Closing the Cyber Workforce Gap by Improving the Pipeline

Agencies across the federal government offer programs to stoke interest in federal cybersecurity careers.

James Mersol

Tue, 05/28/2019 - 11:42

Photo credit: elenabs/iStock

Although cybersecurity is a topic that receives a great deal of attention these days, that attention is not reflected in the strength of the cybersecurity workforce. Not only does the federal government face current challenges with hiring and retention, but also survey data predicts a looming information security shortage globally as educational programs fall short of demand for cybersecurity expertise.

The good news, however, is that the government is meeting this problem head on, implementing several extracurricular programs, reskilling courses and hiring reforms to address the shortages in both the short and long term. Moreover, these shifts reflect the government's changing perspective on its cybersecurity workforce, the first steps in a culture shift that will encourage cybersecurity employees to seek careers with the government and remain on that career path for years if not decades.

The International Information System Security Certification Consortium's most recent cybersecurity workforce study indicated that 63% of the nearly 1,500 information security professionals surveyed did not think they had "enough workers to address current threats." Moreover, 59% said that the gap posed "extreme or moderate risk" to their organizations. Closing this gap is essential not only to defend against present threats, but also to innovate in a field where both the threats and the technology are constantly evolving. In sum, the study reports that there are 2.93 million unfilled cybersecurity positions worldwide.

Within the federal government, 87% of the 2,620 information security professionals surveyed said that "hiring and retaining qualified information security professionals" was either somewhat important or very important to securing their agency's infrastructure, making it the No. 1 factor for security in the survey. 69% said there were too few cybersecurity experts in their agency, citing hiring, retention and "insufficient understanding of the requirements for information security" as the top reasons for the shortage.

These surveys paint a grim picture for both the short and long terms of cybersecurity. However, the federal government recognizes the potential impact of the cybersecurity gap and that it must take steps to find a solution that trains new cybersecurity professionals to meet the current shortage, incentivizes them to remain in the field and educates the next generation of cyber experts.

Guidance from the Top

To standardize qualifications, roles and career paths for cybersecurity roles across all federal agencies in order to increase transparency for workers unsure what direction to take their careers and to encourage information sharing across federal agencies, NIST in 2017 established the National Initiative on Cybersecurity Education (NICE), which published the Cybersecurity Workforce Framework (NICE Framework). The NICE Framework outlines goals for the federal cybersecurity workforce and designs a taxonomy for breaking down an agency's workforce into categories, specialty areas, work roles and knowledge, skills and abilities.

President Trump on May 9 signed the Executive Order on America's Cybersecurity Workforce, which recognizes that "a superior cybersecurity workforce will promote American prosperity and preserve peace" and calls for rotational programs between the Department of Homeland Security and other agencies, implementation of the NICE Framework throughout government hiring and contracting requirements, and funding for cybersecurity education, among other initiatives intended to bolster the numbers of U.S. cybersecurity experts.

The most important part of the equation alongside IT modernization and treating data as a strategic asset is "getting talent to the table," said federal deputy CIO Margie Graves at the May 15 AFCEA Law Enforcement and Public Safety (LEAPS) Forum. "And it is the one that I think is the most challenging because, not only in government, but also in industry, we don't have as much of a pipeline as we would like for cybersecurity specialists or data scientists."

Despite the challenge, Graves is optimistic. She said that legislation from Congress, policies from federal government, and guidance from the Office of Management and Budget (OMB) all point to developing that pipeline and training federal employees in critical cybersecurity skills. Moreover, these policies are already encouraging partnerships between the federal government and universities across America, further extending that pipeline.

The good news for everyone concerned about the cybersecurity gap is that these national directives are only a small part of a whole-of-nation effort to close that gap. Through programs encouraging students from elementary school to graduate school, as well as efforts in multiple agencies to attract cybersecurity experts to federal careers, the government is ensuring that the U.S. will have the "superior cybersecurity workforce" that it needs.

The Next Generation of Cybersecurity Experts

The 2017 Global Information Security Workforce Study (GISWS) found that "68% of workers in North America believe [the] workforce shortage is due to a lack of qualified personnel," highlighting a need to train students now so that they enter the workforce ready to fill that gap. The government is sponsoring programs to encourage the next generation of IT and cybersecurity professionals.

One such program is CyberPatriot, which receives funding from the Department of Homeland Security. It has held cyber defense competitions for the past decade, and as of October 2018 featured 6,387 registered teams from all 50 states, Puerto Rico, Guam, the U.S. Virgin Islands and Defense Department schools around the world. 77% of CyberPatriot competitors have gone on to pursue STEM majors in college. Additionally, in recognition of the gender gap in the IT field – 90% of the surveyed workforce is male – all-girl CyberPatriot teams pay no registration fees.

