DHS Tackles Cybersecurity Workforce Shortage With New Training Centers

CISA and a DHS S&T Center of Excellence will develop a nationwide network of cyber institutes for budding cyber professionals.

Kate Macri
Tue, 11/10/2020 - 12:41

The Department of Homeland Security's Science & Technology Directorate and Cybersecurity and Infrastructure Security Agency (CISA) awarded $2 million to the Critical Infrastructure Resilience Institute (CIRI) to develop a network of cybersecurity institutes to train the next generation of cyber professionals and crush a ballooning cyber workforce shortage.
CIRI, led by the University of Illinois at Urbana-Champaign, is one of the DHS S&T Centers of Excellence and already focuses on cybersecurity in its research and development efforts for the agency.

Together, CIRI and CISA will conceptualize and plan the network of cybersecurity institutes.

“The goal of the plan is to build out this cyber institute notion, but it won't be like the COE because it will be more like a training institute,” Gia Harrigan, program manager at DHS S&T, told GovernmentCIO Media & Research.

It all started in April when CISA asked Rob Karas, CISA’s associate director of cyber defense education and training, to form a task force to address the cybersecurity workforce shortage. At the time, CISA estimated there were approximately 300,000 unfilled cybersecurity jobs.

Now, there are upward of 500,000 unfilled cybersecurity roles across the public and private sectors, which CISA considers a national security risk.

“It's just growing,” Karas said of the shortage. “It's everywhere. You look at California, Idaho, Oregon, Florida. This is a risk because the landscape has changed. Forty years ago we talked about borders and walls. Now it's all digital, and attackers could be anywhere in the world. We don't have qualified professionals to address this. We need to ramp up to face this threat.”

The solution, he said, is establishing technical training centers where four-year cybersecurity degree students can study toward a concentration in incident response or control systems. But Karas wants the program to be open to everyone regardless of demographics or educational background.

“The content we're creating can also stand alone; it can be just a technical trade school,” he told GovernmentCIO Media & Research. “Someone doesn't have to go four years of college to get into the cybersecurity field. We have some minimum numbers — we want to make sure we're inclusive of various groups, rural groups and underserved populations.”
CISA and CIRI are still deciding how many hubs they want to have, how many universities will work with CISA and what kinds of scholarships, internships, curriculum and hands-on training to develop. Harrigan said part of the planning process involves figuring out a sustainable business model for the institutes.

“It's a big jigsaw puzzle,” Karas said.

Karas’ task force is taking notes from DHS S&T’s PISCES program, which connects cybersecurity students with needy local governments for hands-on cyber experience.

“We're running it up in Western Washington State University,” Karas said. “Students are actually getting hands-on ability, they're reviewing logs, and if they see any bad traffic they create a report and send it to a state fusion center. So these students are actually getting hands-on training at universities. They work with local governments that don't have the resources, so they're getting free resources and students are getting training on how to do day-to-day activity.”

Karas doesn’t worry about Silicon Valley or critical infrastructure companies poaching newly minted cyber professionals from his cybersecurity institutes, though. He’s more interested in hacking away at the workforce shortage across the board.

“If I can create 600,000 professionals, we'll have an oversupply,” he said. “My job right now is just to fill that gap, whether for the federal government or CISA or a water company in Lincoln, Nebraska. Of course I have openings at CISA I want to fill, but the bigger goal is to put a dent into that half a million job openings. We need to change the supply [and] demand, it needs to be backward.”

CISA’s new cybersecurity institutes could also demystify the hiring process at federal agencies and private companies. Organizations reskill one-third of cybersecurity hires, Karas said. Most new hires don’t have the exact skills the job calls for.
“We're a big advocate of hands-on training and learning and also tying all people's skills that they've learned back to [the NIST NICE cybersecurity] framework,” Karas said. “The NIST NICE cybersecurity framework tells you what skills you need to be an incident responder, so our training will tie back to that framework, which will be tied to different job roles.”

Karas said the program should be up and running in about two to three years.