of Standards and Technology (NIST) reported that only 20 percent of business leaders at energy utilities surveyed felt confident that they had the cyber talent they needed. These experts are essential for developing and implementing advanced security measures, conducting threat assessments, and responding to incidents swiftly and effectively.

Despite the evolving and complex threat environment, there are still around 450,000 cybersecurity vacancies in the United States. We need more cyber professionals to safeguard critical infrastructure across the country. While no sector or region is immune to the underlying difficulties of recruiting and retaining skilled cyber professionals, these challenges are exacerbated by the unique and inherent characteristics of electric cooperatives and rural areas.

Electric cooperatives are not-for-profit, at-cost utility providers, meaning we operate without a profit incentive. This model allows co-ops to serve more remote areas with low population density, averaging only 25 percent of the customers and revenue per mile of line, compared with the rest of the industry. Unlike investor-owned utilities, electric cooperatives operate without shareholders. Because of this, financing costly investments often requires reliance on debt, which must be approved by each cooperative's Board of Directors and ultimately paid back through rates paid by their members. Boards are careful stewards of their members' resources and mindful of the economic impact of rate increases to end-of-line consumer-members, particularly given that cooperatives provide service to 92 percent of the Nation's persistent poverty counties.

Therefore, investing in the most sophisticated security technologies and competing for skilled cyber professionals can be a challenge. Recruitment and retention for these professionals are complicated by competitive salaries and benefits offered by larger, urban-based firms, which can lure away skilled workers. Cooperative staff, whether in IT, cyber, or non-technical roles, often wear multiple hats within the organization.

Since electric cooperative service areas are often largely rural, they can be seen as less attractive to professionals seeking vibrant social and professional networks, further complicating recruitment efforts. Rural areas also face significant challenges in developing a robust cybersecurity talent pool. One of the primary issues is the limited access to specialized education and training programs. Many rural regions lack institutions that offer advanced cybersecurity courses, making it difficult for residents to acquire, and keep up to date on, the necessary skills and changing tech-

niques and tactics locally. Additionally, the overall awareness of cybersecurity careers is often lower in these areas, leading to fewer individuals pursuing this field.

CYBER PIVOTT ACT

We want to thank and acknowledge Chairman Green's leadership on introducing the Cyber PIVOTT Act during the last Congress. This proposed legislation was a positive step toward addressing the complex and multifaceted difficulties surrounding the cyber workforce in general, and particularly in rural areas.

NRECA was particularly pleased with the inclusion of language that would extend cybersecurity internship opportunities to critical infrastructure providers in rural communities. We hope this provision will raise the visibility of electric co-ops as a viable and rewarding career path in cyber. Developing a talent pipeline with off-ramps into rural communities will help grow a local, skilled cybersecurity workforce to protect critical infrastructure in these communities. The Cyber PIVOTT Act will bridge the skills gap, enabling rural communities to strengthen their cyber defenses and secure their critical infrastructure.

ELECTRIC COOPERATIVES SOLUTIONS

Electric cooperatives are identifying innovative ways to address cyber workforce challenges. Co-ops are increasingly focused on building local talent through partnerships with educational institutions and providing opportunities for remote work and professional development. We are also seeing partnerships between large generation and transmission cooperatives, State-wide associations, and distribution co-ops to share tools, equipment, and expertise across shared systems to bolster cyber defenses. In the Tennessee Valley, we have a long history of collaboration and partnership among TVA and its 153 local power companies, which are electric cooperatives and municipally-owned electric systems. This partnership extends into the cybersecurity arena. Our State and Valley-wide associations have made cybersecurity a top priority, from conferences and training to work groups and webinars.

Additionally, NRECA is leveraging members' fees and Federal dollars to build a robust cybersecurity program to assist cooperatives in attracting cybersecurity talent, building professional and mentoring networks, and providing skill development and training opportunities.

The Rural Cooperative Cybersecurity Capabilities (RC3) Handbook is a series of comprehensive guides designed for specific roles within cooperatives to help enhance their cybersecurity posture. Last year, NRECA published the final handbook in the series targeted toward H.R. managers to provide practical advice on implementing recruitment and retention strategies and employing on-going professional development.

NRECA and electric cooperatives are also utilizing funds through the Department of Energy's (DOE) Rural and Municipal Utility Cybersecurity Program, or RMUC, to make investments in cybersecurity technology, training, and educational opportunities. RMUC is a generational opportunity to improve the cybersecurity posture of electric cooperatives by providing resources to critical infrastructure operators with the greatest need of support.

Through RMUC, more than 200 personnel from 123 cooperatives participated in an intensive, 3-day training program last year, hosted by DOE. The program was designed to advise attendees on how to improve cybersecurity for industrial control systems and operational technology.

Additionally, NRECA was awarded \$9 million in RMUC funds to strengthen peer-to-peer information sharing, boost mutual assistance, promote cybersecurity awareness, and build internal expertise through the expansion of the NRECA Threat Analysis Center (TAC) and the development of the Cyber Champions Program.

Finally, NRECA hosts an annual technical conference, known as Co-op Cyber Tech, that brings together cybersecurity professionals from rural electric cooperatives to collaborate, share knowledge, and develop skills. The event features hands-on content and sessions on the latest cybersecurity trends and technologies.

CONCLUSION

Cyber threats endanger electric reliability and present a major risk to the Nation's safety, security, and economic stability. Electric cooperatives have a mission to safeguard the electric grid of the communities we serve and live in ourselves.

While electric cooperatives are making smart investments and building strategic partnerships to develop our cyber professionals, more work needs to be done. Initiatives like those in the Cyber PIVOTT Act bring much-needed focus to the cyber workforce needs of rural America. Creating a talent pipeline that includes pathways into rural areas will foster a local, skilled cybersecurity workforce to safeguard critical

infrastructure in these regions. Co-ops and our rural communities have a lot to offer in protecting America's critical infrastructure.

I thank the committee for its bipartisan work on this issue and look forward to answering your questions.

Chairman GREEN. Thank you, Mr. Jones, for your testimony.

Mr. Stier is now recognized for his 5 minutes of opening statement.

**STATEMENT OF MAX STIER, PRESIDENT AND CHIEF
EXECUTIVE OFFICER, PARTNERSHIP FOR PUBLIC SERVICE**

Mr. STIER. Thank you very much, Chairman Green, Ranking Member Thompson, and all the Members of the committee, and especially for the extraordinary way that you have operated as a committee bipartisan and focusing on this issue over the long term and being extraordinarily thoughtful.

It is, unfortunately, I think, a little unusual and deeply appreciated on such a fundamental issue.

We know that it's important when we're thinking about cyber to be focused on the whole picture. That includes, obviously, the private sector as well as the public sector. My focus will be on the public sector.

One important difference in today's world is that our Government is no longer the market maker. It's a market participant and so that relationship between the private sector and the public sector has changed and it's fundamental to think about what that interrelationship actually needs to be.

In the public sector, we have made progress but the truth of the matter is that gaps remain. It's extraordinary that GAO in 1997 identified information security as an item on their high-risk list. It's still there, human capital issues since 2001.

I think this committee should be asking the question we're making progress but what more do we really need to do to change the circumstances? Because the incremental change we're seeing so far, frankly, isn't good enough.

I'm going to offer 3 categories of opportunities for improvement, beginning with reforming the broader system. We often in the Federal Government operate way too much in the vertical. When you're thinking about something like cyber it should be a holistic approach. We need to be looking at, frankly, strategic human capital management across the board, looking at it as one Government and integrating the efforts so we have information from all agencies.

We know there's a 2,000-person gap in the cyber work force at DHS but, frankly, we don't really know what the full picture is. So, understanding it from a comprehensive view is fundamental here.

Second, we need to focus on implementation of things you've already done, in particular the bipartisan Chance to Compete Act. The notion that we should be focused on skills-based hiring is a fundamental one, especially in the cyber area.

Getting that implemented effectively so it actually is making a real difference is going to take work, oversight, and continued follow-up from this committee.

Third, very important, when you look at the pay system it's nuts. We have a pay system the Federal Government that was designed

in 1949 and that's basically how we pay Federal employees. That is when the Federal work force was almost exclusively clerical and now it's professional.

The world has changed. Our Government has not kept up and, frankly, we need to change that. The pay system is a very, very prominent place in which that needs to be done.

Second, we need to go for big swings and partly I mentioned earlier about strategic human capital and doing that holistically. We need to see cyber more broadly managed as a Government-wide asset, not agency by agency. There's enormous efficiencies that can be generated by that.

We need to improve an entry pipeline.

You know, Mr. Chairman, the PIVOTT Act I think is fundamental. You forgot one thing when you mentioned the different agency organizations that were endorsing your legislation. Please include the Partnership for Public Service.

You know, going forward we've been supporting this notion in essence of an ROTC-like program for decades. It is such smart things. We shouldn't build separate institutions. We should use the institutions that already exist.

Third, we need to look at development of mid-career and senior talent. On that front, one of the things we need to think about with the public sector work force is more exchanges between the public sector and the private sector.

There's too much insulation between those and, frankly, it's not only the knowledge that needs to be shared but they need to understand how the different entities work and you do that by working in different entities. So, having more flow of talent, I think, is going to be fundamental.

The third piece that I'm going to flag here, and this is the one that I think is going to be the most challenging, and that is just bluntly we need to stop the harm that is taking place right now. You know, there is no truly real damage being done to the Federal work force, specifically the cyber work force, and it gets to—the list is in terms of the hiring freeze the, you know, push for people to resign, the collection of information about probationary employees.

The best way I can capture this is to read 2 paragraphs of an e-mail that I received last night from a student in a CyberCorps scholarship program.

She writes, "The CyberCorps Scholarship for Service program provides educational funding for students in cybersecurity exchange for working in the Federal Government after graduation. This scholarship has been vital to my career and academic journey. Without the funding I would have been unable to attend graduate school and I was thrilled by the opportunity to work in public service upon graduation."

"It has been a goal of mine for some time to join the Federal work force and this program seemed like the perfect opportunity. In recent weeks, I've had job offers rescinded and opportunities paused until the hiring freeze is over. The Executive actions have led to significant uncertainties for me and my CyberCorps classmates, students who face tremendous pressure to find a Government job or risk owing the Government over \$170,000."

“I urge you to speak with the panel about the importance of ensuring the hiring freeze national security exemptions apply to all cybersecurity jobs in the U.S. Government.” Getting this, I felt an obligation to share.

Thank you so much and look forward to the conversation.

[The prepared statement of Mr. Stier follows:]

PREPARED STATEMENT OF MAX STIER

FEBRUARY 5, 2025

INTRODUCTION

Chairman Green, Ranking Member Thompson, and Members of the committee, thank you for the opportunity to participate in this discussion on strengthening America’s cyber workforce. My testimony today will focus on the cyber workforce needs of the Federal Government.

I am Max Stier, the president and CEO of the Partnership for Public Service, a nonpartisan nonprofit which, over the last 24 years and across administrations of both parties, has been dedicated to building a better Government and stronger democracy.

The Partnership was founded on the premise that any organization’s best asset is its people and that the Federal Government needs dedicated, skilled talent to deliver on promises to the American people.

Our organization over the years has produced a number of reports on cyber talent that speak to the themes relevant to today’s hearing—developing a comprehensive cyber workforce strategy, improving Federal hiring and developing better pipelines into cyber positions encouraging the Nation-wide development of technology skills.¹ We also help place recent graduates in cyber and artificial intelligence fellowships at Federal agencies.²

We believe that the Federal Government should continually modernize its practices and earn the trust of the public. We’ve recently outlined 5 key areas for reform in our Vision for a Better Government:³ develop better Government leaders; make it easier to hire and keep great public servants; hold poor performers accountable; unleash the power of data and technology to achieve better public outcomes; and provide efficient, constituent-friendly services to the public.

The Partnership is gravely concerned about escalating actions that undermine the capabilities of the Executive branch to carry out mandates from Congress, including protecting our national security with a skilled cyber workforce. The list is growing by the hour—freezing of Federal funds, mass firings of Federal employees, threatened coercion of all Federal employees to leave the workforce and disturbing decisions on access to Government systems that impact the private information of your constituents. Collectively, these actions only increase the cyber threat to our country.

By contrast, the committee’s approach today is the right one. With respect to the Federal cyber workforce, this committee for years has focused on key workforce issues: How do we identify and fill cyber skills gaps throughout the Federal Government? What is working and not working for the numerous efforts across the Federal Government—which often are carried out in silos—and how do we leverage success stories across the broader Government-wide cyber workforce? What are ways to best foster Federal, State/local, and private-sector coordination in strengthening the cyber workforce?

As Members of this committee have noted in past hearings, the cyber responsibilities of the Federal Government are vast—not only protecting the systems of Federal agencies but working in partnership to protect the cyber spaces of our Nation’s critical infrastructure, the public at large, and all levels of Government. This hearing today provides a thoughtful forum on how to equip the Federal workforce to address these urgent challenges.

¹Partnership for Public Service, “Cyber In-Security: Strengthening the Federal Cybersecurity Workforce” (July 2009), “Cyber In-Security II: Closing the Federal Talent Gap” (April 2015), “Leading Ambitious Technology Reforms in Government” (Aug. 2017).

²Partnership for Public Service, Cybersecurity and Artificial Intelligence Talent Initiative, <https://gogovernment.org/fellowship/cybersecurity-ai-talent-initiative/>.

³Partnership for Public Service’s “Vision for a Better Government” (Aug. 15, 2024), available at <https://ourpublicservice.org/publications/vision-for-a-better-government/>.

STATUS OF THE FEDERAL CYBER WORKFORCE

While attention to cyber needs has increased greatly across the Federal Government over the last decade, the gaps in agencies' needs remain vast. The Partnership's analysis of data over the last 5 years shows that overall, the Federal cyber workforce grew from over 101,000 in 2019 to over 114,000 in 2024.⁴ This is far short, though, in meeting the Government's overall needs.

For example, the Department of Homeland Security reported to your committee last June that the Department had over 8,000 cyber employees but still had over 2,000 cyber vacancies.⁵ That's exactly the type of skills gap analysis—updated regularly—that we need from each Federal department and agency so that we can best determine how to fill those gaps and how to align Federal efforts with the overall cyber workforce needs of the entire country.

As discussed in your previous hearings on the cyber workforce, we need skills at all levels—entry-level, mid-level (who either already have cyber skills or are good candidates for reskilling) and senior professionals willing to bring their years of expertise into the Government. I want to call particular attention to the age demographics in the Federal cyber workforce. The percentage of Federal cyber workers under age 30 is just under 8 percent, while those age 50 and over represent 48 percent of the Federal cyber workforce.⁶ My recommendations today will offer ways to improve the talent pipeline at all levels, with particular attention to developing the pipeline of future leaders as so many current cyber employees approach retirement.

The committee is well familiar with these challenges and the many studies on the cyber workforce. Notably, the Government Accountability Office first designated information security as a Government-wide High-Risk area in 1997 and subsequently expanded it to include the cybersecurity of critical infrastructure and the privacy of personally identifiable information. GAO then identified strategic human capital management within the Federal Government as a high-risk area in 2001.⁷ In a 2024 High-Risk update, GAO identified the need to address cybersecurity workforce management challenges as 1 of 10 critical cybersecurity action areas.⁸

In its most recent report on the cybersecurity workforce, GAO reviewed the cybersecurity workforce planning efforts of 5 Federal agencies.⁹ GAO found that the Department of Homeland Security had fully implemented most practices that are central to effectively managing the cybersecurity workforce. These practices included (1) setting the strategic direction for the workforce, (2) conducting workforce analyses, (3) developing workforce action plans, (4) implementing and monitoring workforce planning, and (5) evaluating and revising these efforts. The other agencies reviewed, however, were not as consistent in their implementation. Importantly, efforts to destabilize the broader Federal workforce will put these hard-earned gains and strategic planning efforts at risk.

Agencies struggling to implement effective cybersecurity workforce practices identified several challenges they faced including:

- Pay disparity between Federal agencies and the private sector
- Department budget limitations
- Maintaining an adequate cybersecurity workforce
- Recruiting well-qualified applicants
- Time-to-hire cybersecurity personnel for vacant positions
- High attrition due to cybersecurity employees choosing different career paths.

This hearing today is a welcome opportunity to discuss how the Federal Government addresses these challenges.

⁴Based on Office of Personnel Management's FedScope data from Sept. 2019 through Sept. 2023, and March 2024, for occupational categories 0854 (Computer Engineering), 1550 (Computer Science), 2210 (Information Technology Management), and 2230 (DHS Cybersecurity Specialist).

⁵House of Representatives Committee on Homeland Security, hearing entitled "Finding 500,000: Addressing America's Cyber Workforce Gap" (June 26, 2024), available at <https://homeland.house.gov/hearing/finding-500000-addressing-americas-cyber-workforce-gap/>.

⁶Analysis based on Office of Personnel Management's FedScope data as of March 2024.

⁷Government Accountability Office, "High-Risk Series: An Update" (Jan 1, 2001), available at <https://www.gao.gov/products/gao-01-263>.

⁸Government Accountability Office, "High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges" (June 2024), available at <https://www.gao.gov/assets/gao-24-107231.pdf>.

⁹Government Accountability Office, "Cybersecurity Workforce: Departments Need to Fully Implement Key Practices" (Jan. 2025), available at <https://www.gao.gov/assets/gao-25-106795.pdf>.

RECOMMENDATIONS

The Partnership's recommendations on strengthening the Federal cyber workforce largely mirror our broader recommendations for ensuring that our Government has the capabilities and capacity to meet its mission and more effectively deliver services to your constituents. Our overall recommendations are reflected in the Partnership's Vision for a Better Government, mentioned above, which highlights 5 priorities: leadership, Federal hiring and retention, performance management, data and technology, and constituent experience with Government services.

Much of the Federal Government's civil service legal framework dates back decades—in the case of our pay and classification system, over 75 years. The passage of the Civil Service Reform Act of 1978 marked the last broad overhaul of Government-wide laws governing personnel management. Our overall framework for human capital is built for a bygone age when a great bulk of the Federal workforce was clerical, not for this day when highly-specialized skills such as cybersecurity are critical for protecting the health and safety of the people our Government serves.

