Cyber Workforce Development

TO MEET TODAY'S NATIONAL DEFENSE CHALLENGES

By **Tom Wingfield**, OSD(P)/HD&GS/DASD for Cyber Policy

Famed German-born scientist Albert Einstein was once asked how, if he had one hour, he would go about saving the world. After a moment's reflection, he said that he would take fifty-five minutes to define the problem, and the last five minutes to solve it.

We are now framing the problem of how to ensure that the most important part of the cyber ecosystem — the human component — is prepared to design, build, maintain, operate, and defend our cyber infrastructure. Despite the clarity of need, the scarcity of skilled cybersecurity thinkers and workers remains a well-documented global challenge for industry and for governments alike. Certainly, some sectors lag behind, but most government and industry leaders are now cognizant of and attentive to the need for increased security and resiliency in cyberspace.

Accepting cybersecurity skills were both scarce and unevenly distributed, even in the U.S. national security sphere, President Trump issued an executive order in May 2019 to jumpstart federal cybersecurity workforce enhancements. "The Nation is experiencing a shortage of cybersecurity talent and capability, and innovative approaches are required to improve access to training that maximizes individuals' cybersecurity knowledge, skills, and abilities," he wrote. Further to that point, the recently published Executive Summary of the Cyberspace Solarium Commission, a bi-partisan, Congressionally-chartered commission, stated that "Congress and the executive branch should pass legislation and implement policies designed to better recruit, develop, and retain cyber talent while acting to deepen the pool of candidates for cyber work in the federal government."

In response to these mandates, the United States Department of Defense (DoD) — with over 1.4 million active duty personnel, 1.1 million reservists, and 861,000 civilian employees stationed in the United States or overseas across 163 countries — understands cybersecurity is a critical component to achieve its missions, and that attentive and careful development of its cyber workforce is key to its success.

For DoD, a first principle is to define the focus of effort: the Defense Cyberspace Workforce, which the Department now formally defines as consisting of "positions that are recognized as critical to the defense of the nation and is comprised of personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources to include supportive work roles; conduct related intelligence activities, enable future operations and project power in and through cyberspace."

This definition is further refined by the DoD Cyber Workforce Framework (DCWF), which serves as the authoritative reference for the Department's comprehensive approach to cyber workforce talent management that addresses military, civilian, and contracted personnel. The benefits of the DCWF are many: it implements a role-based approach for the identification and reporting of cyberspace positions for enhanced workforce planning; it establishes an enterprise-wide qualification program focused on verifying knowledge and capability, promoting continuous professional development, supporting role-based progression across the cyberspace

workforce; it sets baseline standards for the Department that do not rely on antiquated personnel structures; lastly, the DCWF Program directly supports operational needs and workforce readiness, while allowing for customization and flexibility at the Component-level.

To develop the DCWF, the DoD leveraged the National Initiative for Cybersecurity Education (NICE) Workforce Framework by the National Institute of Standards and Technology (NIST), as well as the Joint Cyberspace Training and Certification Standards issued by United States Cyber Command. This allowed the Department to build a bridge between national standards and our operational forces, and to cover a broad and varied range of cyber work roles — the DCWF contains 54 of them — and job functions.

a manmade domain. The United States, along with its allies and partners, requires a greater number of citizens — practitioners and policy-makers alike — who are properly educated and trained in cyber capabilities. Challenges posed by remote working situations during the recent pandemic, for instance, have highlighted the importance of strong cybersecurity, sound cyber hygiene practices, and broad cyber literacy. We need a capable cyber workforce to make it all work. Whether they are employed in the public or private sectors, these cyber-aware workers are the front-line guardians of our collective ability to protect national and economic security.

To grapple with cyber workforce issues is to recognize there is no single underlying problem. To further develop our respective cyber workforces, we all face an interconnected array of issues tying together primary and higher education, diversity and inclusion, industry certifications and competencies, recruitment, retention, apprenticeship and work-based learning, national hiring practices, and much more. Coordinated efforts across the entirety of a business or a bureaucracy are necessary to reverse current trends; underscoring the complexity of this challenge, solutions to fill this gap rely on input from a variety of stakeholders.

We need a capable cyber workforce to make it all work. Whether they are employed in the public or private sectors, these cyber-aware workers are the front-line guardians of our collective ability to protect national and economic security.

Moving forward, DoD recognized the need for a flexible personnel system for civilians in the Defense Cyberspace Workforce. Motivated by and in synch with the 2018 *DoD Cyber Strategy and National Defense Strategy*, the Cyber Excepted Service (CES) Personnel System is designed to address acute challenges in recruitment, development, and retention of DoD's civilian cyberspace workforce. The CES recognizes the complexity of managing today's cyber workforce, offering a readily available and funded tool-set that transcends current governmental HR practice and systems. Indications are that Services which have completed conversion to the CES are leveraging these enhancements with great success in improving civilian manning and incentivizing cyberspace professionals.

The Department remains committed to supporting interagency cyber workforce initiatives, actively partnering with NIST and other federal partners to support NICE, and building resources that are shared across the federal government and at the national level. This work includes sharing best practices and lessons learned with international partners seeking to leverage NIST standards to develop training and education programs, often in cooperation with the United States. The objective in every case is to create a diverse group who govern, design, defend, analyze, administer, operate, and maintain the ecosystem of policies, systems, and networks on which our way of life depends.

As with other long-term, multifaceted challenges, education and training of the personnel working on those challenges are key components of any solution — and this is particularly true in cyberspace, which is, after all,

As such, any discussion on cybersecurity workforce development is a network of conversations. These conversations must be conducted domestically and with like-minded international partners, and they need also to be mindful of cross-border interdependencies in cyberspace, always grounded in projections of risks and an awareness of threats. Cyber workforce improvement efforts touch upon a number of technical and occupational fields, each with its own needs and policy prescriptions, from hardware acquisition and modernization, to human resource imperatives, such as training, education, hiring, and retention. In the final analysis, such considerations should be in the forefront of the minds of leaders all over the world because a nation's cyber workforce is among its most precious strategic assets. □

Tom Wingfield is deputy assistant secretary of defense. He supports the U.S. secretary of defense and other senior Department of Defense leaders by formulating, recommending, integrating, and implementing policies and strategies to improve the department's ability to operate in cyberspace.