Tim Amerson, director of cybersecurity management in the Office of Information Technology for the Department of Veterans Affairs, has been coaching a CyberPatriot team for the past four years. He said that many of the students he has coached have decided to pursue STEM-related majors and careers, many of them changing their plans from before they joined the team.

Even when the "curriculum isn't doing it," Amerson said, referring to STEM education, CyberPatriot exposes students "to the latest information constantly," ensuring they're learning about cutting-edge threats and solutions to cyber risk. CyberPatriot gives these students "six to seven years of experience and exposure" if they join a team in middle school, Amerson added, enabling some students to enter the cybersecurity field as skilled professionals without needing to earn a college degree.

That approach may seem counterintuitive, but it matches with the data – twice as many surveyed information security professionals considered relevant knowledge and experience essential qualifications for cybersecurity roles than those who said an undergraduate degree in cybersecurity or a related field was essential.

Outside of the federal government, the SANS Institute runs two programs aimed at getting students involved in cybersecurity careers. The first, Cyber Fasttrack, is an online program that teaches current college and graduate students (as well as recent graduates of those programs) skills such as intrusion detection, network forensics and penetration testing, with the goal of connecting top performers in the program with scholarships and hiring opportunities. In March, SANS introduced its second program, CyberStart, intended to offer a similar range of courses in those skills to current high school students.

The SANS Institute's programs are based off of the United Kingdom's Cyber Discovery Program, SANS Institute Founder Alan Paller explained at the DHS S&T Cybersecurity and Innovation Showcase March 19. The U.K. government sought to identify 600 "elite-talented" specialists – those who would be not only able to learn the skills needed to become cybersecurity professionals, but also displayed certain aptitudes, such as tenacity, curiosity and problem-solving, that indicated their chances of becoming leaders and innovators in the field.

The Cyber Discovery Program was wildly successful, Paller said. While the initial target was to identify those 600 elites in four years, the program identified 700 elites and 250 "super-elites" in only six months. The pilot program for CyberStart, which enrolled female students in 16 states, was similarly promising. 36% of girls in the program said they were interested in cybersecurity at the start of the program; following CyberStart's conclusion, 70% were interested.

These programs could lead students to pursue careers in agencies that many do not initially consider when thinking of cybersecurity. For example, most grads might think of the Defense Department or Department of Homeland Security, but not the Department of Health and Human Services, said HHS CISO Janet Vogel at the 2019 RSA Federal Summit.

"We protect the health information for 1 out of 3 Americans," Vogel said. "We use that information to reach out to people."

Even if federal law enforcement draws cybersecurity grads, most expect to work in Washington, D.C., not Clarksburg, West Virginia, said Brian Griffith, IT management section chief for the FBI's Criminal Justice Information Services (CJIS), which is headquartered in Clarksburg. CJIS had difficulty convincing cybersecurity professionals to relocate, but has found recent success recruiting new hires from IT and cyber programs at West Virginia University, Carnegie Mellon University, the University of Pittsburgh and other local universities where students are more likely to be locals interested in remaining close to home, Griffith said.

Reskilling Today for the Jobs of Tomorrow

In the short term, the Federal CIO Council, a part of OMB, has partnered with the SANS Institute to create the Cyber Reskilling Academy. Like CyberFasttrack and Cyberstart, the Cyber Reskilling Academy's goal is to identify government employees outside of the CIO's office who possess the aptitudes that indicate their ability to acquire skills in cybersecurity quickly; the full-time program gives its trainees the skills to become a cyber defense analyst in just six months. In that time, students will learn the essentials of computing, network architecture, programming, and the Windows and Linux operating system, Paller explained.

The Cyber Reskilling Academy has already proven as popular as the programs for high school and college students. "We had 25 slots set up with the SANS Institute to do an assessment of existing personnel within our government," said Margie Graves. "We thought maybe we would have a couple hundred applicants. We had 1,517 applicants for this particular [program]. We hope to scope and scale it appropriately in the future."

Following the tremendous number of applications for the first cohort, OMB accepted applications for the Cyber Reskilling Academy's second six-month cohort, which starts on July 8. Should its success continue, said federal CIO Suzette Kent, future cohorts will focus on skills for positions other than cyber defense analyst roles, further increasing the options for those who complete the program.

Improving the Personnel Pipeline

Although the government is taking steps to train both the current and next generations of cybersecurity professionals to help close the global gap, the educational programs in schools especially will not pay dividends if those students choose careers in the private sector over federal cybersecurity positions.

