Feds Face a Tough Challenge in Closing the Cyber Skills Gap

White House and DHS issue new report raising warnings about raising a "world-class cybersecurity workforce."

Kevin McCaney

Sun, 10/21/2018 - 23:23

Sailors stand watch in the Fleet Operations Center at the headquarters of U.S. Fleet Cyber Command/U.S. 10th Fleet (FCC/C10F) at Fort George G. Meade, Maryland, Sept. 27, 2018. (U.S. Navy photo by Mass Communication Specialist 1st Class Samuel Souvannason

Government leaders face a constant struggle attracting tech's brightest minds to work in government. And yet the threat continues to grow as attacks on agencies grow by millions by the day.

It's nothing new, but the Homeland Security Department and the White House have added a new level of urgency with its recent report to improve the talent inside the government's cybersecurity workforce.

“The seriousness of the nation’s cybersecurity workforce gaps merits a high-level initiative to raise awareness and create a sense of urgency about the importance of growing and sustaining a world-class cybersecurity workforce,” according to a report to the White House by DHS and the Department of Commerce.

Demand and Supply

DHS’ other overarching themes for this year cover three worthy areas of focus: Strengthening the Nation’s Cybersecurity Ecosystem; Tackling it Together; and Securing Critical Infrastructure from Cyber Threats. They address the ever-increasing agility and variety of cyber attacks, including the report this week by Bloomberg Businessweek that Chinese spies infiltrated nearly 30 U.S. companies via a tiny microchip inserted into motherboards during their trip through the supply chain. They stress the importance of a “whole of nation” effort to defend against those attacks, and the threats to essential services highlighted by a DHS alert earlier this year about a Russian cyber campaign targeting U.S. power grids, government entities, the aviation and water sector, and essential manufacturing industries.

All of those efforts, however, ride on having a workforce big enough and skilled enough to handle the ever-expanding Hydra head of malicious cyber activity. And that’s an area where government agencies, and pretty much everyone else, is coming up short. Market researcher Cybersecurity Ventures projects that there will be 3.5 million unfilled cybersecurity jobs globally by 2021. The growing shortage is reflected domestically in current numbers from the Computing Technology Industry Association (CompTIA), which in June reported that there were 301,837 cybersecurity job openings nationwide, with 13,610 of them in the public sector. DHS, in announcing the National Cybersecurity Workforce Framework in August, put it simply: “The number of cybersecurity-related jobs already outpaces the number of people qualified to fill them, and that demand is growing rapidly.”

The shortage has been highlighted in several recent Government Accountability Office reports recommending that DHS and other agencies needed to take "urgent action" to identify critical skill requirements and, among other things, assign employment codes to cybersecurity positions.

A GAO report in April detailed steps Federal agencies needed to take to identify skills gaps, recruit and hire personnel, and promote cyber and STEM education. Congress also has put its weight behind those efforts, with the Federal Cybersecurity Workforce Assessment Act mandating that agencies identify gaps and revise the coding for cyber jobs, and conduct annual assessment of those skills gaps beginning in December of this year.

Through the framework and other efforts, agencies have launched a number of initiatives to attract and retain talent, as well as support development of the next generation of cyber workers. DoD, for example, has hiked the pay grades and incentives for cyber warriors and is looking to speed up the recruitment and hiring of personnel through the Cyber Excepted Service, which lets it work outside of the USAJobs platform. The National Initiative for Cybersecurity Education (NICE) also provides a common lexicon for cybersecurity work, to help define jobs and provide guidance on workforce development.

Uphill Battle

But it's still a steep climb towards a full cyber workforce, in light of both the global shortage of skilled workers and the challenges that government agencies have in competing with the private sector for talent. For one thing, the pay gap between what an agency pays compared with the salaries from the likes of Google, Apple or Amazon, or the potential payoffs of having a piece of a promising startup, is too large for agencies to overcome with purely monetary incentives. The lengthy process of security clearances presents another hurdle, as does, in the case of the military, the requirement that most of its cyber warriors need to enlist.

However, the programs in place has shown some positive results, as are some of the government's outreach programs. In some cases, potential cyber personnel aren't aware of the opportunities that exist in government, which circles back to the quest to raise awareness on all things cyber. At a recent forum on cyber warfare hosted by the Army and including representatives from the National Security

Agency and industry, several speakers talked about college students and other young people they'd met who were surprised to hear about what the U.S. Cyber Command does, and who were attracted by the idea of service to country.

There are no guarantees that the demand for cyber workers will be met, but initiatives underway and programs could be moving in the right direction.

View printer friendly version
Federal Cybersecurity
Department of Homeland Security
cyberattacks