To its credit, Congress—and this committee in particular—has worked on a bipartisan basis over the years to provide programs and authorities to bolster our Nation's cybersecurity defenses and attract cyber talent into Government.

Here are ways Congress can build on those efforts:

Maintain nonpartisanship as a bedrock principle of the civil service.—Throughout our nearly 25-year history, the Partnership has highlighted the need for updating the ways that the Government should manage its workforce, to align with the modern economy. Our 2014 report, *Building the Enterprise: A New Civil Service Framework*,¹⁰ is just as relevant today as when we issued the report over a decade ago. The report includes recommendations for modernizing the Federal pay system to attract top talent, streamlining the process through which agencies deal with poor performers, and strengthening the Senior Executive Service—all recommendations aimed at increasing the accountability of civil servants. As I have said many times in the past, good Government starts with good people, and our Nation is fortunate to count some of the brightest, most dedicated professionals among its ranks. But too often they succeed in spite of the current system, not because of it.

At the same time, the Partnership has staunchly defended the nonpartisan nature of our civil service. Recent Executive actions take us farther from, not closer to, a civil service system that prizes merit, expertise, and professionalism free from political interference. A civil service staffed by people chosen for their political loyalty rather than their skill will result in a Government less capable of serving the public and more likely to become a tool for retribution and actions counter to democratic principles. A more political Government is not a better Government for the American people, and it does not help make our country safer.

We welcome a conversation on improving the effectiveness of the civil service framework. Politicizing the workforce and freezing budgets, though, will be extremely damaging to the Federal Government's current capacity to address our national security needs and to recruit and retain talent to fill critical skills gaps, including in the area of cybersecurity.

Create high expectations for leaders within Government.—Good leaders create the conditions necessary for employees to perform at their best. In 2019, the Partnership developed the Public Service Leadership Model,¹¹ recognizing the unique nature of leadership in Government, centered on stewardship of public trust and commitment to public good. We believe this model should be the standard for all leaders across the Federal Government.

Federal leaders—both political and career—should be held accountable for the organizational health of the organizations they helm, including the workforce.—Congress should hold leaders responsible for recruiting and retaining highly-qualified talent, developing future leaders, engaging employees, and holding subordinate managers accountable for addressing performance. The Partnership recommends Congress require political appointees to have transparent performance plans to drive this accountability at the highest levels of leadership.

Congress also should urge agency leaders to use the annual Federal Employee Viewpoint Survey and the Partnership's Best Places to Work in the Federal Government® rankings¹² to drive better results in their agencies. Employee engagement

¹⁰Partnership for Public Service, "Building the Enterprise: A New Civil Service Framework" (April 10, 2024), available at <https://ourpublicservice.org/publications/building-the-enterprise/>.

¹¹Available at <https://ourpublicservice.org/public-service-leadership-institute/public-service-leadership-model/>.

¹²Available at <https://ourpublicservice.org/performance-measures/best-places-to-work-in-the-federal-government/>.

is not just about happy employees. Higher scores in employee engagement equate to better performance and higher quality service, which in turn become valuable recruiting and retention tools and help agencies better serve the public.

Undertake a comprehensive analysis of existing tools.—Congress and the Office of Personnel Management have created a number of tools to better position the Government to recruit, hire, train and retain the cyber workforce. These include direct hire authorities, special cyber personnel authorities at the Departments of Defense and Homeland Security, a Federal cyber rotation program, the National Institute of Standards and Technology’s National Initiative for Cybersecurity Education (NICE), and numerous agency programs such as the National Security Agency’s support for cyber clinics in various States and the Department of Labor’s country-wide cyber apprenticeship program.

Within the jurisdiction of this committee, of course, is the DHS Cybersecurity Talent Management System (CTMS), authorized by Congress in 2014 and envisioned as a forward-thinking model that would allow DHS to be more flexible in hiring and managing its cyber workforce. The program was not officially launched, though, until 2021, and as of the date of your June 2024 hearing on the cyber workforce, only 189 hires had been made at DHS under this new authority—a tiny fraction of the DHS cyber workforce.

While reports such as the Office of the National Cyber Director’s National Cyber Workforce and Education Strategy have put out broad visions for cyber talent,¹³ we still need a comprehensive review of existing efforts to give Congress the information it needs to assess the effectiveness and implementation of these different tools, assess why some authorities (such as the DHS CTMS) have been challenging to implement, and determine what adjustments might be warranted. We need a concerted effort to not only assess the effectiveness of different programs and authorities but also to know whether special flexibilities for some agencies put other agencies at a disadvantage in recruiting cyber talent. And undoubtedly there are many success stories that could be replicated throughout the Government and with other levels of Government and the private sector.

For the Federal sector as a whole, this effort needs to be undergirded by careful, regularly updated human resource planning to know specifically which cyber skills and positions agencies and their subcomponents need. Also, as agencies also look to scale the effective use of AI and other emerging technologies, Congress and the White House need to make sure these efforts are aligned with cybersecurity efforts.

Continue to promote innovative talent pipelines.—The commitment of this committee to addressing the Government’s cyber workforce needs, as exhibited by this hearing today, has a profound impact on driving priorities within agencies. Further actions the committee can take include:

- Focus on getting young people into Government. Members of Congress routinely use their intern programs as a pipeline for hiring, and Federal agencies should do the same. In addition to leveraging and coordinating existing cyber-specific programs, Congress on a Government-wide basis could make it easier for agencies to hire young people, including by increasing the cap on direct hire authority for students and recent graduates. Congress should also authorize so-called conversion authority for agencies to hire interns or fellows sponsored by third parties, so that the Government can move quickly to hire high-performing interns or fellows and not lose them to other job offerors.
- Promote ROTC-like opportunities to encourage young people to enter public service—an idea shared by Chairman Green in his bill in the last Congress, the Cyber PIVOTT Act.¹⁴
- Use your oversight capacity to ensure effective implementation of the bipartisan Chance to Compete Act,¹⁵ passed into law late last year to ensure agencies are identifying the skills they need, using technical assessments to identify highly-qualified applicants, and removing barriers such as degree requirements to open the door to technologists with alternate qualifications, backgrounds, and experiences.
- Promote public-private talent exchanges. Providing formal opportunities for individuals from the private sector to temporarily work in the public sector, and vice versa, is an effective way to cross-fertilize knowledge across the sectors and increase each sector’s understanding of the other. Congress should extend Gov-

¹³For a summary of the National Cyber Workforce and Education Strategy, see Center for Security and Emerging Technologies, “Highlights from the National Cyber Workforce and Education Strategy” (Aug. 10, 2023).

¹⁴H.R. 9770, 118th Congress. The Partnership has long endorsed a ROTC-like model as a pipeline for the whole Federal civil service.

¹⁵Pub. L. 118–188 (Dec. 23, 2024).

ernment-wide the talent exchange authority already authorized for the Department of Defense.¹⁶

These types of strategies will better equip Federal agencies to find and hire cyber talent across the country. This is important because over 80 percent of the entire Federal workforce is outside the D.C. area. Moreover, used smartly and with proper oversight, telework and remote work are strategic business tools used by both the public and private sectors to enhance an organization's ability to recruit and retain top talent, increase productivity and reduce the real estate footprint. Just over 64 percent of the Federal cyber workforce is outside of D.C., Maryland, and Virginia.¹⁷

Elevate the human resource functions of agencies.—There are outstanding and innovative H.R. professionals across the Government, but there are also skills gaps in their offices. They are often overwhelmed by responsibilities and the complexities of Federal human capital law. Often, H.R. specialists are not familiar with the authorities they have available to them, and do not have the technologies, data, and analytical skills that would better enable them to recruit and hire while also engage in strategic workforce planning for the future. Ways Congress could strengthen the H.R. function include ensuring that agencies undertake strategic workforce planning and that Chief Human Capital Officers have a voice in the strategic and budget planning processes so that agency leaders will be informed of the H.R. needs necessary to carry out their policies and programs.

Congress also should jump-start efforts to increase the skills and professionalism of the Federal H.R. community by requiring OPM to re-start technical training for H.R. specialists, conduct a review of overall training needs and how those needs can be met, and fund IT needs of the H.R. community.

CONCLUSION

Federal agencies face frenetically-growing needs to protect our Nation's cybersecurity as threats from external actors escalate. To do so, we need the talent, skills, and capacity to meet these needs. This calls for a Government-wide strategic human capital planning effort coordinated between Congress and the White House to ensure agencies have necessary authorities and resources.

As we enter a period where arbitrary moves to reduce the size of the Federal workforce are occurring, there is an increased risk that we lose the exact cyber talent we need. I commend the committee for its continued focus on this critical issue and look forward to working with you on reforms to hiring, performance management, leadership development, and other improvements that will make our Federal workforce systems modernized to meet the needs of the future.

Chairman GREEN. Thank you, Mr. Stier.

Members will be recognized by order of seniority for their 5 minutes of questioning. I want to remind everyone to please keep their questioning to 5 minutes. An additional round of questionings may be called after all Members have been recognized.

I now recognize myself for 5 minutes of questioning. First, I want to thank the witnesses for their support of the PIVOTT Act. I do think, obviously, it is the right way to go about solving this issue.

Having served in the military and seeing how the ROTC program not only benefits the military but then serves the Nation as those individuals get a college degree and expertise and then they leave the force and go out and serve the country working for companies in Government offices elsewhere, that really I think whoever created that is a legacy for the Nation.

The GI Bill is an excellent example. Men and women came home from military service and left the military and had a degree paid for and then went on to serve the country.

So, thank you for all of you for your kind words about that.

¹⁶Section 1104 of the National Defense Authorization Act for Fiscal Year 2017, Pub. L. 114–328 (Dec. 23, 2016).

¹⁷Analysis of FedScope data as of March 2024. We need to ensure that our policies recognize this is a nationwide effort.

Obviously, this 500,000, and I have heard numbers ranging from 500,000 to 700,000, so but it is a really big number. It is our greatest cybersecurity threat without a doubt.

When we look at the issues that create the risk, this is our No. 1 risk. If we don't have the right people in the right place defending our networks, we are going to lose.

Let me ask really a question for all of the witnesses. How has this cyber work force gap affected your organizations? If we had a broader or more prepared work force how would that impact your ability to do your job? So, how has the deficit hit you and if we didn't have this deficit, how would that impact you?

We will start with you, Dr. Russomanno.

Mr. RUSSOMANNO. Well, thank you, and I wish our chief information officer were here to help answer your question. But I do know that we have vulnerabilities within the university. We have very sensitive data, student records, what have you and so, yes, we do have vulnerabilities. Many of those vulnerabilities are through, quite frankly, human behavior so the training aspect is critically important.

A basic level of cybersecurity competency, regardless of your position within an organization, is critically important. A fundamental knowledge of cybersecurity for all, if you will, in terms of basic competencies would go a long way in mitigating a lot of the attacks we see today.

So, certainly within the university environment we're doing all we can. I think universities by and large have fared fairly well compared to the private sector in many instances, but there are significant gaps to be addressed. We would benefit directly from the Cyber PIVOTT Act.

Chairman GREEN. Let me ask Mr. Stier to, kind-of, comment on that question. Then I am going to, because I only have a few minutes, but if you could say where, you know, what is the impact to, you know, not your organization but, you know, businesses from your perspective?

Mr. STIER. Look, I think the impact is profound and we know that there are breaches that are going on. There are national security issues that are very hard to quantify in terms of the harm we're talking about because we have enemies abroad who are collecting information about our country and it puts us at risk in the most fundamental way.

So, you know, look, the reality obviously is that we've moved away from a world in which we do everything physically to a world in which we do almost everything digitally and we haven't kept up with that transformation of our world activity with the work force that can manage that different threat.

I think the point that was just made earlier that it isn't just the cyber work force, it's the entire work force that needs to be sophisticated enough to be able to—and especially the leaders.

I mean this is one of the things that we see in Government writ large which is even if you have technical expertise, if the leaders aren't sufficiently literate the reality is they don't even know what they should be asking for or how to deploy resources effectively. So, investing in leadership literacy in cyber and other things, especially now AI, we think is fundamental.

Chairman GREEN. Well, let me ask the other 2 witnesses that are here. When it comes to recruiting people to come do cyber training and be cyber, you know, experts, what is the biggest hurdle to recruitment of those students who would then come or employees who would then come and be trained on cyber?

Mr. JONES. Mr. Chairman, I would say for the electric co-ops what we face primarily is the work force shortage and then attracting with appropriate salary. Of course, we're talking about a 900 cooperative network, a lot of rural areas that we serve, so we have some natural limitations there relative to someone wanting to come to certain places to work but certainly the talent pool itself is the primary obstacle.

Chairman GREEN. Well, clearly with the limited supply the price is going to be high.

Mr. JONES. Yes, sir.

Chairman GREEN. Mr. Rashotte.

Mr. RASHOTTE. I think being a cybersecurity vendor we're in a different situation. The large majority of employees are cybersecurity professionals within our company so our competitive nature is a little bit different.

What we do see, though, is a lot of our customers and partners are coming to us looking to us as a source for recruitment and I think what they're starting to see now is it's not just a recruitment issue but a retention issue. So, they're not able to retain that talent through into their more senior roles so at the top leadership roles there is starting to become a significant gap because of the retention.

Chairman GREEN. Again, it all comes back to supply and demand, doesn't it? Because that retention, that movement about the industry is because there are all these openings out there and people are paying more. So, thank you for that.

I yield to the Ranking Member for his 5 minutes of questioning.

Mr. THOMPSON. Thank you, Mr. Chairman.

I thank our witnesses for your presentation. Clearly, we accept the premise that we are short of people in this space. The Chairman talked about 500,000. That is probably a good number and the retention issue associated with it is a big challenge also.

But, Mr. Stier, you raised some question on the Government side that I think we need to drill down on. We have for the last 2 weeks been under significant pressure as a Government and our employees are being told that there is a hiring freeze, you have got to go home.

I guess the question would be how does the impact on hiring freezes have on the ability of Federal agencies to do their job? I will do that first and then I will go to the other part.

Mr. STIER. Congressman, I think that the answer is very clear. I read you the e-mail from the student in the cyber, you know, scholarship program, CyberCorps scholarship program.

The reality, I mean, we all have organizations that we're running. Our most important asset are our people and creating environments that enable them to perform at their very best is essential to our jobs as leaders in our organizations. When you create an atmosphere, frankly, of fear, you're diminishing your capacity to perform.

So, whatever else one might say, it's not the way to run an organization. When we're talking about cybersecurity, which, obviously, has such a fundamental national security and broad impact on our society, is dangerous.

So whether it's the hiring freeze or some of the other actions that are taking place, there's plenty of ways to improve our Government. We need to actually engage in a massive reform of our Government. The things we're seeing right now are taking us the wrong way.

Mr. THOMPSON. Well, and I appreciate your comment. So, even a temporary pause can be disruptive. Can you talk about that temporary pause and delay as it relates to slowing the hiring process?

Mr. STIER. Well, look, I think that the reality is many new administrations coming in actually engage in some kind of hiring freeze, so I think, to me, it's the broader picture that we need to be looking at right now.

We already have a hiring system in the Federal Government that is not just ridiculously slow, and that's a big problem, but even more important is that it doesn't often identify the best talent or really operate in a strategic fashion. So, you don't actually have subject-matter experts owning the hiring process. It's often the H.R. professionals who don't really know what they should even be looking for.

So, there is a fundamental need to reform the hiring process. When you do a hiring freeze you layer on top of what is already not working well and a whole another set of problems, not only with those people who are already in the pipeline but, frankly, in your ability to attract people from the outside who are looking at the hiring freeze and saying how can I go there? There's no opportunity for me there.

So, it is enormously disruptive. We do need to think about the brand of the Federal Government as a hiring employer and that needs a lot of work because right now it is not presenting itself in a way that is most attractive to the talent that we need in our Government to serve us better.

Mr. THOMPSON. Thank you. Right now there is one individual who is 19 years old working for DOGE who has access to all our information, employee information. Can you just tell us how do you protect in your own company employees' Social Security numbers and other information?

We'll start with Dr. Russomanno.

Mr. RUSSOMANNO. Sure. What you've described is, you know, one of the chief responsibilities of our chief information officer. Of course, we have obligations around FERPA and student records so I know that we do all we can to adopt the latest technology to ensure the safety and security of our student records.

Moreover, we do, as a research R1 university, we do a lot of research, a lot of intellectual capital, intellectual property and what have you. So, once again, our chief information officer and our IT organization I think they do a stellar job in terms of protecting our assets given a really very lean organization, so we have been very fortunate, quite frankly, that we have not had significant issues with respect to breaches.

Mr. THOMPSON. Well, my time is up but I think you have made my point is just anybody doesn't have access to that kind of information. You have a defined process that is closed and that is it. That is how you protect your employees as well as your organization.

Thank you. I yield back.

Chairman GREEN. The gentleman yields.

I now recognize the Chairman emeritus of the committee, my friend from Texas, Mr. McCaul.

Mr. MCCAUL. Well, thank you. Thank you, Mr. Chairman, a very important issue. I think STEM education, and I know this is not in the jurisdiction of this committee, is also very important.

In 2014, the Ranking Member and I introduced the CyberCorps Scholarship for Service Program. Since that time we have had \$600 million in funding, 5,000 scholarships, and 3- to 4-year work requirements.

First of all, Dr. Russomanno, I apologize, and Mr. Stier, could you touch on the success of the program and what needs to be done to enhance it?

In addition, how will the PIVOTT Act complement those efforts?

Mr. RUSSOMANNO. Well, thank you, Congressman McCaul, for that question. As I said in my opening remarks, I've had the opportunity to be part of CyberCorps at 2 different universities and have seen the impact on both universities where urban-serving, drawing, you know, serving students from a variety of backgrounds.

One of the real strengths of CyberCorps is the internship component, the career fairs. The national career fairs in the District of Columbia are a wonderful opportunity for students to network to learn more about the various Federal agencies where cybersecurity is, of course, a very important aspect. So that internship opportunity has really been important.

Now, in terms of improving that, I think more distribution of those types of affairs across the Nation would be critically important. If you look at urban-serving universities, many times students may be reluctant to leave their immediate geographic area.