The government cannot afford to overlook that many cybersecurity professionals leave the government for the much higher salaries and other perceived incentives that the private sector can offer. “That’s legitimate – it’s the American dream,” said Shane Barney, CISO for U.S. Citizenship and Immigration Services. “But at the same time, it really hurts us. That’s a difficult gap to breach. At the end of the day, some say money’s not everything, but you usually say that if money’s not that important to you.”

Hiring the right people is a “perennial challenge” for the government, said Vivek Kundra, the first federal CIO, speaking at the May 7 Cloud Security Alliance Federal Summit. He recommended that the government, at the OPM level, redesign its hiring procedure towards not only cybersecurity professionals, but IT professionals overall.

“You’ve got to fundamentally rethink not just the hiring process in government, but also how to build the pipeline,” Kundra said. “For too many functions, you have to struggle until a position is open and then put in a hire. That model is broken – it just won’t work. You need to be able to forecast need and to flex up and down in terms of people.”

A flexible, proactive hiring process is only one part of the equation, he added. “You have to invest in terms of training and enablement from the people that are already on board,” he said. “There are a lot of people who are hungry [for cybersecurity careers], it’s just that the career paths aren’t there.”

For federal agencies, the challenge is attracting new cybersecurity professionals, although the ones who join find job satisfaction. Agencies admit that they could do more to address the difficulties in hiring new cybersecurity professionals, especially when it comes to the application process.

“If you search USAJobs for product owner or product manager, nothing comes up across the whole federal government,” said Drew Myklegard, executive director of API management at Veterans Affairs, speaking at an April 9 government entrepreneurial breakfast. “We’re rewriting our [position descriptions], we have [GS-2210 hiring qualifications] so we can direct hire talented people.”

OPM has issued a special hiring authority that should make that process a lot faster across government, added Graves.

“You can decide within your agency where your biggest need is and you can go after direct hires in those arenas,” she said. “That’s a major step forward.”

The Importance of Mission

Industry-wide, 68% of information security professionals surveyed in 2017 said they valued working for an organization “where their opinions are taken seriously,” and 62% of those surveyed said they wanted to work in a place where they could “protect people and their data.”

In this respect, federal agencies can and do offer rewarding work to cybersecurity professionals, so long as they view the work as integral to the agency’s mission rather than a function ignored by senior leadership.

This perspective contributes greatly to the satisfaction of professionals in the VA, for example.

“It’s kind of an easy job for us,” said Dominic Cussatt, deputy CIO at the VA. “The respect our workforce has for our constituency and the pride in the work they do to support the veterans is just there.”

Advertising the importance of that mission may prove key to attracting to cybersecurity jobs within the government, especially in agencies that IT jobseekers have historically overlooked.

Graves agreed that the mission is a “powerful weapon” for recruitment. “If you can go to work in the federal government and address the big problems that are facing our society — like the opioid crisis, like law enforcement, like all of the other great issues there are in the federal government — that really resonates with people,” she said. “They want to make a difference, they want to do something on a daily basis where they’re proud to serve.”

Long-Term Growth for Agencies and their Cybersecurity Staff

Focusing on mission rather than specific skillsets is beneficial not only for the federal cybersecurity workforce, but also for the long-term growth of the agencies that they serve, said FBI’s Brian Griffith.

“As we move to an Agile workforce and the idea that people work as part of teams, you really don’t need a few specialized people within the enterprise,” he said. “We focus on hiring personality types rather than hiring specific skillsets. [We] hire people with the desire to learn and grow … and those who see the mission and want to be part of it because the technology is going to change.”

Providing both training and a clear career path is a major incentive that federal agencies can provide. “Once you get more talent in, they know what a career of a product owner or a product developer looks like,” said Myklegard. “The next challenge shouldn’t be the next GS level … It’s about outlining the trajectory of where an individual wants to go.”

The federal government’s plans are in line with what information security professionals say is crucial to encourage employee retention. In the 2017 GISWS , “offering training programs” and “paying for security certification” were tied for the most important initiatives for retaining information security professions in the federal government, with 62% of respondents saying they were “very important.”

Rewriting requirements and qualifications for cybersecurity positions will also incentivize cybersecurity professionals to pursue long-term careers – not just positions – with the federal government.

“We’re writing sequential job descriptions as [our employees’] skills mature and evolve,” said Cussatt. “We want to build a process that’s responsive to the constant change of technologies and practices. We have a very good training budget, but people weren’t taking advantage of it because they didn’t know what they needed to take or how to grow. We’re giving them some direction.”

View printer friendly version

cybersecurity
workforce
training
Federal CIO
veterans affairs
FBI
NIST
Trump Administration
Standard