PARTNERSHIP
FOR PUBLIC SERVICE

Max Stier

President and CEO

Partnership for Public Service

Written statement prepared for

The House Committee on Homeland Security

Hearing entitled,

“Preparing the Pipeline: Examining the State of America’s Cyber Workforce”

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 nationwide 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 five 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 governmentwide cyber workforce? What are ways

[1] Partnership 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).
[2] Partnership for Public Service, Cybersecurity and Artificial Intelligence Talent Initiative, https://gogovernment.org/fellowship/cybersecurity-ai-talent-initiative/
[3] Partnership for Public Service's "Vision for a Better Government" (Aug. 15, 2024), available at https://ourpublicservice.org/publications/vision-for-a-better-government/

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.

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 five 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%, while those age 50 and over represent 48% 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 governmentwide 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

[4] Based 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).
[5] House 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/
[6] Analysis based on Office of Personnel Management's FedScope data as of March 2024.
[7] Government Accountability Office, "High Risk Series: An Update" (Jan 1, 2001), available at https://www.gao.gov/products/gao-01-263

a 2024 High Risk update, GAO identified the need to address cybersecurity workforce management challenges as one of ten critical cybersecurity action areas.[8]

In its most recent report on the cybersecurity workforce, GAO reviewed the cybersecurity workforce planning efforts of five 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.

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 five 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 governmentwide laws governing personnel management. Our overall framework for human capital is built for a bygone age when a great bulk of the federal

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

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

[10] Partnership for Public Service, "Building the Enterprise: A New Civil Service Framework" (April 10, 2024), available at https://ourpublicservice.org/publications/building-the-enterprise/
[11] Available at https://ourpublicservice.org/public-service-leadership-institute/public-service-leadership-model/

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® rankings[12] to drive better results in their agencies. Employee engagement 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.

---

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

[13] For 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).

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 governmentwide 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] The Partnership has long endorsed a ROTC-like model as a pipeline for the whole federal civil service.
- 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 government-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] We need to ensure that our policies recognize this is a nationwide effort.

Elevate the human resource functions of agencies: There are outstanding and innovative HR 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, HR specialists are not familiar with the authorities they have available to them, and do not have the

[14] H.R. 9770, 118th Congress.
[15] Pub. L. 118-188 (Dec. 23, 2024).
[16] Section 1104 of the National Defense Authorization Act for Fiscal Year 2017, Pub. L. 114-328 (Dec. 23, 2016).
[17] Analysis of FedScope data as of March 2024.

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 HR 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 HR needs necessary to carry out their policies and programs.

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