There could be family dependencies and so on on that first-generation student, so I think having opportunities distributed throughout the Nation, many of those jobs are concentrated in the D.C. area, I believe that would be a great opportunity and maybe working additionally with the private sector with regard to incentives to provide further distribution and penetration across the United States. We heard about rural-serving areas as well.

So, I think that could be an opportunity to further penetrate the great benefits of CyberCorps across our Nation.

Mr. MCCAUL. Mr. Stier.

Mr. STIER. Well, first of all, thank you for creating the program. It's done a lot of good. Thank you for looking to how to make it better because we're, obviously, are going to do that always.

My thought would be to really think about career pathing. I think one of the real challenges is you may get entry talent coming in but how do you retain them?

Can you create something that may be an add-on to the program that provides a private-sector placement so that they're getting both the private-sector and the public-sector experience with the

expectation that they'll take that private-sector experience and return to the Government as a way of again bringing best practice from the private sector into the Government?

We need to see more of that flow back and forth as I mentioned earlier and I think if you think of this as a longer-term pathway that will be very important.

Then the last thing I would say to your last point, I think the PIVOTT Act is an improvement. We need to scale. We're talking about such a huge problem. If we don't scale, you know, it's a good thing but it's not meeting the need.

Mr. McCAUL. Yes. I think marking up and passing the PIVOTT Act will, I think, complement the success of the CyberCorps program.

The role of the guard, you know, this is my guardsman. It is at Camp Mabry in Austin. You know, they have tech jobs in the daytime and they are weekend warriors in the Cyber Command, you know, on the weekends. I see that as a great enhancement to our both Federal work force, but also with the State as well.

My Governor just created a Texas Cyber Command in San Antonio where the Air Force has its Cyber Command, and I see that Federal-State partnership really enhancing that. I think it is very helpful when the States get engaged in this and not just relying on the Federal Government. Do you have any thoughts on that?

Mr. RUSSOMANNO. Well, I would say once again, CyberCorps and the PIVOTT Act with that service component is a great model. The question is how do other entities adopt that model?

Certainly I think there's ample opportunity at the State and local levels to look at how the CyberCorps project has been successful and in turn then adopt those best practices in their local areas, as well as the private sector.

Mr. McCAUL. I think, Mr. Russomanno, you mentioned the role of veterans, too. I mean, they have a skill set that they may not be aware that the private sector or State or Federal Service could, you know, enhance their careers beyond the military. I think that is an area we need to enhance and look at as well.

Then finally on the exemption issue, I just wanted to close by saying that it is my understanding that CISA and the DoD are exempted from the Executive Order. So, for your student who may be worried about this, that is good for them to know also the national security and public safety exemption to the Executive Order as well.

With that I yield back.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Correa—

Mr. CORREA. Mr. Chairman—

Chairman GREEN [continuing]. For his 5 minutes of questioning. Good to see you.

Mr. CORREA. Thank you very much. May I respectfully have 10 minutes?

Chairman GREEN. Well, you know how I do this so ask your question—

Mr. CORREA. Seven minutes, you have got a deal. Thank you, Mr. Chairman.

I want to thank our witnesses for being here today. This is the most important issue that we have dealt with in Homeland Security for a number of years now. We all read about those big hacking situations, Colonial Pipeline. What we don't read about are those victims, big and small, that actually pay the ransom and continue to remain quiet.

We also don't read about folks back home on Main Street, my Main Street, small businesses getting hacked, losing information, not paying the ransom, and getting hit hard, No. 1, by those people that hacked them and then No. 2 with a lawsuit. The loss in economic value is high.

Gentlemen, all of you had some great information here today and my question would be as follows. We are losing personnel. It is hard to recruit individuals to go into the sector, not only because it's STEM but because of the pay. The private sector will always pay more than the public sector.

Yet I look at Government, the FBI, the CIA, and other Government agencies that are active in this area in critical ways. How do they compete with the private sector? How do they recruit to get people to go into those jobs?

I think we have had this discussion in this committee as well. I think at the end of the day these young men and women that join the ranks of the public sector are really patriots. They want to do it because they love this country. They want to do it because they want to do the right thing.

Right now we pick up the newspapers, we have an FBI hiring freeze. We have a hunt for FBI agents that were involved in the January 6th investigation. These men were following orders. These individuals, men and women, were doing what they thought was right for this country.

So, I am looking at somebody in college who is maybe looking at going into the FBI for a career, what are they saying? What is the motivation here?

Just as I was walking over here, I picked up a report that says CIA Offers Buyouts to Workforce, similar to those proposed to other Government agencies, except for those that are in sensitive areas.

Well, the rookies coming into the CIA like FBI got to learn the business. Cyber is one of those that you don't walk in and say, aha, I got it. I got a 4-year degree or a 2-year technical degree. You have to be there for a number of years.

So, I want going to ask each one of you very quickly how does this hurt our country's recruitment when you have across the board Federal agencies asking their workers to actually resign or take early buyout offers?

Mr. Russomanno. I only have a minute-and-a-half so if you could be brief?

Mr. RUSSOMANNO. Thank you, Congressman Correa. I would say, you know, our focus really is on providing opportunities for students and, you know, respect for—

Mr. CORREA. OK, got you.

Mr. Jones, how about you?

Mr. JONES. Congressman, I would say that when I think about electric co-ops and the opportunities we provide I would say that there's virtue in service and that is an attractor that we have.

When we have people that come to work for us maybe they're not making the most money, but the virtue of——

Mr. CORREA. Do you have a steady job?

Mr. JONES. Yes, sir.

Mr. CORREA. You know what you are doing for the public, for the community, and that is what it is about. So, if you get a buyout offer saying you have got to leave, how does that affect your recruiting?

Mr. JONES. Well, it certainly would impact, sir, but as far as all the particulars and the——

Mr. CORREA. Mr. Rashotte.

Mr. RASHOTTE. I think you're right in that the majority of people that are in cybersecurity roles are doing it because they love it. Creating an environment for those people to thrive and providing them as much education as we can through free education——

Mr. CORREA. And uncertainty causes what?

Mr. Stier.

Mr. STIER. Of course it hurts. That's an obvious proposition. I think that it's important to focus on that this is a purpose-driven work force. It is what enables you to recruit people even if you're not going to make as much money.

We do need to change the pay scale. It's worth noting as well that a third of Federal employees are veterans and it's because they care. They serve their country in their uniform and they want to serve their country as civil servants.

Mr. CORREA. Thank you, Mr. Chairman. I'm out of time.

Chairman GREEN. The gentleman yields.

I now recognize the former Chairman of the Border Subcommittee, the gentleman from Louisiana, Mr. Higgins, for 5 minutes of questioning.

Mr. HIGGINS. Thank you, Mr. Chairman.

In the last Congress I posed a question to this committee. We discussed the nature of the work force is what we are here to talk about today.

The historical comparisons of work force participation is a concerning trend, but perhaps offers us an opportunity as it relates to the cyber realm and our work force requirements to address emerging threats to our country and how can we draw upon the available work force?

We discussed how to prepare and recruit America's cyber work force and I remarked upon a documented phenomenon of America's so-called disconnected generation. Just a few stats, the current labor force participation rate among Gen Z, ages 20 to 24, is 71 percent. That's roughly 4 percent lower than the millennial generation and 6 percentage points lower than the preceding generation when they were in the same age range.

This is to me, my perspective is this is a sweet spot that perhaps in our work force we should focus on and specifically, according to a recent study among Gen Z, a staggering 73 percent of those young Americans report feeling constantly alone.

As it relates to the to the disconnect from the labor force, perhaps there are several factors that contribute to that, but let's talk about the conceptual nature of this field, the cyber field.

The cyber battlefield is vast but unseen and the call to man our cyber defenses, while critical, it lands differently than, say, a call to serve in uniform or on the front lines in the traditionally historical perspective like public or military service.

So, how do we bridge this gap and how do we access this vast work force that is available of young Americans that are not engaged? I would like to submit for the record, Mr. Chairman, a Rand Corporation report entitled, "How to analyze the cyber threat from drones." I seek unanimous consent to offer it, Mr. Chairman.

Chairman GREEN. Without objection.*

Mr. HIGGINS. Thank you.

This report touches on the things we are discussing and how we can connect our relevant fields, gentlemen, to this work force. I ask you, Mr. Russomanno and Mr. Rashotte, how are you adjusting your particular intersections with the cyber realm to make cybersecurity attractive to this generation that is available?

Mr. Russomanno.

Mr. RUSSOMANNO. Thank you, Congressman Higgins, for that question. With respect to Gen Z, I think it's very important to message early on and glad to hear about these early K through 12 initiatives is how vast the cybersecurity field is. Many times folks think about computer science, engineering, these disciplines that have tremendous prerequisite chains, a mathematical foundation, a basic science foundation. Those are wonderful programs.

Our Nation needs those programs to advance the state-of-the-art, but there's ample opportunities to apply the state-of-the-art and I don't believe we're articulating those opportunities broadly enough to Gen Z.

So, at the University of Memphis, for example, we have the Polytechnic Initiative that's really looking at expanding our cybersecurity degree portfolio to better align with community college and other training programs.

Mr. HIGGINS. Are you seeing an engagement from these young Americans where they appear there is some heightened awareness of the cybersecurity field and they are attracted to that? Are we recruiting these young Americans through that program?

Mr. RUSSOMANNO. I believe so. The real challenge is for these students to see themselves in these careers because oftentimes they may think of the barrier in terms of the mathematical preparation, basic sciences preparation. So really that focus on that applied practice, which I think the PIVOTT bill in particular is addressing to expand the work force through community college and technical school opportunities.

Mr. HIGGINS. Thank you. My time has expired but, Mr. Chairman, could Mr. Rashotte briefly respond to the same question how is he—

Chairman GREEN. Absolutely.

*The document has been retained in committee files and can also be found at https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2972/RAND_RR2972.pdf.

Mr. HIGGINS [continuing]. How is he helping the work force see their way into the cybersecurity realm?

Mr. RASHOTTE. I think the public-private partnerships are critical and from a roles perspective I think cybersecurity roles can sometimes be quite nebulous. So, someone going into education in a cybersecurity career what does that career look like? What is the actual role?

So, we're taking a lot of emphasis around working with organizations to try to define those roles. What is a SECOPS analyst, for example? Working with organizations like NIST with the nice career paths and trying to map it. We've actually mapped our entire catalog of cybersecurity training courses to the nice pathways to try to make that more well-defined.

We're also working with hundreds of academic institutions to integrate our enterprise certifications into academic programs to make it more relevant and more hands-on.

Mr. HIGGINS. Thank you, sir.

Thank you, Mr. Chairman, for the indulgence. I yield.

Chairman GREEN. Absolutely. The gentleman yields.

I now recognize the doctor, Congressman Thanedar from Michigan for his 5 minutes of questioning.

Mr. THANEDAR. Thank you, Chairman Dr. Green and Ranking Member Thompson. Thank you for having this hearing.

I thank the witnesses to be here and appreciate their expertise and comments.

Look, in the first week in office, President Trump illegally fired 17 inspectors general, the independent watchdogs responsible for providing critical oversight of Federal agencies. We know that the administration is scared of anyone tracking what they are doing and this effort is just one part of their effort to avoid any accountability.

IGs play a critical role in routing out waste, fraud, and abuse and help protect employee whistleblowers and purging them reflects a hope in the Trump administration that nobody will check their abuse of power.

Mr. Stier, why are independent inspector general so important, and what will be the impact of this most recent purge?

Mr. STIER. So, the inspector generals are, I think, a innovation in our governance in our system that came out in 1978 with the response to some of the choices that were made by President Nixon that looked to exceed his Presidential authority. Congress acted to create the IGs as a way of making sure that there was eyes and ears inside agencies to address waste, fraud, and abuse issues, as you've described.

I'm going to try to bring this back to the cyber issue if you don't mind? I would just say that, you know, one of the issues that they have focused on has been this question of cybersecurity in agencies. I think it's important in terms of the system that we're talking about here that IGs, while they are political appointees, they're nonpartisan political appointees.

They're intended to extend beyond a single term or administration because the intent is to make sure that you have somebody who has the expertise and, you know, frankly, the independence to ensure that you all in Congress are getting the information that

you need to be able to do the oversight that is required, as well as the agency leadership as well.

So, it is disturbing to see wholesale firings of IGs. It's actually something that I think will diminish the capacity of our Government to perform well and for you to do your jobs well.

Mr. THANEDAR. Thank you so much. I want to change the focus a little bit. I want to look at this shortage of technology people. I mean, we currently are under threat for cyber attacks. Many of our agencies, many of our organizations are under attack.

While we are talking about long-range plans in terms of academic training and 4-year college programs, weekend programs, but this needs to be a two-pronged approach. What are we going to do today now to protect our institutions and then what are we going to do in the future to be able to recruit the people that we need?

Now, I ran small technology businesses. Hiring technical skilled people is always a challenge, and we are always competing internally, not only in the private sector. So, we need to be—what kind of employer Federal Government is and what recent changes that have been done in terms of the cuts.

Was that due to the morale of existing employees, Federal employees, and those who want to be into the Federal Government because of patriotic reasons, because of their love for this country?

What are we doing to attract people and are we a good employer? Are we also looking at the anti-immigrant bias? With the current administration there are a lot of cybersecurity personnel trained outside of United States and what are we doing to make sure that we are able to hire them and attract them and compete while Canada and Australia and others are also competing for the same talent?

Any thoughts? Maybe, Dr. Russomanno, if you can comment on that?

Mr. RUSSOMANNO. Sure. No, your point is well-taken in terms of the here and now. You know, some of the things that we're really focusing on is reaching down to the high schools, you know, creating dual enrollment curricula to provide not only the competencies around cybersecurity, but exposure to the career to get excitement, right, to help build that pipeline in the high schools and developing that talent that can then hopefully matriculate to the academic programs, whether they're at their community college, technical school, or a 4-year institution.

So, really developing that, that comprehensive pipeline that's not a bumpy road but a smooth road with roadside assistance. That's what we're focused on.

Mr. THANEDAR. Thank you so much.

Thank you, Chairman, for this extra 38 seconds.

Chairman GREEN. The gentleman yields.

I now recognize the gentleman from Texas, Mr. Luttrell, for his 5 minutes of questioning.

Mr. LUTTRELL. Thank you, Mr. Chairman.

Mr. Rashotte, you said that you are across the continental United States so I come from a very rural district and there is an appetite and they are very hungry for everything, if you will. Can you come out and give an educational course in my K through 12

schools? K through 12 is in one building. Is that something do I reach out to your organization? How does that work?

Mr. RASHOTTE. Yes, thanks for the question. Absolutely. We've made our entire curriculum, our entire catalog of cybersecurity training available on multiple modes so that we can address these types of challenges.

We've actually hired a team of K to 12 educators within Fortinet to develop K to 12 education for teachers.

Mr. LUTTRELL. We just onboard the software and—

Mr. RASHOTTE. Absolutely.

Mr. LUTTRELL. OK. That is beautiful. The bad part about it is I have been up here for 2 years and some change and I didn't even know you guys existed. Therein lies the problem because we have chatted about we want to recruit out of the military, which I think is a fabulous idea.

Mr. Jones, you're out in the rural areas. A lot of folks don't want to live out in the country like we do. If we offer these job opportunities and we talk about pay and when we—which is a challenge. It always is.

But the hard part about bringing experience and expertise into the military, the private sector going to come in and snatch them and pay them 3 times as much as we can Federally. So there is the problems, one of the very many problem sets, if you will.

Mr. Stier, you laid it out. Job well-done. I love the way you laid everything out because we need to hear that here. You all are the subject-matter experts.

My first question is there is no portal. There is no enclave of information where the mass, either whether it is in the universities, and Mr. Russomanno, you and I spoke about that.

I have a university in my district that is eagerly trying to put together an academic profile or a degree plan for cybersecurity so those folks downstream, whether it is at the Federal or private, have or can communicate with the universities like, hey, here is where we are in 2025. This is the expectation that we have and this is where we need our men and women to be once they graduate and they will take it from there.

That is where I need traction. I need you all, however this is going to work. So, my question is is there an existing department, whether or not it's CISA or Federal and if it's DoD and CISA together, where can something live that universities, private sector can go, as well as lower academics can go and converge these 2 problems?

Mr. Russomanno, have you got some for me there?

Mr. RUSSOMANNO. Yes. I mean, I would, you know, a lot of our experience is working with the National Science Foundation. That for me it comes to mind as a facilitator to bring together institutions toward shared goals.

For example, we'd love to partner and work with, you know, universities in your district. We're working on a national model. We welcome other partner institutions.

Mr. LUTTRELL. Is it actually that easy for me to tell Willis High School to reach out to the National Science Academies and say, hey, look, there you go?

Mr. RUSSOMANNO. Well, I think it starts with partnerships among like-minded institutions, I mean, working together and then influencing potential calls for proposals from the National Science Foundation to address your goals, as one approach.

Mr. LUTTRELL. Is it—OK. But, you know, I hate to—sometimes doing a lot of work is something that a lot of people don't want to do. I am trying to ease the movement, if you will.

Mr. RASHOTTE, you got anything on that for me? Like, what specifically in your opinion can, like, if when we have CISA in here I was, like, all right, hey, here is your role and responsibility. You are to reach out to every single K through 12 school in the continental United States and see where they are in the cyber space or whomever.

Mr. RASHOTTE. I mean, it's something that we've done a lot of work with at the State level with different—where we have our K to 12 program operating in 43 different States now and that has primarily been an effort through State and local government. But it has been quite successful and I think we can continue pushing that.

Mr. LUTTRELL. OK. I will ask this because I am going to reach out to every single one of you, just if you will, I don't care if you throw it at the wall or put it on a white board.

In the military we had mission success and we worked our way back to the starting line and how do we get there? What is the most streamlined process? Who we taking and where are our contingency plans at?

That is something that we thrive on in here because inevitably it is going to come up to either legislation or dollar bills. Again, you guys are the subject-matter experts so I appreciate that communication.

Yes, sir, Mr. Jones.

