STATEMENT FOR THE RECORD: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Homeland Security Committee

Preparing the Pipeline:
Examining the State of America's Cyber Workforce

PREPARED BY:

RADM (Ret.) Mark Montgomery
Senior Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Jiwon Ma
Senior Policy Analyst at the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Washington, DC
February 5, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

The PIVOTT Act is Pivotal to Securing the Future of the Federal Cyber Workforce

Written Statement for the Record
U.S. House of Representatives Committee on Homeland Security
Hearing on "Preparing the Pipeline: Examining the State of America's Cyber Workforce"
February 5, 2025

By RADM (Ret.) Mark Montgomery and Jiwon Ma
Foundation for Defense of Democracies

Last week, a number of experts testified to the significant threat that the United States faces in cyberspace, 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 four-year degrees, overlooking highly skilled professionals with in-demand industry certifications and real-world expertise that do not fit traditional academic criteria for hiring.

Ongoing Federal Efforts

Over the past two 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 two-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 onboarding 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, onboarded, 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.