Testimony

of

Dr. Costis Toregas

Director, GWU Cyber Security and Privacy Research Institute

and

Fellow, National Academy of Public Administration

Before the

U.S. House of Representatives

Committee on Oversight and Accountability

Subcommittee on Cybersecurity, Information Technology and Government Innovation

January 17, 2024

Chairwoman Mace, Ranking Member Connolly and members of the Subcommittee, I appreciate the opportunity to testify today. I am Dr. Costis Toregas, director of the Cyber Security and Privacy Research Institute (CSPRI) of the George Washington University, and a Fellow of the National Academy of Public Administration (the Academy), chartered by Congress in 1984 as an independent, non-profit, non-partisan organization to help government leaders address critical challenges.

Your invitation letter suggested that you want to review efforts to develop an AI-ready workforce that enhances American strength and prosperity- a timely and vital goal in an era when Artificial Intelligence (AI) is in the forefront of many conversations in industry, education and government circles.

A focused approach to the complex topic of AI, and understanding what the role of workforce stakeholders might be, can be broken down in three major stages:

Stage 1: Understanding what is AI; as a tangible example, the Academy has created a video series of webinars to prepare managers of government agencies understand the dimensions of AI, some current examples of its use and resources to improve their understanding of AI concepts and capabilities.

Stage 2: Encouraging AI development, commercialization, and deployment. A practical example of this deeper approach to AI is my own university's (GWU) Trustworthy AI in Law and Society (TRAILS) initiative supported by the National Science Foundation which will develop new AI technologies that promote trust and mitigate risks, while also empowering and educating the public about AI.

Stage 3: Creating a workforce able to use AI in the workplace is the last stage that is perhaps not as glamorous as the first two, but which holds the key to success five to ten years out. If the US is unable to create an AI-empowered work force in numbers that are higher than today's low percentages, we may lose our competitiveness not only in AI, but in commerce and other sectors on a global scale.

The Subcommittee has already and wisely given priority to the first two stages; the most recent hearing on December 6, 2023 focused on the benefits and risks of AI deployment, and allowed members to hear views on the Administration's Executive Order 14110 covering federal agency development and use of AI by agencies. I want to focus my comments today on the third stage of ensuring the nation has a workforce able to use AI in the workplace, and I want to suggest steps the Subcommittee can take to promote progress and success in this more focused area.

Although AI as a scientific topic has been around for decades, the demand for AI uses and talent has spiked only in the recent past with the release of popular applications such as ChatGPT that brought AI to the many. As a consequence, workforce issues in AI have not yet been well researched and studied. Here are some personal observations from my experiences in the field:

> standard terminology for AI skills needed to monitor workforce development efforts is still under development

> Degrees and certificates for AI students are not uniform, come from different types of institutions (Computer Science, Professional Development, Business) and are regarded in different ways by potential employers

> Professional certifications for AI skills are lagging behind those in the cyber security domain and employers do not have a clear idea of how to quicky assess a job applicant's qualifications. In cybersecurity, certification organizations such as CompTIA or ISC2 provide a feeling of assurance to hiring managers that the holder possesses skill mastery in particular fields; the same cannot be said in the AI field today

> frameworks such as NIST's Risk Management Framework (RMF) was released only recently and has not created robust implementation experiences and feedback yet

> job descriptions for AI positions are confusing and not comparable across sectors of commerce.

Given this, it is challenging to review efforts to develop an AI-ready workforce and suggest strategies for the future.

One way to move forward with some level of confidence is to look at the allied field of cybersecurity, which probably precedes AI in the workforce development arena by at least a decade. One might see cyber security and AI workforce issues as looking similar (homomorphic) and therefore structures and mechanisms we built as a nation to address the critical shortages in cybersecurity workforce can offer clues as to good approaches for AI workforce development policies as well. Below I have summarized some problems and resolution strategies we have implemented as a nation in the cybersecurity space for the Subcommittee's consideration and possible application in the AI workforce quandary.