Mr. JONES. Well, Congressman, I would say reach out to your local electric cooperatives and let us be a facilitator and part of that process. We want to be drivers with that regard. We have a national association that can help be a facilitator, and I'm happy to be a bridge to you as well. So, feel free to reach out to me.

Mr. LUTTRELL. Thank you.

Mr. Chairman, I yield back, sir. Thank you.

Chairman GREEN. The gentleman yields.

I now recognize the Ranking Member on the Cyber Subcommittee. You are still in that role, right?

Mr. SWALWELL. Yes. Yes, I am.

Chairman GREEN. OK, excellent. I am glad to see you staying there. We are going to come to your community. I think we are going to do a field hearing.

Mr. SWALWELL. That would be great.

Chairman GREEN. Yes, in the Palo Alto area—

Mr. SWALWELL. On cyber work?

Chairman GREEN. On cyber, yes. So, I recognize the gentleman from California for his 5 minutes of questioning.

Mr. SWALWELL. Great. Thank you, Chairman.

This committee was stood up to address threats to the homeland after September 11, something my colleague to the right knows a lot about being here since its inception. Today, I just want to brief-

ly address the question as to whether we are safe today as a country because what I am seeing from this administration is that we are taking our eye off the ball.

We had a terrorist attack in New Orleans to start the year. ISIS, al-Qaeda, other terrorist organizations want to hit us and hit us hard. We've got the Super Bowl this weekend back in New Orleans. We have the World Cup in 2026, and we have the Olympics in 2028 in the United States. There are a lot of prime national security targets.

However, what we are seeing are actions from this administration that do not make us safe. The most basic job of Government is for people to feel safe.

So, when President Trump releases 1,600 violent criminals into our communities, people who brutally attacked police officers, we should not be surprised that they are already committing crimes.

One of them just last week in Indiana was pulled over by a police officer and shocking. Didn't want to obey that officer's orders, fought the cop, tried to use his own gun on the cop, and thankfully the cop shot and took that individual down. Others are committing acts of child pornography who have already been released.

So, are we safe when 1,600 violent individuals are released into the community? No, we are not safe.

President Trump is seeking to fire thousands of FBI agents and has already fired many senior officials. Why? Because these individuals happened to work on cases that he was involved with where he was accused of stealing national security secrets and leading a coup against his own Government.

These Federal agents keep their head down and they go where they are assigned. It is not a fantasy football draft. They don't get to pick the cases that they work on. They just do their job and they follow the evidence.

But what happens when you take thousands of FBI agents out of the Hoover building? They don't work on terrorism. They don't work on child trafficking. They don't work on public corruption. They don't work on violent crimes.

So, are we safe when we take thousands of cops off the beat to protect us from terrorism? No, we are not safe.

The President is seeking to force resignations at the Central Intelligence Agency. These are the best spies in the world who have spent years developing foreign languages, are assigned all over the world, have taken years to train to get necessary experience, and they will be taken off the beat to find the threats that face us as a country.

Are we safe when they are not on their watch? No, we are not safe.

As we speak, Elon Musk, who no one elected, no one asked for, is at the Department of Treasury with a cyber gang with access to every American's tax returns and personal identifying information. So speaking of cyber vulnerabilities, are we safe when unvetted individuals have access to your most precious data, information about your employer, your health care, your Social Security number? No, we are not safe.

Our job is to make the American people safer and, Mr. Stier, if we gut and take off the beat the individuals who are supposed to

work at CISA and monitor international cyber attacks against our local businesses, does that make us more able to respond to a cyber attack and protect Americans data or less able?

Mr. STIER. Congressman, as we've covered it already, work forces are not improved in terms of their capacity to do their job if they are in crisis. We have a Federal work force that is in crisis right now.

On the issue of cyber issues, it puts us certainly at greater risk, both with respect to the specific cyber talent and more generally the work force at large. So, easy answer is this is not enabling our Government to do its job in the way that the civil servants who are there would like to do it.

Mr. SWALWELL. I am all for getting rid of waste, fraud, and abuse. I support any efforts to do that. But when it comes to national security, you better be pretty damn careful about where we make cuts because my promise to you is we will be hit if we take our eye off the ball.

I yield back.

Chairman GREEN. The gentleman yields.

I now recognize the Chairman of our Terrorism Counterterrorism Task Force Subcommittee, the gentleman from Texas, Mr. Pfluger.

Mr. PFLUGER. Thank you, Mr. Chairman, and thank you for having this hearing. I think that is a great point. We have been hit over the last 4 years. We have seen gaps in our security.

We have been vulnerable, and I think you holding this hearing today is an acknowledgement of a new direction that we are going. We are going to make sure, damn sure, that we are protected.

So, I thank our witnesses and our panelists and I want to start—listen, I represent Angelo State University. I have mentioned this in this hearing room many times. Dr. Russomanno, I will start with you.

What lessons, and Angelo State is a center of academic excellence in cyber defense, what lessons should Angelo State be learning and what programs should they be trying to seek to help with the shortage of cyber professionals that we have, especially those that come from places like rural Texas that want to be a part of our security and defense? Give us some of the lessons you have learned and those that I can share with an institution like that.

Mr. RUSSOMANNO. You know, I think the key is expanding the portfolio of training with respect to cybersecurity readiness. Once again, many folks think of just computer science and engineering as those pathways, but there's others.

With respect to the national security threats that have been voiced, I know Gen Z students they want to make a difference, right? They are looking for meaningful work. That wasn't necessarily the motivation of an 18-year-old in my generation, but Gen Z wants to make a difference.

So, a call to this national security threat is something that Gen Z could rise to, and I will point out the ISC2 study from last year pointed out that our cybersecurity growth is flat year-over-year last year. So, as the threat is increasing our work force growth is flat.

We have to broaden the academic programs and training programs available to our students and articulate the urgency and the

opportunity for Gen Z to make a difference in this challenge our Nation faces.

Mr. PFLUGER. Are those training programs adequately suited to address the threat, to meet the threat, or is it Volt, Typhoon, and some of these things that we have seen recently? I mean, are they outpacing what we are learning or is it adequate right now?

Mr. RUSSOMANNO. We need more investment and applying the state-of-the-art to our cybersecurity threats. I think the Cyber PIVOTT Act is addressing broadening that work force, focused on applying the state-of-the-art.

Mr. PFLUGER. Thank you.

Mr. Jones, I'll go to you and I have 2 questions for you. No. 1, talk about internships and, kind-of, pick up where Dr. Russomanno left off. What do those internships look like? What is most beneficial? How do we take a center of excellence, a student that comes from rural west Texas and put that individual into a proper internship?

Mr. JONES. Yes, Congressman, thank you. So opportunity, obviously, for someone to come in and learn about cybersecurity, about the techniques that we have in place, but also to learn about an electric co-op, you know, that we're, you know, for a place like you're describing a good place to work with a virtuous mission.

So, there's a good exchange there and we hope to raise the profile of what electric co-ops do in internship programs like that.

Mr. PFLUGER. Well, that is where I was going with the second part of the question is how worried are our cooperatives, which service communities like mine in many, many cases? How worried are we that that piece of critical infrastructure is vulnerable to an attack that would shut down the lights?

Mr. JONES. Well, Congressman, I would relate it this way, if I may? So, electric co-op managers we have a universal and always have had a universal item that keeps us at night and that's the safety of our team members.

We have a dangerous profession, but we have an accompanying worry that keeps us up at night now and it's certainly cybersecurity, so this weighs heavy, I can assure you, on every electric co-op manager across this country.

So, we're taking it seriously. We're working together. We're collaborating. We appreciate this opportunity to collaborate with the Federal Government. We want to be the best partner we can be, but yes, it is top of mind for all of us.

Mr. PFLUGER. Thank you.

We have got 45 seconds left. I will leave the time to the additional or the other two witnesses. What keeps you up at night? How will the PIVOTT Act help with those threats? You have got about 20 seconds each.

Mr. RASHOTTE. I think I'd like to emphasize again this idea of broadening our scope of cybersecurity training and the roles and so on where today I think we typically focus on training people that just have cybersecurity in their job role or in their job title where I think it's a broader focus than that.

We need to make sure that people coming out of business schools understand cyber threats. We need to understand that people coming out of law school understand risk mitigation and so on.

From a physical cybersecurity perspective we don't just train people that have security in their job title, and I think we need to take the same approach here and really broaden our view of who needs that cybersecurity knowledge.

Mr. PFLUGER. My time is expired. I am sorry. If you would like to enter something for the record please do so.

I yield back.

Chairman GREEN. The gentleman yields.

I now recognize the gentlelady from Illinois Mrs. Ramirez for her 5 minutes of questioning.

Mrs. RAMIREZ. Thank you, Chairman.

Well, let's be serious. We are here talking about preparing the pipeline. The title of this hearing is laughable. How do we prepare the pipeline or examine the state of America's cyber work force when unelected, unaccountable, President Musk and Trump are asking over half of the Federal work force to resign and issuing Executive Orders freezing hiring and funding for Federal agencies? How do you prepare the pipeline?

Under a Musk and Trump Presidency it is clear that the security of Americans' information is not a priority. I mean, let's think about this.

A private civilian with no security clearance bullied his way into the Treasury. He set up private servers and stole sensitive information from an agency. Let me repeat that because I think some of my colleagues on the other side need to hear it again. A private civilian with no security clearance bullied his way into Treasury, set up private servers and stole sensitive information from the agency.

Folks, if that isn't a national security crisis, a cybersecurity crisis, I don't know what is. The true threat to our homeland security is felon Musk, Trump, and their blatant misuse of power to steal information and coerce employees to leave agencies.

The billionaire boss and his puppet, I am going to let you all decide which is which, are on a mission of privatization for their own profit. Well, my mission and I think the mission of a number of members here, is to protect the people.

With that, I want to really turn on to questions, and look. One challenge the Federal Government has when it comes to cyber work force recruitment and retention is competing with the private sector.

We know the Government is not going to be able to pay as much as tech companies like Google or CrowdStrike pay, but the Federal Government has relied on offering a strong benefit package that also includes retirement benefits. That is how you recruit. It helps recruit and retain workers.

Now, Republicans are proposing to cut Federal employee benefits to pay for tax cuts for the richest man in the world and Trump's other billionaire bosses. I worry this will make it even harder for us to recruit and prepare a pipeline and keep cybersecurity professionals.

So, Mr. Stier, how have Federal employee benefits played an important part in recruiting and retaining employees? Let me give you the second part of that question. How could cuts to retirement

benefits harm efforts to attract new cybersecurity workers and keep the cyber defenders we currently have? Mr. Stier.

Mr. STIER. Sure. So, I think returning to why is it that people come into Government more broadly it's because of mission more than anything else, but mission alone, people don't work only for mission alone so compensation is clearly quite important.

I noted earlier that the pay system we have today across the Government is based on a 1949 law. It was based on this notion of everyone could be paid the same at the similar level of work. In a world in which you have different occupations like cyber that's foolishness.

So, you know, the answer No. 1 is what should be done is modernize the Federal pay system so that you actually have some market sensitivity by occupation, which is something we largely don't have.

With the cyber work force we have different systems at DoD, DHS, but there's been no analysis about what is the right system and why should that system be applied to a single agency rather against the entire cyber work force?

So, if you want to address how you recruit and retain on the compensation side a better cyber work force, modernize the pay system, treat it as a unified work force across the entire Government so you don't have agencies competing against each other and you will create better return for the American taxpayer and a safer country.

Mrs. RAMIREZ. Thank you, Mr. Stier.

So, let me follow up on that. Upon taking office, Trump resurrected Schedule F, his attempt to bring back the Gilded Age spoil system and hire Federal workers based on partisan loyalties rather than qualifications and merits.

This policy could lead to mass firings of qualified cybersecurity policy experts across the Federal Government and would dangerously politicize civil service.

So, Mr. Stier, the last question I have here, in 20 seconds, why is a nonpartisan civil service so important? How does politicizing the Federal work force undermine national security?

Mr. STIER. We have a history in our country where we had the spoil system before in the 19th Century. You wound up with corruption and incompetence. You see that globally whenever you have a system move away from merit with respect to the civil service.

You see poorer performance in the Government and you see corruption. So, it is not the right way to move. We do need to reform our Government. That's not the reform we need.

Just a point of order, and I normally don't do this, it's Stier, just to let everybody know so we can maybe going forward do it—

Mrs. RAMIREZ. Thank you, Mr. Stier. I take that very personally and the Chairman—

Mr. STIER. Yes, I'm sure.

Mrs. RAMIREZ [continuing]. Knows too, so I apologize for that.

Mr. STIER. No problem, not at all.

Mrs. RAMIREZ. Thank you.

With that, I yield back.

Chairman GREEN. The gentlelady yields.

I now recognize the gentleman from Arizona, one of our border States, Mr. Eli Crane for his 5 minutes of questioning.

Mr. CRANE. Thank you, Mr. Chairman. I appreciate the opportunity to be here today and talk with some subject-matter experts about the pipeline of our cyber force and how we are going to compete with some of the threats as we see some of our adversaries increasing cyber attacks on the country.

I just came from an oversight committee and now I am back here and it is really the same nonsense going on in there. I just want to say to Elon Musk, wow, man, you are really effective because these guys are completely melting down. You must be doing something right.

I think we might need to request some of your funds to get these guys maybe some pallets of tissues, some safe spaces, maybe a couple therapy dogs, because they are absolutely melting down. So, good job, Elon.

Now, I want to cover something that Mr. Swalwell said a couple seconds ago. Mr. Swalwell talks about—he talked about the responsibilities to protect the American people because this President pardoned the J6 prisoners, many who had been in prison for several years.

It is just funny because I didn't hear that same concern from Mr. Swalwell or many of the Democrats on this committee when then President Biden was allowing hundreds of thousands of illegal aliens, many of whom were criminals, rapists, and murderers and terrorists coming into this country on a monthly basis. So, my point being is if you want to protect Americans you can't just do it when it is politically advantageous.

I want to start with you, Dr. Russomanno. As the executive vice president of academic affairs at Memphis and the former dean of engineering at Purdue University, I am sure you were well-versed on developing the cyber work force. My question is how is the University of Memphis utilizing programs like CyberCorps Scholarship for Service programs to build out the pipeline of the Federal cyber warriors?

Mr. RUSSOMANNO. Thank you, Congressman Crane, for your question. I think it's important to remind everyone what CyberCorps is all about and how it impacts students.

One is covering tuition. Another is providing a stipend that enables students not to have to work while they're pursuing their degree. Another is an opportunity to build social capital through networking, through internship fairs and other opportunities to learn more about the Federal Government and a way they can make an impact through cybersecurity.

This is a tremendous enabler, if you will. We've talked about how do we get more of our youth involved in cybersecurity? Certainly helping them through their daily living is a fundamental way so they can focus on their studies to help our Nation.

Mr. CRANE. Thank you.

Next question for Mr. Rashotte. According to the U.S.-China Economic and Security Review Commission, the cybersecurity school at the Wuhan-based National Cybersecurity Center, plan to build 4 to 6 cybersecurity schools by 2027.

The CCP has devoted significant resources to building their cyber force and while the exact number of cyber warriors isn't available, it is safe to estimate that if the CCP issued a directive it could bring a significant cyber force to bear against the United States, especially given that according to U.S. Cyber Command there are only 6,200 personnel across 133 teams working on cyber threats in CISA and DHS was roughly 3,100 employees.

My question is how can academia, private industry, and the Federal Government partner together to ensure our cyber work force pipeline is able to keep pace with the number of cyber warriors our adversaries can churn out?

Mr. RASHOTTE. Thank you for the question. I think that the partnerships between industry and academia are critical and our approach has been to break down every barrier we can in terms of access to training and education.

We've done that at Fortinet by making our entire catalog of training available free to anyone who needs that training, and we've challenged others to do the same.

Mr. CRANE. Thank you.

My next question is for you, Mr. Jones. How important is it to utilize American resources within our power grid so that our adversaries aren't getting a foothold in our critical infrastructure, similar to Volt Typhoon hack? I was recently watching the Shawn Ryan show. The topic was we are in an invisible war with Erik Bethel.

My question is, and I am paraphrasing from the show, how can companies who have a fiduciary responsibility to their investors to gain and seek profit balance that financial responsibility with other factors like patriotism?

Mr. JONES. Well, I think that the electric cooperatives in our country have a rich history of patriotism, Congressman, so I think we do take that seriously. You know, the virtues of our mission service, making sure that we are doing our part to provide reliable power for now almost 50 million Americans, and that's always held the line for us.

Mr. CRANE. Thank you.

Mr. Chairman, can I enter this into the record? I know there has been some discussion here about layoffs and buyouts. This is an article, "CISA among DHS offices exempted from taking OPM's deferred buyout offer".

Chairman GREEN. Without objection, so ordered.

[The information follows:]

ARTICLE FROM NEXTGOV/FCW SUBMITTED BY HON. ELIJAH CRANE

CISA AMONG DHS OFFICES EXEMPT FROM TAKING OPM'S DEFERRED BUYOUT OFFER

By David Dimolfetta / January 31, 2025

President Trump's DHS chief said she wants to scale back the cybersecurity agency's size and mission scope.

At least two offices in the Department of Homeland Security were told Thursday that they are not allowed to take a deferred buyout offer from the Office of Personnel Management that was sent to the Federal workforce earlier this week, arguing that their positions are vital for national security purposes.

Those bureaus include the Cybersecurity and Infrastructure Security Agency, as well as Customs and Border Protection, according to multiple people familiar with the matter and email notifications obtained by Nextgov/FCW.

The exemptions are not a total surprise. The Trump administration's deferred resignation offer email sent to Federal workers earlier this week said the proposal is available to all government employees except "military personnel of the armed forces, employees of the U.S. Postal Service, those in positions related to immigration enforcement and national security, and those in any other positions specifically excluded by your employing agency."

Bridget Bean, who's serving as acting director of CISA, told the cyber agency's employees in an email that "per guidance from DHS Management, CISA employees are not permitted to participate in the Deferred Resignation program."

Email correspondence to CBP employees sent Thursday showed the exempted positions are "considered national security." It adds that relevant staff should "be aware that no further processing actions will be completed for a deferred resignation on your behalf" if they previously accepted the proposal. It was sent by Acting Commissioner Pete Flores and Acting Deputy Commissioner John Modlin.

Nextgov/FCW has reached out to DHS spokespeople for comment.

The offer for feds to continue to be paid until Sept. 30—provided they resign by Feb. 6—was emailed to every Federal worker Tuesday evening, seemingly via a new email server installed at OPM in recent days that gave the Trump White House the capability to reach some 2.3 million Federal civilian employees. On Thursday, OPM sent a follow-up email with a list of Q&A notes encouraging employees to take the offer.

The exemption notices demonstrate how agencies and their leaders are taking different approaches to the severance program. But CISA being among them is notable because the Trump administration has vowed to reduce the size and scope of the cyber agency.

CISA has historically enjoyed bipartisan support from members aligned on the notion that cybersecurity is a national security concern and shouldn't be mired in politicization. But some Republican claims that the agency's misinformation efforts have targeted conservative voices in the past 2 years, as well as a second election win for Trump, are setting the agency on a course for potentially far-reaching reevaluation.

DHS Secretary Kristi Noem recently said the cyber agency needs to be smaller and more nimble, and that it should cease its work on calling out misinformation and disinformation that propagates across social platforms. Trump has not yet nominated leadership for CISA.

The Cyber Safety Review Board—a DHS investigatory body stood up through a Biden-era cybersecurity executive order to probe major cybersecurity incidents—was cleared out of at least its non-government members early last week as part of a DHS-wide push to cut costs under the Trump administration.

Nextgov/FCW Staff Correspondent Alexandra Kelley contributed to this report.

Mr. CRANE. Thank you. I yield back.

Chairman GREEN. The gentleman yields.

I now recognize the gentlelady from New Jersey, Ms. McIver for her—oh, wait. Are you—I didn't see this. I didn't see. Mr. Magaziner snuck in on me so if we will defer is it OK?

I will recognize Mr. Magaziner for his 5 minutes of questioning, and my apologies.

Mr. MAGAZINER. Thank you, Chairman. We are here today because we all care about cybersecurity, or at least I thought we all did. Last week, Donald Trump's Office of Management and Budget illegally cut off funding for grants across the Federal Government, including grants for cybersecurity.

This is a memo that was sent from the Department of Homeland Security to States that outline DHS grants that were being cut off for review, including but not limited to the Cybersecurity Education and Training Grant, cut off; the CISA Cybersecurity Awareness Grant, cut off; the Cyber Tip Line, cut off; State and local cybersecurity grant, cut off pending review per OMB instructions. Review for what?

Is cybersecurity too woke, too green? It was only after an enormous public outrage and a Federal court order that the Trump ad-

ministration pulled back that OMB memo. During those days when this funding was frozen, China was continuing to put thousands of people a day in cyber warfare against the United States, to say nothing of Russia and Iran and criminal gangs.

But that is not all. The Federal funding hiring freeze is impacting cybersecurity jobs all across the Federal Government, and I want people to hear this. There are Federal cybersecurity jobs, not just at CISA or DoD, but in every agency.

So cybersecurity jobs at the U.S. Treasury, hiring freeze, cybersecurity jobs at HHS, which manages Medicare, Social Security, CMS, cut off. Critical agencies are impacted by this hiring freeze.

We heard a letter earlier from Mr. Stier from a CyberCorps participant whose job in the Federal Government, his cybersecurity job, was rescinded due to Trump's hiring freeze, which is still ongoing. Agencies all across the Federal Government are not able to make these crucial cybersecurity hires across the board almost.

So to my Republican colleagues, if you care about cybersecurity and I am serious about this, call the White House. Call the White House right now and tell them to lift the hiring freeze of cybersecurity roles across the Federal Government, not just at CISA, not just at DoD, but at every agency.

Let's address the elephant at the room. This weekend Elon Musk sent a group of unvetted 20-year-olds to take over the U.S. Treasury's payment system responsible for tax refunds, Social Security checks, Medicare benefit payments, and more. The Treasury's payment system has the names, Social Security numbers, bank routing numbers, and tax information of every American, medical information of millions of Medicare recipients.

We have no idea who these children are that Elon Musk has working for him who now have access to the private personal data of every American. We don't know what permissions they have. Can they just read the data? Can they edit it? Can they initiate payments? Can they cut off payments at will? Can they share your personal data with people outside the Federal Government?

The one thing we know about this army of children that Elon Musk has poring through your data is that not one of them has been through a Federal FBI background check. Other than that, we don't know very much.

Oh, by the way, we just learned through public reporting that Elon Musk has put a private server in his office and has downloaded every American's personal data into that private server.

So, I invite any of our panelists, any of the 4 of you, to defend this. Are any of you comfortable with Elon Musk and this staff of untrained, unvetted, unelected, unconfirmed teenagers having access to every American's personal data with no transparency or oversight? Does anyone want to take a stab at defending that?

Well, that silence I think gives us the answer that I was expecting at least. Does any of our panelists think that the Trump administration freezing hiring of cybersecurity roles in agencies across the Federal Government help our national security? Of course not.

So, listen, if we are going to have conversations about cybersecurity I welcome it, but it needs to start with the administration tak-

ing steps to protect the private data of Americans, to lift the hiring freeze of cybersecurity professionals, and to stop giving our adversaries win after win after win in the cyber domain, as they have been over the last 2 weeks.

I will yield back.

Chairman GREEN. The gentleman yields.

I would like to—I don't normally do this and save my comments on this one until the end, but 19-year-olds aren't children. We have Medal of Honor winners who have fought and died for this bleeping country who are 19-year-olds. So, if you're 19 years old out there I don't consider you a child.

I now recognize Ms. Greene from Georgia for 5 minutes of questioning.

Ms. GREENE. Thank you, Mr. Chairman. Thank you for clearing that up. There are 19-year-olds that are serving our country and defending our Nation. We believe in merit. We believe in people that can do the job.

That is why America elected Donald Trump this past election and part of his campaign was DOGE and Elon Musk. They were on the campaign trail together, as a matter of fact, the last 2 months of the campaign and America overwhelmingly voted for this effort.

I'm so happy that we are talking about cybersecurity and cyber professionals today.

Mr. Stier, in your testimony you talk about maintaining nonpartisanship as a bedrock principle of civil service. You wanted to talk about nonpartisanship meanwhile your \$24 million nonprofit dedicated to attracting talent for the Federal work force and making the Government more effective is funded by some of the most progressive benefactors. This includes the Gates Foundation, the Democracy Fund, and the Ford Foundation. It also hosts galas to honor people like Lisa Monaco and other Biden officials.

A goal of your entire organization is essentially de facto job placement to entrench more DEI hires into the Federal work force, the opposite of nonpartisan, apolitical, merit-based civil service.

Diversity, equity, and inclusion is a huge priority for the partnership, as listed on your website. Listed on the website is a framework to integrate the principles of diversity, equity, and inclusion into the partnerships, programs, initiatives, and strategies.

Since the nonprofit's main initiatives are helping people apply for Federal roles in advancing career development in the Federal work force, your nonprofit is aimed at infusing DEI, an inherently partisan practice into the Federal work force.

I worry about this especially with regards to the cybersecurity work force who needs high-quality, skill-based positions such as those serving on DOGE. Cybersecurity is extremely important. It shouldn't be about race. It shouldn't be about sexuality. It shouldn't be about identity.

In your testimony you also expressed concerns that President Trump's administration's recent actions and that they will counter democratic principles, yet your unwritten goal of entrenching more woke employees into the swamp is the opposite of democratic principles.

The Trump administration's actions are the embodiment of democratic principles. This is what the American people want. This is what they voted for.

The American people overwhelmingly voted for President Trump in a decisive landslide victory to reform how our Government operates, most importantly, how the Federal work force operates. The mission of your partnership is building a better Government and stronger democracy. Building a stronger democracy is allowing the will of the people to take effect, not actively working to oppose it.

There have been multiple reports that you were in communication with the officials at the Biden administration prior to President Trump taking office. Is that true?

Mr. STIER. We run the Center for Presidential Transition so we've helped the Trump campaign when they were trying to set up their transition operation in 2016. We've helped every administration get set up right, both Republican and Democratic. Yes we've been in contact with the Biden administration. We've had an open door to everybody.

If you would like to have the facts, I can provide those to you but let me know because the reality is we do honor civil servants not political appointees. The program that you identified on Lisa Monaco, she was presenting an award as smart political leaders should——

Ms. GREENE. Thank you, Mr. Stier. I will reclaim my time.

Mr. STIER. But let me know when you ever want me to——

Ms. GREENE. Thank you.

Mr. STIER [continuing]. The facts for——

Ms. GREENE. Did you discuss any strategies for how to prevent President Trump from firing Federal workers?

Mr. STIER. I'm sorry, in what context?

Ms. GREENE. Did you discuss any strategies for how to prevent President Trump from firing Federal workers?

Mr. STIER. In what context? I do not think that it's a good idea to offer the entire work force non-strategically an opportunity to resign and to press them to do so because you're going to lose cybersecurity professionals that you don't want to lose. If you want to have——

Ms. GREENE. DEI? DEI professionals? Are you trying to stop President Trump's administration from hiring——

Mr. STIER. We are not engaged——

Ms. GREENE [continuing]. DEI employees that you placed in the Federal Government?

Mr. STIER. We are not engaged in trying to stop anyone from getting fired because that's not the role we play. What we do say, though, is when civil servants—let me finish the answer.

Ms. GREENE. Well, Mr. Stier——

Mr. STIER. Let me finish the answer.

Ms. GREENE [continuing]. Let me ask you one last——

Mr. STIER. You asked me a question.

Ms. GREENE. I have a few——

Mr. STIER. Excuse me, Mr. Chairman? If I'm asked a question do I get to answer it?

Chairman GREEN. It is her time. She can claim it.

Mr. STIER. OK. Then go ahead and go ahead.

Ms. GREENE. I would like to reclaim my time. Thank you, Mr. Stier.

Mr. STIER. Thank you.

Ms. GREENE. Does your organization receive taxpayer dollars?

Mr. STIER. Do we receive taxpayer dollars?

Ms. GREENE. Yes.

Mr. STIER. We provide services to the Government so we do receive taxpayer dollars on the—

Ms. GREENE. Right. I have \$3.4 million right here from the American taxpayers. They are not interested in DEI, Mr. Stier. They are interested in qualified people.

Thank you—

Mr. STIER. And we provide qualified—

Ms. GREENE [continuing]. Mr. Chairman. I yield back.

Chairman GREEN. The gentlelady yields. I now recognize Mrs. Johnson or wait, Ms. McIver. I didn't get you before. Thank you.

The gentlelady from New Jersey for 5 minutes of questioning.

Ms. MCIVER. That is OK. Thank you, Mr. Chairman. Thank you, Chairman, thank you Ranking Members, and thank you to the witnesses for joining us today.

I was a little caught up in that last questioning trying to bring myself back. So, as we face an evolving and increasingly sophisticated cyber threat landscape, our Nation's security relies on a robust, well-trained, and diverse cybersecurity work force. Unfortunately, the recent decisions, as mentioned multiple times here, including the harmful hiring freezes and Federal grant interruptions under the Trump administration, have weakened the critical pipeline needed to safeguard our digital infrastructure.

Last time I checked the offering of folks to take a buyout wasn't just offered to folks of diversity or women or disabled. It was offered to all employees so it is not about just laying off DEI or employees that are woke because everyone got this offer to be able to take a buyout.

These policies have stalled critical recruitment efforts, delayed hiring of qualified candidates, and created vulnerabilities that will persist.

Adding to this damage are the extreme rollbacks in diversity, equity, and inclusion initiatives which are crucial for addressing the long-standing representation gaps in this field. By limiting opportunities for women, people of color, and unrepresented communities to enter and advance in cybersecurity, we are missing out on a vast pool of talent.

With that being said, Mr. Stier, I would like to go back to you and give you some time to address some of the things you were talking about in the previous question, but more so to talk about how in your opinion these specific hiring freezes hinder the development and retention of cybersecurity expertise across all of our Federal agencies?

What steps, in your opinion, can Congress take to reverse or reduce the long-term impact, because there will be, of these policies on our national security?

Mr. STIER. Well, look, as we've talked all along here and as the committee both Republican and Democrat recognize, we're in a hole and the world is getting more scary, not less. So, the reality is we

need to see more investment in the capacity of our public sector to respond to the cyber challenges.

When you have hiring freezes that actually encompass the cyber work force, of course that's going to diminish capacity of the organization. That's a pure logical proposition.

The reality is that CISA is under a hiring freeze, even though the offer of, you know, delayed or deferred resignation is not being presented to them, so it is harming CISA but more importantly it's harming every organization inside the Federal Government that needs cyber talent in order to protect vital interests of our country.

So, this is an issue that is not just about the hiring freeze. We have to be thinking about the morale more broadly of the work force and that is not good. In terms of responding, I just want to say that, you know, I'm invited to testify here. I'm trying to offer the best information I possibly can to this committee and, honestly, I'd like to be treated with respect. I don't think I was.

Ms. McIVER. Thank you. Thank you for that and I am sorry that you were not able to experience that. I think as human beings and as just grown-ups, what we are supposed to be, we should be able to treat each other with respect and be respectful and allow you the time. That is why I wanted to give you time to talk about that—

Mr. STIER. I appreciate that.

Ms. McIVER [continuing]. And I am thankful for your organization and the work that they are doing and not, you know—I know it is very hard being in this type of, you know, situation and addressing some of the things where people want you to be anti-people of color, anti-women, anti-, you know, against people with disabilities.

But at the end of the day I commend you for everything that you are doing and know that the day will be better after this hearing.

So with that, I yield back my time. Thank you.

Chairman GREEN. The gentlelady yields.

I now recognize the Chairman of the Subcommittee on Cyber, the gentleman from New York Mr. Garbarino.

Mr. GARBARINO. Thank you, Mr. Chairman. Thank you very much for having this hearing and very excited to support the PIVOTT Act. I know you read a couple names off of the co-sponsors. I guess we didn't put our paperwork in, but we are going to be filing that right away so we are going to be—

Chairman GREEN. OK, be glad to have you on the bill.

Mr. GARBARINO [continuing]. Co-sponsors so I am sorry we didn't get that in soon enough. That was our fault.

But thank you all to the witnesses for being here.

Mr. Rashotte, shot, which one is it?

Mr. RASHOTTE. Rashotte.

Mr. GARBARINO. Rashotte. Wonderful, thank you. I wanted to focus. In your testimony you identified early educational engagement is essential, not only to growing the cyber work force but also making students and families aware that these careers exist to begin with.

Last year I led a DHS Cybersecurity Internship Program Act with Congresswoman Clark, and we were very proud of that bill. How do you think we can look to improve outreach to draw stu-

dents and the public at large to these opportunities in cybersecurity?

Mr. RASHOTTE. Yes, I think we need to start as young as we possibly can. I know when we started our efforts in providing K to 12 education and curriculum, we didn't think we'd be able to start as young as we could. We had teachers coming to us and say that we could provide cybersecurity awareness training at kindergarten.

That really surprised us, but it's been incredibly effective. So, I think there's a long game here where we really have to focus at that young of an age so that truly when kids are coming home and talking about becoming doctors, lawyers, engineers they're also talking about becoming cybersecurity superheroes.

Mr. GARBARINO. So, when you talk about kindergarten, what, kind-of, is happening at kindergarten to get students in it?

Mr. RASHOTTE. So, we're providing lesson plans to teachers so that we're not adding additional lessons but we're taking existing lessons that teachers are providing and adding cybersecurity aspects into it, so basically helping kids understand, you know, what might be a threat, just opening their eyes.

Mr. GARBARINO. Would it be helpful do you think if CISA validated cybersecurity curricula for K through 12?

Mr. RASHOTTE. I think our main focus right now is developing that curriculum by teachers for teachers and that's been our approach at that level.

Mr. GARBARINO. But does CISA have a role in helping develop that curriculum?

Mr. RASHOTTE. I think there definitely could be a role for sure, yes.

Mr. GARBARINO. Do you know if currently under the Department of Education. U.S. Department of Education if there are any cybersecurity roles that they play in helping States to develop curriculum for cybersecurity?

Mr. RASHOTTE. It's not an area that I've focused in. Our partnerships from within my organization, the training institute, have been more directly with the academic institutions and their role.

Mr. GARBARINO. OK. So, K through 12 is big but what about expanding cyber education? What else can we do with expanding cyber education after K through 12?

Mr. RASHOTTE. I think we can take programs that have historically been focused at colleges and universities and start to move those downstream into high schools and there we're starting to see a lot of kids now coming out of high school that are essentially self-taught and are going directly into the work force.

I think if we take some of those programs that we've traditionally focused at college and university, they can definitely be applied at the high-school level and make sure that those kids coming out and going directly into the work force are even more prepared than what they are.

We're seeing some of these self-taught kids extremely capable and qualified.

Mr. GARBARINO. That is great. I mentioned that the Chairman's PIVOTT Act and how that helps with the scholarships and getting people into the work force but, you know, there are a half a million open cybersecurity jobs at least now nationwide.

What can we do to get people into there? Is there training programs? Is there certification programs that people can start now that they don't have to wait to do 2 years in college because that is necessary, but is there something to get people in the work force now?

Mr. RASHOTTE. Absolutely. Again, I think this is, we see this again with kids coming out of high school directly into the work force, a lot of self-training going on.

A lot of corporate entities, such as Fortinet, we're making our training and certification freely available so that kids either coming out of the degree program or coming directly out of high school can access that training with minimal barriers and in some cases no barriers at all.

Mr. GARBARINO. Thank you very much.

Dr. Russomanno, you talked about in your testimony about the challenges colleges face in aligning education and work force needs. Coming from higher education, how can we promote skills-based training and modernize degree programs to address this gap?

Mr. RUSSOMANNO. Well, thank you for that question. You know, as part of our Polytechnic Initiative at the University of Memphis we also have benefit of having our own Independent School district. We have a pre-K through 12 Independent School district associated with the university.

So we're working very hard on expanding our dual enrollment focusing on cybersecurity, applied AI, and advanced manufacturing. There's a lot of technology that goes into advanced manufacturing that many students are not aware of, you know, the advanced robotics, the sensors, the cybersecurity, the AI.