Lessons learned in the cybersecurity workforce development arena

- There is an insufficient number of potential employees in traditional education pathways- there is a need to create alternative on-ramps through apprenticeships, camps, upskilling programs and with a focus on underrepresented minorities and women. Working with national networks for these groups such as Women in Cyber Security (WiCyS) is key to establishing a feeling of safe space for the new professions and can increase the number of underrepresented classes in the work stream. A key lesson is the need for intentionality in approach- strategies must explicitly target desired groups and provide robust paths and help to traverse them
- Cyber security is truly multi sectoral and exists in all major disciplines; computer science and IT disciplines have dominated the discussion, perhaps to the detriment of developing workers who can be prepared for jobs beyond the technology sector, and which nevertheless require understanding of cybersecurity principles
- Cybersecurity changes rapidly; learning platforms such as teaching methods and curricula are slower to adapt and are left behind unless there are strong incentives and capacity to keep pace
- It is vital to bring job description detail to today's reality- the role of OPM and HR professionals is key to attracting talent; relationships to the hiring community are key to establishing favorable workforce pipeline conditions

- We do not have a single education system but 50 individual state Board of Education-based systems of learning; this is of course a strength in that it reflects local values and community needs, but in a technology area such as cybersecurity (and now AI), it can be a weakness and slow down the development of the numbers of uniformly-trained workers that industry and government employers need and will need in the future
- Specific agencies set up to manage cybersecurity for the federal government (for example the Cybersecurity Infrastructure Security Agency (CISA)) have the challenge of appreciating the individual agency needs and strategies and delivering appropriate solutions and support; a recent report by the Academy suggested explicit strategies to improve coherence and collaboration potential with a key recommendation to expand outreach to underrepresented populations and communities and enable broader access to cybersecurity curricula
- Networks of educators and education institutions with a common interest in cybersecurity can help create a community of interest, solidify commitments to stay in the field and create support for common curricula and student engagement practices (a current example is the National Cybersecurity Training and Education center (NCyTE), managed by Whatcom Community College in Bellingham WA and supported by the National Science Foundation as a national center for Cybersecurity education); NCyTE coordinates cybersecurity curricula and faculty development efforts and provides support to several hundred community colleges and universities
- Who establishes learning standards? There is a strong debate currently between performance based vs knowledge based targets of education, and several models of standards developed and championed by diverse government agencies and others
- The role of external, experiential learning platforms such as cyber security competitions like the National Cyber League and the President Cup Cybersecurity Competition can be useful in attracting and retaining new and young talent to the profession
- The federal workforce will always have a hard time matching the salary attraction of private sector offers and the entrepreneurial sector; scholarship programs with a service provision such as NSF's Scholarship for Service (SFS) and DoD's Cybersecurity Scholarship Program (CySP) have shown promise and can be used as blue prints for the AI sector; ways to improve their scalability can help their effectiveness

Many of these issues have correspondence in the AI world, and experiences of the last 15 years in cybersecurity workforce development can provide a blueprint for the upcoming AI workforce decisions that must be made in our society.

Suggestions for Subcommittee consideration

1. Develop a statistical capacity at national level to track current numbers of students and teachers in AI by region, as well as estimated AI workforce needs of government and industry in the future. A partnership that produces profiles in the cybersecurity domain is Cyberseek, built on a robust public-private partnership. This will of course require a typology ahead of the data collection that defines student and faculty types, job descriptions and other foundational descriptors yet in the developmental stage.

2. Encourage states to harmonize AI programs for K-12 through national conversations of experts and discussions of curricular frameworks and rubrics, and promote the broad notion of a digital citizenship program for all students that would include digital literacy, cyber security, privacy, AI and civics in a digital era. Efforts of agencies such as the AI4k12 program and EducateAI of the National Science Foundation are a good start, but do not have the reach nor the urgency of implementation

3. Support the development and maintenance of curricula focused not only on the "what is AI" or "how can AI be improved and regulated" but rather "how can AI be used". In this space, good candidates for execution are the more than one thousand locally based and supported public, independent and tribal community colleges, and they can be strong performers in the new field of AI workforce development as they are able to change course quickly and adopt AI-focused curricula and degrees or certificates far faster than other types of educational institutions

4. Focus on the need for additional AI educators and establish support programs that incentivize attraction and retention at high school, community college and university level. A retention strategy can involve funding for networks of educators who are working in this space in order to give them needed support and encouragement through Best Practice sharing, job fairs, curriculum exchanges and student networking

5. Help launch a tripartite partnership between the private sector, the education community and government agencies around workforce development issues in AI; the mandate of such a partnership could include the establishment of a long term vision for AI workforce expansion and the steps necessary to align academic performance to industry needs. Such a partnership platform to promote and carry out needed discussions and decisions acceptable to all sides does not currently appear to exist.

Chairwoman Mace, that concludes my written remarks, and I would be pleased to answer any questions you or the Committee members may have.