So trying to get that penetration into the high schools through dual enrollment is part of a focus for us at the Polytechnic Initiative at the University of Memphis. Hope to partner with others.

Mr. GARBARINO. Thank you, Chairman. I yield back.

Chairman GREEN. The gentleman yields.

I now recognize the gentleman from New York, our Nation's one of our really our financial center, our greatest financial center, obviously very concerned about cyber, Mr. Goldman for 5 minutes of questioning.

Mr. GOLDMAN. Yes, Mr. Chairman, thank you very much. I agree those in New York City and around the country are very concerned about cyber.

We must be operating in la-la land here having a hearing on "Preparing the Pipeline: Examining the State of America's Cyber Work Force" where we have 3 academics who have been brought in by the majority to talk about the education and training that we need for more cybersecurity employees, while at the same time the President and his unelected billionaire master are gutting every single Executive branch agency. What's the point of having a pipeline with education if you are taking away all of the jobs?

If you are sending unvetted teenagers with no security clearance into our various Executive branch agencies, allowing them to hack and slash into the Government payment systems, the Government portals, the Government databases without any regard to cybersecurity, putting them on private servers and quite obviously to anyone whether you are an expert on cybersecurity or not, you under-

stand how that jeopardizes the security of every single American's personal identification information.

It provides an opportunity for China, who just executed the largest cybersecurity breach of the Federal Government ever a couple months ago, to have access to private servers that are so clearly easier to hack into.

We have no idea whether these people have security clearances, whether they got their security clearances because Donald Trump passed an Executive Order saying that he can just bestow security clearances on anyone for 6 months. So maybe he did that.

I mean, maybe it is the same thing as Kash Patel saying that Donald Trump thought about declassifying Classified information and therefore it is declassified and that is going to be potentially the new FBI director who is going to oversee counterintelligence and cybersecurity for the FBI.

This is the guy who supports the purges at the DOJ and the FBI, who promised the purges at the FBI and DOJ, who lied right, left, and center during his hearing, who has circumvented normal protocol and practices when he was with the National Security Council, when he was with the House Intelligence Committee, when he was with the Department of Defense, who every single former Trump administration official has said is wholly unqualified and dangerous to be in that job, and you want to talk about cybersecurity and recruiting more people.

How about we not have heads of Executive branch agencies who are jeopardizing our own cybersecurity, who are jeopardizing our own security? How about having some degree of protection over our personal identification information?

Who on earth would ever want to join the Federal Government now? If you are associated with a prosecution that the President of the United States does not like, you will be fired. You will be fired.

What law enforcement system in a democracy allows or supports the President of the United States to order the firing of non-partisan, highly-trained law enforcement officers simply because they worked on a case that the President didn't like? That is banana republic shit, and that does not belong in this country.

What else doesn't belong in this Congress is this stupid hearing where we are talking about educating a work force where there is no demand for that work force anymore because Elon Musk is destroying that work force.

It is like we are in la-la land, Mr. Chairman. You are pretending as if reality is not happening down the street and we need more education for cybersecurity. This is a joke.

I hope at least, Mr. Chairman, if you are going to have hearings on cybersecurity—

Chairman GREEN. The gentleman's time has expired.

Mr. GOLDMAN [continuing]. That you will at least—

Chairman GREEN. I now recognize Mr. Ogles for 5 minutes of questioning.

Mr. OGLES. I want to thank you, Mr. Chairman.

Thank you to the witnesses, a couple of fellow Tennesseans there.

Mr. Jones, you know, you represent Middle Tennessee Electric, who actually services part of my district.

But before we get to that I do want to put you back on something that you said, Mr. Chairman. One of our colleagues said somewhat of a disparaging remark about 20-year-olds and so as we look to bad actors, whether it is nation-states or criminal activity, the development of applications such as TikTok which have a back door, the capability of assimilating data, new technologies such as DeepSeek, you know, we know that there is a gap. We have half a million openings in the cyber space that, by the way, that is the equivalent to our standing United States Army currently.

So the future is 16-, 17-, 18-year-olds, the future work force. When I say future work force I am just talking about a year or 2 from now. The work force of today that we need to engage are those 18-, 19-, and 20-year-olds, right? That is how we fill this gap.

So to someone to have some disparaging remarks about an age range that is literally critical to backfilling this need is really naive and reckless, I would say, Mr. Chairman, but on point.

Mr. Jones, again, and to all of you for being here. You know, obviously recruitment is a problem. You have got the urban versus rural competitiveness, right? You have got private versus Government. But the reality of the space we are in is that we have half a million jobs that need to be filled.

Mr. Jones, what can be done to better equip and, quite frankly, leverage the work force of today as we fill the pipeline with those 16-, 17- to 20-year-olds, Mr. Jones?

Mr. JONES. Congressman, thank you. So, you know, I'll point to the PIVOTT Act first. Again, I think that's so fundamentally important and we're appreciative of what is happening with regard to that so that's an important part of it.

As far as the work with electric cooperatives, we are really good at collaborating together and by extension we are seeking to collaborate with educational institutions at the local level. So, I think that's important, too.

We can provide, for example, mentorships for people, and again, the challenge is not quite the same, as you are aware for Middle Tennessee Electric as it may be for many other electric co-ops in more rural areas with a few less economies of scale. So, the challenge is different from place to place.

But I believe that our network, our association of cooperatives stands ready to provide something like you're describing to with regard to mentorships, but particularly with regard to engagement with educational institutions in our communities.

Mr. OGLES. Well, and I want to focus on that for just a moment. You know, so your industry, your space there is collaboration amongst the cooperatives. You are working to fill your needs in your industry, I think, so the solution here, you know, the scariest phrase in the English language was from Reagan. He said that, "I'm from the Government and I'm here to help."

So part of the solution is, obviously, what the Chairman is bringing forward, the PIVOTT Act. It is industry working together to work with those educational institutions. So as we move forward it is us working together to identify the needs and so this is eco-

nomic in nature, right, for local communities, for our greater national economy. Obviously, the battlefield of the future is cyber.

So, you know, and otherwise benign industries or spaces such as the electric cooperatives, such as hospital systems, we see China and bad actors and nation-states wanting that information, wanting to see if there is a capability to weaponize that against the American people.

So to play games and to talk about nonsense while this is an important topic that we have to have, as we see advances from other countries and nations as they recognize the need for this and to enhance capabilities, it is really frustrating but I thank you for what you are doing in your space.

Mr. Jones, you touched on human behavior in your testimony. So, you have a dynamic scenario where you have students that can access your system, faculty, young and old, some of them may not be quite as adept technologically speaking, part-time employees. So how do you create access whilst having compliance and security when you are looking at your systems? Of course, that applies the best practices of the universities and cooperatives, et cetera.

Mr. RUSSOMANNO. Yes, thank you for your question.

Mr. OGLES. Mr. Russomanno, it is for you.

Mr. RUSSOMANNO. Even though the CIO is really primarily responsible for this area, I would say that we are doing a lot with a variety of phishing drills and other internally generated vulnerability scenarios to try to improve internally the knowledge base of our faculty, our staff, and our students to ensure this critically important data, whether it's student data, research data, the comprehensive mission of the university, that we're doing all we can internally with a variety of mock drills to ensure we are employing best practices.

Mr. OGLES. Yes, sir.

Mr. Chairman, I exceeded my time. I yield back and thank you, sir.

Chairman GREEN. The gentleman yields.

I now finally get to recognize the gentlelady from Texas, Mrs. Johnson. You are recognized for 5 minutes for questioning.

Mrs. JOHNSON. Thank you, Mr. Chairman. I just want to say it's an honor to be on the committee.

We have a great panel. You are all very impressive in your comments. What I am hearing from you is we are in a cybersecurity crisis in this country and that we are in a cybersecurity crisis because we have a work force that is severely diminished.

We have lacked educational preparedness. We are lacking a plan to recruit and develop the best and the brightest talent from every corner, from black kids, brown kids, women, Asian kids, diversity, equity, and inclusion. We need all the kids on this fight, is that correct? All of them.

So one of the things that has not been discussed about today that I am very concerned with, well, another point that you have all highlighted is the need for a definite more robust cyber education plan to reach into high schools, to reach into colleges, to create internships.

We have CyberCorps, which is a great program, but it needs to be enhanced but it is an educational program. So, I am very con-

cerned in light of the backdrop of what we have already seen over the last 2 weeks of shuttering our Federal work force, shuttering USAID, intimidating our law enforcement, intimidating cyber enforcement personnel, but we haven't even talked about what Trump plans to do with the Department of Education.

The *New York Times* is reporting he is planning to shutter it, too. So, I assume that you all agree with me that if the Federal Government dismantles the Department of Education that could have catastrophic implications to the security and the safety of this country. Would any of you disagree with that?

You know, I think that is really important for the American people to realize that this is not politics. This isn't theater. This is the foundational premises of our security.

Mr. Jones, I want to ask you a question. I am a Texas Democrat. I have a grid in our State that is messed up, that has failed, and I lived through a situation where our grid failed for 10 days and hundreds of people died and businesses suffered mightily and people suffered mightily.

As a rural electric co-op you provide critical infrastructure to millions of people in this country. You provide power. Hopefully, you will provide broadband, but opportunity, which I believe is a critical infrastructure as well, but how devastating would it be to your co-ops for a cyber attack to shut down your grid?

Mr. JONES. Well, it's something we think about a lot and I recall, of course, the situation you're describing from 3 winters ago, I believe it was in Texas.

Mrs. JOHNSON. Correct.

Mr. JONES. Of course, that was many things went to that. Not a cybersecurity incident but that wasn't your point. But I mean, it's, you know, we want to keep the lights on. That's what we're here for.

Our members depend on us and so this subject is so important for us for that reason, so we're putting in place as best we can resources, processes, technology, to make sure that we are doing our part. But this is bigger than us and that's why we're here, too. So, we welcome this conversation.

Mrs. JOHNSON. Right and I welcome this hearing, Mr. Chairman. Mr. Chairman? Because I do think that cybersecurity is one of the biggest vulnerabilities of our country and it is the new frontier of security and threat.

It is really frightening and scary to many people out in this country the fact that the Trump administration is doing everything it can to undermine the confidence in the cybersecurity work force that we have in this country by dismissing employees, by shuttering and hiring freezes, by dismissing the Department of Education, by doing all of the things, by undermining the CIA, by undermining the FBI. To prevent cyber crime in this country we are in a critical mass.

Mr. Stier, I want to go back and give you an opportunity on DEI. We need everyone. DEI is about reaching kids who have not been adequately reached in the past and giving them opportunity to see the light. We need to do that, right?

Mr. STIER. There's no doubt that we need to pull from talent where we can find it everywhere. I think really, quite importantly,

we need to create environments in any workplace that enable people to do their best and that's how you get better performance.

So, that is a basic proposition. We ought to be doing good management in Government just like we should see good management everywhere.

Mrs. JOHNSON. Thank you so much.

Mr. Chairman, I yield my time.

Chairman GREEN. The gentlewoman yields back.

I recognize the gentleman from Alabama, Mr. Strong for his 5 minutes of questioning.

Mr. STRONG. Thank you, Mr. Chairman.

Mr. Russomanno, I recently introduced legislation, the CyberCorps Enhancement Act, to extend the visiting CyberCorps Scholarship for Service program's participation period from 3 to 5 years allowing local colleges and universities to continue to produce highly-trained cybersecurity experts.

As you know, local colleges and universities, including the University of Alabama in Huntsville, affectionately known as UAH in my district, leverage these programs to recruit, retain, and place highly-skilled cybersecurity experts with an average ACT test score of a 28.5 where 80 percent of the graduates remain locally after graduation.

In fact, UAH has the second-highest number of participants and graduates in the program submitting north Alabama leadership in cybersecurity education. This will pay dividends for the FBI Cyber Threat Division that is locating in Huntsville as we speak.

Mr. Russomanno, can you discuss the benefits of expanding the participation period to enable students to pursue advanced degrees?

Mr. RUSSOMANNO. Yes. Thank you for your question, and we've enjoyed the opportunity to partner with UAH in the past.

Yes. This is a multi-prong opportunity for us. In any way that we can offer opportunities to all students, and I definitely agree with all students, and how we then commit ourselves to a successful student outcome.

I think the expansion of eligibility in terms of number of years, also the opportunity for the delayed service commitment to provide an opportunity to either pursue a baccalaureate degree or an advanced graduate degree, I think those aspects of both the CyberCorps and potentially the PIVOTT Act are critically important.

You know, many times students are looking not only for that first job but a satisfying career progression that provides opportunity for added responsibility. I think what you cited provides an opportunity to do just that. Thank you.

Mr. STRONG. Thank you. I also want to mention we have a State-wide cyber high school located in the second-largest research park in the United States in Huntsville, Alabama. It is another level of starting this progression so that we can bring more to colleges and universities.

As we have covered, the Chairman's Cyber PIVOTT Act and my CyberCorps legislation, both aim to strengthen the cybersecurity work force pipeline. How would these programs complement each other to address the current cybersecurity talent shortage?

Mr. RUSSOMANNO. Well, in my opening remarks I talked some about some of the challenges around transfer matriculation, so I think we have some opportunities to improve smooth pathways for advancement.

So, if you look at technical schools, community colleges, there are some challenges in getting the knowledge and skills and abilities acquired through those programs to matriculate to 4-year universities. So, that's an opportunity for improvement for us.

Mr. STRONG. Thank you. In addition to this legislation what more can we do to ensure we recruit and train future generations of cybersecurity experts in the United States?

Mr. RUSSOMANNO. Once again, I think it's the partnerships that have been talked about here today, a steadfast commitment on partnerships between the public and the private sector. I think we all ultimately have the same goal here, provide opportunities for students that make an impact to improve the safety and security of our Nation.

Mr. STRONG. Thank you. I also wanted to touch on the pay differences between cybersecurity professionals in Government and the private sector. In your opinion, what more can we do to recruit and incentivize the best of the best cybersecurity professionals to stay in Government and to contribute to protecting our Nation's security from adversaries and those who look to harm America?

Mr. RUSSOMANNO. Once again, I think that opportunity for pursuing continued education while a civil servant is critically important, whether that's a Baccalaureate degree, a Master's degree, even a Ph.D. Having those opportunities within the Government, I think, would be very attractive in terms of retention.

Mr. STRONG. Thank you.

Mr. Jones, first, I want to commend you. I am very familiar with your power system. We have evaluated Winchester in that area and it had been very beneficial years ago when I was the county commission chairman in Huntsville, Alabama.

The energy sector has been described as an enabling function for all critical infrastructure sectors, making it one of the most vital and one of the most targeted. Knowing this, it is of no surprise that the energy sector was targeted by Volt Typhoon.

Mr. Jones, given the increasing cyber threats to energy infrastructure how can Federal work force initiatives better support the utility industry in developing skilled cybersecurity professionals? What role should public-private partnerships play in that effort?

Mr. JONES. Congressman, thank you. So I think again the PIVOTT Act and the virtues of that, deepening the talent pool. We need, you know, more not fewer resources so I think that's the essence of what I would suggest in the limited time. But happy to be a partner with you.

Mr. STRONG. Yes. I want to thank each of the witnesses for being here.

Chairman Green, I yield back.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Hernández, is that right—

Mr. HERNANDEZ. Yes.

Chairman GREEN [continuing]. For 5 minutes, the gentleman from Puerto Rico.

Mr. HERNÁNDEZ. Thank you, Mr. Chairman. When we talk about DEI we tend to focus on an ideological or a partisan perspective, but I am more concerned about the practical consequences that anti-DEI policies can have on U.S. citizens on the U.S. mainland and on what concerns me the most, which is Puerto Rico, the Commonwealth of Puerto Rico, which I represent here in Congress.

Puerto Rico has officially 2 languages but in practice we all speak Spanish in our everyday lives. Unfortunately, in my opinion, a significant majority of Puerto Ricans do not speak English even in among Government employees, which brings me to the following.

We have a history of cyber attacks in the island against the Puerto Rico government where we have had the collaboration of the U.S. Federal Government in addressing these cyber attacks. In light of the anti-DEI agenda, Mr. Stier, how do you see the impact of this agenda in Puerto Rico given that the Government operates predominantly in Spanish?

Mr. STIER. I'm sorry but I don't think I can really speak directly to the impact on Puerto Rico with any expertise. I will—

Mr. HERNÁNDEZ. Then sorry, I will broaden the question. Having a diverse Federal work force helps the Federal Government collaborate. Let's assume diverse means Spanish-speaking or familiar with Hispanic cultures. It will enable them to work more effectively with a Spanish-speaking government official.

Do you see that having any potential consequences in cybersecurity efforts and partnerships?

Mr. STIER. As we covered earlier, I do think that it's fundamental to draw best-in-class talent from all communities and that requires investment to make sure that that can happen. We've heard this in terms of rural areas versus urban areas. This is true across the board.

So, we do have an incredible gap that we're trying to close. It's getting larger not smaller in my view, so we need to work harder. I think fundamental to that will be intense efforts to get talent from everywhere.

So, to that extent, and the back half, too, is create environments that enable people to provide their best no matter who they are. That's part of the responsibility of good leaders and good culture.

Mr. HERNÁNDEZ. Would you agree that beyond any ideological or partisan concern it can just be simply practical to have a diverse work force?

Mr. STIER. One hundred percent. Look, I think that this is the focus that I'm trying to stay on is the practicality here. There's a lot to be done. It has huge consequence and ensuring that you have, you know, best-in-class talent from everywhere, and again, environments that enable your people to perform no matter who they are, that is just, you know, good management and in the Federal context effective use of taxpayer dollars.

Mr. HERNÁNDEZ. Well, thank you.

I yield the remainder of my time.

Chairman GREEN. The gentleman yields.

I now recognize the gentlelady from South Carolina, Mrs. Biggs, for 5 minutes of questioning.

Mrs. BIGGS. Thank you, Chairman Green, for holding this important hearing today.

Thank you to all of our witnesses for your testimonies.

I believe that while cybersecurity vulnerabilities affect all communities, unique challenges faced by South Carolina's Third District and similar rural communities around the country make us particularly vulnerable and disproportionately impacted by cyber attacks.

So, I have heard from electric co-ops and wastewater system operators as recent as yesterday in my office and other utility providers that serve hundreds of thousands of my constituents. It is evident that a key component of these challenges is the limited availability of a local, readily-accessible professional cybersecurity work force.

Providers in rural areas, like in my district, Greenwood Newberry, Abbeville, Oconee, and McCormick, they frequently lack the funding necessary to implement robust cybersecurity infrastructure and training. Furthermore, they struggle to attract and to retain qualified cybersecurity professionals who are often drawn to larger urban centers with more lucrative opportunities.

So with this combination of limited resources and a shortage of skilled personnel, it leaves our rural communities particularly vulnerable to malicious actors seeking to exploit their digital weakness.

So because of the heightened vulnerability of rural communities and critical infrastructure sectors to cyber attacks, I find the Cyber PIVOTT Act's emphasis on placing cybersecurity interns in these areas particularly compelling. So, this focus addresses a critical need bridging the cybersecurity skills gap where it is most acutely felt.

As a proud original co-sponsor of this legislation, I believe that the strategic placement of these individuals represents a promising approach to strengthening our Nation's cybersecurity resilience, particularly in the areas that need it most.

So, in addressing Mr. Jones, from your perspective what critical hands-on skills can entry-level talent learn from interning with a utility company like those in your co-op?

The second question I would like to tag on to that is in return how can interns provide value to your work force?

Mr. JONES. Well, Congresswoman, thank you for the question. You have summarized a lot of our concerns very well.

So, yes, so internship opportunities I think the skills that they could glean would be real-world and technical certainly, but something that speaks to your second question I should say in addition to that, is that we tend to be able to when we expose people to what an electric co-op is and the virtues of service, you know, again, we're good jobs in rural areas.

If we expose them to what we do, we are able to show them about who we are and we can often win people, especially younger people who want purpose in what they do because we have an incredible purpose as part of our organization.

So, I think that those internship programs will provide well-rounded opportunities for them that allow us to expose, you know, who we are. You know, and we've done this for a long time. When you think about classically what a co-op student is, it's you think

of an engineering student that comes to the utility and learns more about engineering, is mentored.

The same thing can happen with this and through the PIVOTT Act, I believe, and so we're excited about that.

Mrs. BIGGS. So, have you found that keeping those individuals—what would be your perspective on that, retaining good quality?

Mr. JONES. So in terms of trying to retain those individuals, again, I think that there's something to be said for the virtue of our mission and purpose but, you know, understanding what the market is demanding from the standpoint of salary and benefits, you know, we have to do our best to get those right. That's the challenge that we have.

So, we look to any suggestions that others have in that regard, but it's something that we're working very hard to do. Again, we collaborate so well within the cooperative community. These are conversations we're having routinely. Today at MTE we're having a meeting with a number of TVA electric cooperatives and municipal systems talking about this very issue, too, so it's something we're serious about.

But it's a bigger issue than we are, so we're happy to have conversations and get advice from others.

Mrs. BIGGS. Thank you so much.

My time is up so I yield back.

Chairman GREEN. The gentlelady yields.

I now recognize the gentleman from Texas, Mr. Turner. Appreciate you, and fire away 5 minutes.

Mr. TURNER. Thank you, Mr. Chairman. I think we can all agree, regardless of whether we are Democrats or Republicans, that the cybersecurity threats are increasing, that we are in a major crisis that we need to address. I think we can all agree on that.

I will tell you that over the last few days I have gotten a number of calls from people in Houston and the former mayor of Houston, concerned about the payment system. You have got Social Security information, medical information, tax information.

Will you agree with me that when you are sending this information from various sources that it is important to have the right checks in place to make sure that you don't make us more vulnerable to these cyber attacks? Is that important, a consideration that you take in place?

So that is what I am hearing from people.

As we talk about cybersecurity and we are talking about it today, they know it is getting worse, and they are concerned who has my information and, Congressman Turner, is it secure? I am having a hard time explaining that to them.

Another point that I want to ask, it is important, would you agree, that we train the existing work force within the Federal Government throughout the entire Federal system? That is important. I do think it is important to do everything we can to make sure that that training occurs.

But Mr. Russomanno, you made a comment that said young people need to see themselves in these fields. Then Mr. Rashotte, you said we need to break down the barriers of training and we have been 500,000 people short in this area in the United States. Would

you agreed that we need to be very intentional in recruiting, training, and bringing people into this space?

It shouldn't be where, for example, you mentioned K through 12, colleges and universities, community colleges, technical schools, but that also includes Historically Black Colleges and Universities as well in terms of reaching out to them and bringing them into this space. Would you agree?

I think you all also agree that you could be black, white, or brown. You could be from urban America or rural America. Your qualifications are not diminished by who you look like or geographically where you come from but rather I would argue the entire conversation of protecting us in the future is strengthened when we have people coming from all sectors of America. Any disagreement on that?

So, when people argue that if you are diverse, I am an African American, and I go through the training, I go to your schools, I am educated and I am prepared and if I am in this space it doesn't mean that I am incompetent. It doesn't mean that I am unqualified.

Quite frankly, those arguments help to discourage people from moving into these spaces. Would you agree with that? Any disagreement on that?

That is why I am concerned with this conversation about diversity, equity, and inclusion. What I have found in my lifetime is that it is important to have people coming from all walks of life which strengthens our organization. It doesn't diminish them. It strengthens our organization.

So, Mr. Russomanno, since you made the point that it is important for people to see themselves in these fields, could you elaborate on that for me?

Mr. RUSSOMANNO. Well, Congressman, thank you so much for your comments, and I agree with you. We need to embrace everyone from all walks of life, all backgrounds. At the University of Memphis we're particularly proud of our very diverse student body, significant African American population.

You know, in some cases I think we are looking at where we need to reframe how potential outreach is described. If I think what we look at, areas like first-generation students, students that have significant unmet financial need, we can impact many of the populations that you've been discussing, so I agree with your comments.

Mr. TURNER. Thank you.

I yield back, Mr. Chairman.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Knott for 5 minutes, the gentleman from North Carolina for his 5 minutes of questioning.

Mr. KNOTT. Thank you, Mr. Chairman.

I will start with you, Dr. Russomanno. If you had to describe the current state of the cybersecurity ecosystem, would you describe it as one that is lacking in personnel exclusively or are those who are in the space right now here in the United States are they lacking in a skill set? Are they lacking in advancement? Are we being outpaced on that front as well?

Mr. RUSSOMANNO. Thank you for your question. I think, frankly, it's a combination of both although the data is very compelling regarding the need to grow our work force. I think that data is very clear.

However, if you look at certain circumstances where industry in particular is going after mid- and advanced level of cybersecurity professionals, that also speaks to a gap in terms of the knowledge and abilities of our work force.

Mr. KNOTT. OK.

Mr. Jones, in terms of servicing rural communities and, sort-of outside, the urban areas, describe how cybersecurity plays a role in the threats that you face.

Also, and second to that, how is the threat increased if people come here to the United States outside of the law, outside of us being aware of it in terms that they have physical access to your facilities that you represent?

Mr. JONES. Yes, sir. Congressman, thank you. So, one thing I would touch on I believe to the first part of your question, the threats we face, it's something we haven't talked so much about but that I would like to if I could, is that it's not just an issue of technology, process, and specific cybersecurity resources. It is—

Mr. KNOTT. Yes.

Mr. JONES [continuing]. But it's also about a culture of cybersecurity within the organization because, and my colleagues would know better than I probably, but as far as most of the incidents we see, the intrusions that have resulted from an e-mail lapse of some kind or someone clicks on the wrong thing. So making sure that our employees—we have a culture of safety. We have to have a culture of cybersecurity awareness as well.

Mr. KNOTT. Right.

Mr. JONES. Making sure that we're facilitating that throughout the organization is very important.

Mr. TURNER. Right but protecting your facilities physically is also important for cybersecurity as well. They are not all overseas, correct? If we have cybersecurity criminals that are here illegally in this country that adds a layer of vulnerability to the systems—

Mr. JONES. Yes, sir. That's right. That's the screen and we're watching that as well. That's the other component to it.

I would say, if I could speculate with regard to the risks, you know, cybersecurity is one that we're keenly concerned about, we're most concerned about, but the physical pieces as well. We have to have, again, equipment, processes, people in place to safeguard against that potential as well. It's very real.

Mr. KNOTT. Yes.

Now, Mr. Stier, it is Stier, correct?

Mr. STIER. Yes.

Mr. KNOTT. Great. Just briefly, one thing that is upsetting in this job is the speaking with broad brushes and that is unfortunate for our dialog. I think specificity is the best way forward.

As a former Federal employee, I was a Federal prosecutor, I am somewhat troubled by the dialog and because obviously it is inhibited by time, but to say that all civil servants are uniformly described as excellent in their craft, eager to better themselves while they are employed, proficient in serving the taxpayers above all

else or highly focused and patriotic in the execution of their duties, that is certainly true for some.

As a prosecutor, I mean, I worked with agents at just about every agency. We had great agents and we had some that were there that you don't know what they did all day. Part of maintaining efficiency and effectiveness, I think you would admit and agree with me, not admit, I'm not trying to extract it, but——

Mr. STIER. Yes.

Mr. KNOTT [continuing]. Is figuring out efficient——

Mr. STIER. I agree 100 percent.

Mr. KNOTT. Yes.

Mr. STIER. Yes.

Mr. KNOTT. And figuring out ways to constructively remove those who are not motivated.

Mr. STIER. One hundred percent.

Mr. KNOTT. One of the frustrations I had in the Federal work force is when there were people who were partners or people you had to work with in other agencies, firing just was not an option or removing them. If you did cross that threshold, immediate litigation, burdensome, burdensome countersuits would have been implemented.

So given the threat of cybersecurity and the need to maintain a professional, efficient, and effective work force, how can we better extract those who are not focused?

Mr. STIER. One hundred percent and I entirely agree with you. Like all work forces there are better and worse, and I think that the Federal Government more broadly has not had effective focus on these kinds of management issues.

So there are some system changes that ought to take place. It's too complicated to actually fire people. You have to decide depending on, you know, what the issue is, where you go. That could actually be streamlined in a very profound way.

The thing that would change it the most would be actually to get managers better trained on doing the performance evaluation that you're describing and to have leaders that actually support their management to get rid of the poor performers because right now it's easier to ignore the problem than to address the problem.

So the rules can improve things, but it ultimately is a management responsibility and that focus is by and large not there.

Mr. KNOTT. OK. All right.

Mr. Chairman, I am over. I yield back.

Chairman GREEN. Yes. The gentlemen's time has expired.

I now recognize the Ranking Member for his closing statement.

Mr. THOMPSON. Thank you, Mr. Chairman.

First, let me thank our witnesses. Thank you for being here for a little while, but it is still shorter than most hearings so there are some benefits.

Mr. Chair, I ask unanimous consent for the record to be included the following documents: an article in cybersecurity entitled, "Cybersecurity: Government Experts are Aghast at Security Failures at DOGE Takeover"; a copy of a letter committed Democrats have sent to OPM regarding the impact of the hiring freeze on Federal cyber work force; a copy of a letter committed Democrats have sent OMB on security threats DOGE poses to Federal networks.

Chairman GREEN. Without objection, so ordered.
[The information follows:]

ARTICLE BY CYBERSCOOP.COM SUBMITTED BY RANKING MEMBER BENNIE G.
THOMPSON

CYBERSECURITY, GOVERNMENT EXPERTS ARE AGHAST AT SECURITY FAILURES IN DOGE
TAKEOVER

Elon Musk's takeover of key systems across the Federal Government is ignoring decades of laws, regulations and procedures, experts told CyberScoop.

By Derek B. Johnson, February 4, 2025

As the world's richest man and his team from the Department of Government Efficiency continue their quest to dismantle Federal agencies, cybersecurity experts, good government experts and Democrats are increasingly expressing outrage and alarm, in some cases likening the actions to an ongoing data breach.

Elon Musk and employees from DOGE—which is, legally, an external advisory board—have reportedly taken a number of steps since Jan. 20 that could be exposing the personal data of millions of Federal employees, violating Federal laws against sharing classified or sensitive information with uncleared individuals and creating new cybersecurity vulnerabilities for malicious hackers to exploit, these experts say.

Chief among these concerns are efforts by Musk's team to access the Department of the Treasury's payment system housed in the Bureau of Fiscal Service. This system controls much of the spending by the Federal Government, including congressionally mandated spending programs like Social Security.

Federal employees at the Office of Personnel Management are also suing the government, claiming that Musk had a private server installed that has not been vetted or approved for security. OPM's systems contain sensitive employee records for tens of millions of current and former Federal workers, and the hack and theft of OPM records by Chinese hackers in 2015 is considered among the worst Federal security breaches of all time. The use of a private email server by then-Secretary of State Hillary Clinton was the subject of a criminal investigation by the FBI during the 2016 election and was bitterly criticized by Trump and Republicans at the time as a massive security lapse.

The White House claimed Monday that DOGE employees' access to these systems were restricted to "read-only," meaning they could not alter files or make larger changes, but according to reporting from Wired, a 25-year-old former employee of Musk's has been granted administrative access to the system.

Sen. Elizabeth Warren, D-Mass., wrote to Treasury Secretary Scott Bessant this week seeking answers about this "security and management failure."

"The public depends on the integrity of those systems, which control the flow of over \$6 trillion in payments to American families, businesses, and other recipients each year—with millions relying on them for Social Security checks and Medicare benefits, Federal salaries, government contract payments, grants, and tax refunds this filing season," Warren wrote.

According to one former Federal worker with a decade of cybersecurity experience across multiple agencies—including the U.S. Digital Service that was absorbed into DOGE—the actions of Musk and his allies run afoul of "the spirit and letter of the law" for Federal cybersecurity statutes, including the Federal Information Security Management Act (FISMA) and security controls established by the National Institute of Standards and Technology for securing Federal systems.

Access to highly sensitive Federal systems is often subject to strict access and logging requirements. Individuals that do not possess a clearance in which they are allowed to access OPM and Treasury systems would, in any other situation, be viewed as a straightforward security breach with lasting ramifications.

"These systems have now become untrusted, so once this is done and over, to have those systems back to the level of assurances they had on Jan. 20 will require a lot of work and a lot of resources," said the former Federal Government employee, who now works in the private sector and was granted anonymity due to fear of reprisal.

The risks include DOGE employees potentially downloading and taking protected Federal data to creating weak points for attackers through unvetted IT infrastructure like the newly launched private server at OPM. The office's systems also connect to other agencies, like the Defense Counterintelligence and Security Agency, which handles congressional background checks. Lacking independent oversight and

activity logging, there's no way to confirm what information was accessed or changes that were made.

"The biggest issue right now is . . . the secure connection from OPM to DCSA, to either enter in or request security clearance information," the former Federal employee said.

Reps. Gerry Connolly, D-Va., ranking member for the House Oversight Committee, and Shontel Brown, D-Ohio, ranking member on the Cybersecurity, Information Technology and Government Innovation Subcommittee, wrote this week to OPM acting Director Charles Ezell saying that the lack of security and oversight associated with the new email system "threatens to expose Federal workers to personalized social engineering or 'spear phishing' attacks."

"At best, the Trump Administration's actions at OPM to date demonstrate gross negligence, severe incompetence, and a chaotic disregard for the security of our government data and the countless services it enables our agencies to provide to the public," Connolly and Brown wrote. "At worst, we fear that Trump Administration officials know full well that their actions threaten to break our government and put our citizens at risk of foreign adversaries like China and Russia gaining access to our sensitive data."

According to legal experts, Musk and Trump's actions are putting Federal employees in a lose-lose situation. Trump's executive order creating DOGE only gave Musk access to unclassified Federal systems. Under Title V of the E-Government Act of 2002, it is a Class E felony carrying a maximum penalty of 5 years in prison and a \$250,000 fine for Federal employees who have taken the oath of office to "willfully" disclose such information to any person or agency not entitled to receive it.

Bradley Moss, an attorney who specializes in national security, Federal employment and security clearance law, was unequivocal when CyberScoop asked about the legal constraints Federal employees face in this situation.

"No Federal employee should be granting access to anyone—no matter what special 'DOGE' badge they have—absent specific written authorization to do so," Moss said. "The president's [executive order] does not suffice, and Federal employees appear to be trying to hold the line on protocols so far. Unfortunately, those who are doing that are being punished for it, as many are being put on administrative leave or outright fired."

Beneath the classified level, many Federal systems also contain what's known as Controlled Unclassified Information (CUI), which can include financial, law enforcement and privacy-related data on Americans. That data is less sensitive, but still must be legally protected by Federal employees and contractors.

"There are well-established procedures, beginning with Federal employment screening, to determine whether individuals are 'trustworthy,' such that they should be afforded access to these CUI categories," said Robert Metzger, an attorney and Federal cybersecurity contracting expert. "Higher standards and controls apply to persons who would have rights of 'use' of that information."

The potential for unintended consequences on Federal IT and administrative operations is also real. Researcher Danah Boyd compared the structure of the U.S. administrative state to a game of Jenga. As politicians add or remove different blocks from the system, civil servants have usually played the role of repairman, fixing holes and propping up the byzantine American system.

The dismissal of many Federal employees overseeing these systems has made that job more difficult. Boyd believes that Musk's team interfering with vital Treasury financial systems could lead to a "normal accident," causing significant parts of the system to collapse.

"It has been a hard 2 weeks for [civil servants], but, regardless of the legal dynamics, turning over access to the core systems at the heart of an administrative state to a wrecking ball is really, really bad," Boyd wrote.

This story was updated Feb. 4, 2025, with details from a letter sent to OPM by Reps. Connolly and Brown.

LETTER SUBMITTED BY RANKING MEMBER BENNIE G. THOMPSON

February 5, 2025.

Mr. CHARLES EZELL,
Acting Director, U.S. Office of Personnel Management, 1900 E Street, NW., Washington, DC 20415-1000.

DEAR ACTING DIRECTOR EZELL: We are writing to request information on the impact of President Trump's hiring freeze on the Federal cybersecurity workforce. As you may know, the Federal Government has struggled to recruit, hire, and retain

qualified cybersecurity workers for many years. During the Biden Administration, the Federal Government took several steps to address this challenge, including through the issuance of a National Cyber Workforce and Education Strategy and implementation of the Cyber Talent Management System at the Department of Homeland Security (DHS). Now, reckless attacks on Federal workers risk reversing recent progress in addressing the Federal Government's cyber workforce shortage.

On Inauguration Day, President Trump issued an executive order to mandate “a freeze on the hiring of Federal civilian employees.”¹ While the order included an exemption for positions related to “national security,” it failed to provide any definition for that term.² Related guidance from the Office of Personnel Management (OPM) and the Office of Management and Budget similarly failed to clarify how agency heads should implement this exemption.³ While the Department of Defense has continued hiring for civilian positions,⁴ the Cybersecurity and Infrastructure Security Agency, which is the operational lead for Federal cybersecurity and the national coordinator for critical infrastructure security and resilience, does not have a single open position listed on the USA Jobs website.⁵

Agencies throughout the Federal Government are responsible for defending their agency networks, regardless of whether cybersecurity is their primary mission, and any delay in filling vacant cybersecurity positions at Federal agencies risks severe national security implications. Recent cyber incidents have demonstrated that Federal agencies remain top targets for foreign adversaries. In December 2024, the Treasury Department suffered a major cyber incident when Chinese hackers were able to gain access to then-Secretary Janet Yellen's files through a supply chain attack.⁶ In June 2023, the State Department discovered a breach of Microsoft's cloud networks by Chinese hackers, uncovering an incident that affected 22 organizations and over 500 individuals around the world, including the Commerce Department and then-Secretary Raimondo.⁷ The Departments of Treasury, State, and Commerce all have zero open positions listed on the USA Jobs website.⁸ A hiring freeze that precludes Federal agencies from filling cybersecurity positions risks the security of Federal networks and may prevent sector risk management agencies from fulfilling their obligations to help defend critical infrastructure.

On January 28, 2025, OPM emailed Federal employees an “offer” to resign from Federal employment, entitled a “Fork in the Road.”⁹ This offer included an exemption for positions related to national security but similarly failed to define which positions fall under the exemption. While we understand that many DHS components have been exempted from this offer, there is a risk that incentives offered by OPM could reduce the number of cybersecurity professionals across the Federal Government.

To better understand the homeland security implications of the current hiring freeze, we seek to clarify how President Trump's executive order has impacted the Federal cybersecurity workforce and what OPM plans to do to mitigate the national security harms of the President's poorly drafted, vague, and irresponsible hiring freeze.

Please respond to the following questions by February 19, 2025:

1. How many cybersecurity-related open positions are subject to the current hiring freeze? Please detail them by department or agency.
2. How many cybersecurity professionals have chosen to resign under the “Fork in the Road” offer? Please detail them by department or agency.
3. Are all cybersecurity-related positions exempt from the hiring freeze or the Fork in the Road offer?

¹ *Hiring Freeze*, The White House, Jan. 20, 2025, <https://www.whitehouse.gov/presidential-actions/2025/01/hiring-freeze/>.

² *Id.*

³ Memorandum from Matthew J. Vieth and Charles Ezell to Heads of Executive Departments and Agencies, Jan. 20, 2025, <https://chcoc.gov/sites/default/files/OMB-OPM%20-Federal%20Civilian%20Hiring%20Freeze%20Guidance%201-20-2025%20FINAL.pdf>.

⁴ Karen Jowers, *All of DOD exempt from White House's civilian hiring freeze*, Military Times, Jan. 29, 2025, <https://www.militarytimes.com/news/pentagon-congress/2025-01-29/all-of-dod-exempt-from-white-houses-civilian-hiring-freeze/>.

⁵ USAJOBS, <https://www.usajobs.gov/> (last accessed Feb. 2, 2025).

⁶ Jonathan Greig, *U.S. sanctions hacker and company allegedly behind Treasury and telecom breaches*, The Record, Jan. 17, 2025, <https://therecord.media/treasury-sanctions-alleged-salt-typhoon-hacker-company>.

⁷ *Review of the Summer 2023 Microsoft Exchange Online Intrusion*, Cyber Safety Review Board, March 20, 2024, https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

⁸ USAJOBS, <https://www.usajobs.gov/> (last accessed Feb. 2, 2025).

⁹ *Fork in the Road*, Office of Personnel Management, <http://www.opm.gov/fork> (last accessed Feb. 3, 2025).

4. What guidance has OPM provided to agencies on the application of the hiring freeze or Fork in the Road offer to cybersecurity-related positions? Please provide a copy of such guidance.

5. What impact has the hiring freeze had on participants in programs where Federal employment is a condition of scholarship support, such as the CyberCorps: Scholarship for Service program? Please describe any delays or restrictions on hiring such participants.

Sincerely,

BENNIE G. THOMPSON,
Member of Congress,
Ranking Member, Committee on Homeland Security.

ERIC SWALWELL,
Member of Congress.

J. LUIS CORREA,
Member of Congress.

SHRI THANEDAR,
Member of Congress.

SETH MAGAZINER,
Member of Congress.

DAN GOLDMAN,
Member of Congress.

DELIA C. RAMIREZ,
Member of Congress.

TIMOTHY M. KENNEDY,
Member of Congress.

LAMONICA MCIVER,
Member of Congress.

JULIE JOHNSON,
Member of Congress.

PABLO JOSÉ HERNÁNDEZ,
Member of Congress.

NELLIE POU,
Member of Congress.

SYLVESTER TURNER,
Member of Congress.

LETTER SUBMITTED BY RANKING MEMBER BENNIE G. THOMPSON

February 5, 2025.

Mr. MATTHEW J. VAETH,
Acting Director, Office of Management and Budget, 1725 17th St., NW., Washington,
DC 20503.

DEAR ACTING DIRECTOR VAETH: We write to express our serious concerns about the unprecedented access to sensitive government data granted to Elon Musk and his US DOGE Service (DOGE) associates and inquire about what policies and procedures are in place to protect the security and integrity of sensitive government information.

Under the Federal Information Security Modernization Act (FISMA) of 2014, the Director of the Office of Management and Budget (OMB) is responsible for “developing and overseeing the implementation of policies, principles, standards, and guidelines on information security” and “requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of (A) information collected or maintained by or on behalf of an agency; or (B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.”¹

Executive Order (EO) 14158, Establishing and Implementing the President’s “Department of Government Efficiency,” gave DOGE unprecedented access to informa-

¹ 44 U.S.C. 3553(a).

tion systems across government.² It directs Agency Heads “to take all necessary steps” to ensure DOGE “has full and prompt access to all unclassified agency records, software systems, and IT systems.”³ The EO also directs DOGE to adhere to “rigorous data protection standards.”⁴ Although the EO fails to articulate those standards, they presumably include Federal laws including, but not limited to, FISMA, the E-Government Act of 2002,⁵ and the Federal Acquisition Regulation, as well as OMB policies intended to protect Federal networks, including OMB 22–09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*.⁶ Instead, by all accounts, DOGE is running roughshod across Federal networks, accessing untold amounts of information about Americans in complete disregard for security and privacy standards.

According to media reports, in recent days, Elon Musk and his DOGE associates have accessed a broad range of government databases at multiple Federal agencies. These agencies include the Treasury Department, the U.S. Office of Personnel Management, the U.S. Agency for International Development, the Small Business Administration, and possibly others.⁷ The systems include the payment systems that the Treasury Department uses to honor U.S. financial obligations, those that store sensitive personnel data on Federal employees, and reportedly classified information systems, which DOGE has absolutely no authority to access. This reporting also indicates that DOGE officials have transferred data to commercial servers that may not have been vetted for compliance with security and privacy requirements, another potential violation of Federal law.⁸ These databases include personally identifiable information on Federal employees and millions of other Americans, and any risk of exposure to foreign adversaries could have grave national security consequences. Due to the complete lack of transparency about DOGE’s activities, it is possible that DOGE has gained access to other information that the public is not yet aware of.

We know that China and other foreign adversaries are regularly seeking to breach Federal agency networks to gather exploitable information about government officials, American citizens, and U.S. businesses. That is why the U.S. Government has implemented numerous policies and programs to secure sensitive data. Elon Musk and his DOGE associates are not exempt from those policies. Under your statutory obligations, you are responsible for ensuring that Elon Musk complies with data privacy and security requirements, and we urge you to take action to ensure compliance.

The American public deserves to know who is accessing their personal information and why. The government also has an obligation to keep their information secure. To help us better understand what policies and procedures are currently in place to secure data obtained by DOGE and what steps are being taken to secure Americans’ data, we request that you respond to the following questions by February 19, 2025:

1. Which departments and agencies have granted DOGE access to their information systems and data? Please specify the types of information DOGE has accessed and the purpose of the access.
2. DOGE has no authority to access classified systems, but media reports indicate DOGE employees have, in fact, accessed such systems.

² Exec. Order No. 14158, *Establishing and Implementing the President’s “Department of Government Efficiency.”* 90 Fed. Reg. 8441 (Jan. 20, 2025), <https://www.federalregister.gov/documents/2025/01/29/2025-02005/establishing-and-implementing-the-presidents-department-of-government-efficiency>.

³ Id.

⁴ Id.

⁵ 44 U.S.C. § 101.

⁶ OMB Memorandum M–22–09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022), <https://zerotrust.cyber.gov/downloads/M-22-09%20Federal%20Zero%20Trust%20Strategy.pdf>.

⁷ Fatima Hussein, *Elon Musk’s DOGE commission gains access to sensitive Treasury payment systems: AP sources*, Associated Press, Feb. 1, 2025, <https://apnews.com/article/donald-trump-elon-musk-doge-treasury-5e26cc80fcb766981cea56afd57ae759>; Abigail Williams, Vaughn Hillyard, Yamiche Alcindor, and Dan De Luce, *USAID security leaders removed after refusing Elon Musk’s DOGE employees access to secure systems*, NBC News, Feb. 3, 2023 [sic], <https://www.nbcnews.com/politics/national-security/usaids-security-leaders-removed-refusing-elon-musks-doge-employees-access-rcna190357>; Tim Reid, *Exclusive: Musk aides lock workers out of OPM computer systems*, Reuters, Feb. 2, 2023 [sic], <https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/>.

⁸ Caleb Ecarma and Judd Legum, *Musk associates given unfettered access to private data of government employees*, Musk Watch, Feb. 3, 2025, <http://www.muskwatch.com/p/musk-associates-given-unfettered/>.

a. Have DOGE employees accessed classified systems? Please specify the authority under which DOGE employees accessed classified systems, which classified systems DOGE employees have accessed, and the purpose of DOGE access.

b. Do the DOGE employees who have accessed classified systems have security clearances? If so, did they complete the SF-86 form and undergo the background investigations required for Federal employees to obtain access to classified information. Please provide the dates upon which each DOGE employee who accessed classified information received their clearance, the type of security clearance each DOGE employee has, the date of their clearance security education meeting, and who provided the clearance security education meeting.

3. What procedures are in place to ensure that DOGE complies with the E-Government Act of 2002's requirement of Privacy Impact Assessments for the use of new information technology?

4. How is OMB ensuring DOGE is in compliance with the Federal Government's mandatory information security policies under FISMA and other relevant laws?

5. What guidance, if any, has OMB provided to Federal agencies how to mitigate security risks posed by DOGE access to their networks?

6. In the past, the US Digital Service accessed Federal department and agency information systems after being invited to do so. Do Federal agencies have the authority to refuse DOGE access to their information systems and data?

OMB has an obligation to ensure Federal information systems and data security laws are being followed, and we urge to move expeditiously to investigate what Federal laws and policies DOGE may have violated and take appropriate action. We look forward to your timely response.

Sincerely,

BENNIE G. THOMPSON,
Member of Congress,
Ranking Member, Committee on Homeland Security.

ERIC SWALWELL,
Member of Congress.

J. LUIS CORREA,
Member of Congress.

SHRI THANEDAR,
Member of Congress.

SETH MAGAZINER,
Member of Congress.

DAN GOLDMAN,
Member of Congress.

DELIA C. RAMIREZ,
Member of Congress.

TIMOTHY M. KENNEDY,
Member of Congress.

LAMONICA McIVER,
Member of Congress.

JULIE JOHNSON,
Member of Congress.

PABLO JOSÉ HERNÁNDEZ,
Member of Congress.

NELLIE POU,
Member of Congress.

SYLVESTER TURNER,
Member of Congress.

Mr. THOMPSON. I also want to thank again our witnesses for coming and testifying today and sharing that expertise. I was long years ago an instructor. Those of you who are in education, you have my heartfelt support and sympathy for the talent and challenges you have. It is indeed a challenge.

I have rural electric co-ops in my district and one of the things this Government committed to was having electricity to every house in America, and it could not have been accomplished had it not been for rural electric co-ops. So I thank you for that work.

But I also know that all of you take this topic of cybersecurity very seriously.

I am sorry for Mr. Stier for that unjustified treatment that you received from Congresswoman Greene. You are a witness for this committee and we owe all our witnesses a certain amount of courtesy. You did not deserve what you received and if not from anybody else, I apologize. We are better than that.

We should not antagonize people who we invite into this great institution to offer their expertise, and so for that I just wanted to say that I appreciate all of you for being here. But I don't like people being maligned by any Member of this committee.

So, Mr. Chairman, the goal of building a robust cyber work force is to improve the security of our networks, infrastructure owned by both the Government and the private sector.

As we sit here today, Elon Musk and his DOGE team are rifling through America's data and accessing agency networks all while ignoring Federal information, security, and privacy laws, and the Majority is silent about it.

We can't jump up and down about the cyber threats posed by China and the need to build a cyber work force to defend against them while at the same time allowing unchecked access to the Federal networks.

I urge my colleagues on the other side of the aisle to stop pretending like it is business as usual and take these threats seriously.

We all appreciate the urgency of addressing the cyber work force shortage. China and other adversaries are trying to hack our Government and critical infrastructures every day, but the Trump-Musk administration's war on the Federal work force is putting our national security at risk.

While Trump's vague Executive Orders may have theoretical exceptions for national security, its application across the Federal Government has clearly impacted cybersecurity positions.

For example, a search on the USAJOBS website shows that there is a hiring freeze in place at CISA right now. In the administration's reckless rush to force out Federal employees, they sent their resignation letter to CISA employees, only clarifying later that they were not eligible.

Mr. Stier's example in his opening statement of a student in the CyberCorps Scholarships for Service demonstrates just how serious the impact these policies have had on people seeking to join the Federal cyber work force.

Again, I thank the witnesses for their time, and I hope all Members of the committee join together to push back on the Trump administration's dangerous policies toward the Federal cyber work force. Our Nation's security depends on it.

Chairman GREEN. The gentleman yields.

I now recognize myself for a closing statement. First, I would like to mention to everybody, sort-of, an announcement, I guess. We just got another commendation from IBM to support the PIVOTT Act, another stakeholder.

If you look at the list of these companies that thought today's hearing and the discussion about this bill is really an important thing you would wonder why all the people over here were so crit-

ical and some called it even a stupid hearing but I, you know, I digress.

I guess those companies are all, you know, going the wrong way. They're not, of course, and we appreciate the support despite what the left side of this committee has said today.

In closing, I want to thank our witnesses for their informative testimony. I really appreciate all of you sharing your comments.

The cyber threat environment continues to evolve and it is a huge risk to our country. The fact that Volt Typhoon and Salt Typhoon are where they are or where they have been should scare the hell out of every American. We have a massive shortage of people.

As we looked over the past, you know, my first term as Chairman, we identified the priorities. This is the work force shortage is No. 1, and that is why this committee, last week's committee, focused on cyber the first of this Congress and this committee.

Nation-state actors like China, Russia, Iran routinely target critical networks and businesses in both private and public sectors, and it is vital that we scale the work force up.

I am disappointed that some seem concerned about criticizing efforts to create much-needed efficiency and improvement within the Federal Government and the actual misallocation of massive taxpayer funds that could have gone to cybersecurity.

Today's hearing and the Cyber PIVOTT Act are focused on leveraging flexible approaches to close talent gaps and improve our cyber work force using lessons and approaches from the private sector.

I think we would all agree that developing our cyber work force should be a much higher priority than spending \$25 million to promote green transportation in the country of Georgia or spending taxpayer dollars teaching journalists in Sri Lanka to avoid using binary gender language.

Or to take another example, the Federal Government spending \$2 million to promote Moroccan pottery classes, another \$2 million to promote tourism in Lebanon, which is under a travel warning from the State Department, all discovered by the very organization that nearly every Member of that side of the committee spent today's committee hearing talking about when we are here to talk about, you know, this massive cyber shortage and risk to our country.

These are just the tip of the iceberg. Someone told me as I was walking in this morning we sent \$49 million to Guatemala to build a gas station that never got built. Thank God someone's figuring this out, the corruption that has happened.

Of course, they want to jump up and down and say somebody is not supposed to be here, a guy by the way who builds rockets for NASA and has a Top Secret security clearance. I will just correct the record on that.

When you bring efficiency to Government you invest in the core needs of Government. What is a core need of Government? Cybersecurity. The enemy has invaded our infrastructure and our telecommunications networks. We need every penny we have got to go toward things like the PIVOTT Act.

Our approach to Cyber PIVOTT Act has received significant support from the cybersecurity community, trade organizations, businesses. We have talked about this.

I will look forward to making this bill become law this Congress because our Nation needs it, and even the witness from the other side agreed with that.

I will make a quick comment about when you are in a committee hearing as a witness, the representative owns their time, Mr. Steir. If you were offended I apologize, but they own their time.

In this committee room and in every committee room I have seen this happen many times where someone shuts down the witness to say what they want to say.

So, we gaveled down people in this committee on my side of the aisle when they did cross the line and attack the witnesses, you know, verbally with character. I didn't see that happen today and so we let that continue.

But it is interesting how the politics of this place works and what the rules really are. But I want to catch you after this so I can talk with you in person.

I want to again thank the witnesses for being here, the Members for their questioning. This hearing is adjourned.

[Whereupon, at 12:57 p.m., the committee was adjourned.]

