

## Partnerships in Focus for Cybersecurity Efforts at Health Agencies

Agencies find opportunity in increasing diversity within cyber programs and leveraging shared services.

[Faith Ryan](#)

Wed, 01/22/2020 - 10:42



Photo credit: Funtap/iStock

As the federal government navigates an evolving cyber-threat landscape, health agency officials are increasing their attention toward expanding workforce recruitment, training and retention efforts to better safeguard personal health information.

The main focus of these efforts include cultivating a diverse workforce, as well as raising awareness within and across different agencies of the available shared tools and services available to everyone, health officials said during last week's Health IT Summit.

The Food and Drug Administration is one agency that wants to bring in diverse perspectives to strengthen cyber protection efforts.

“We want to have a workforce where everyone’s opinions are valued and respected and are able to contribute to a holistic program where we don’t just have one mindset and one background,” said Leah Buckley, director of counterintelligence and insider threat at FDA. This includes enticing more women into the short-staffed field and hiring people from various backgrounds and sectors, ranging from students who’ve just graduated from college to active-duty military members, to join its growing cyber teams.

With concerns over the overall low percentage of women working in cybersecurity in the public sector, Buckley highlighted contrasting efforts at the FDA in which women make up 31% of its cyber workforce.

FDA also is improving employee professional development opportunities and retention rates through biannual employee review processes, prioritizing training and career development plans, and offering telework days. About half of the agency’s employees have worked for the federal government for less than five years, while over 90% of those employees are looking to grow internally, Buckley added.

To prepare for the next generation of workers, the Department of Veterans Affairs is identifying new ways to improve and train the workforce using the NICE Cybersecurity Workforce Framework, noted VA Cyber Workforce Management Director Stephanie Keith.

Still, there are gaps in the framework for health security job roles.

“We are looking at how we develop what that goal looks like,” for health care technology managers, biomedical informaticists and biomedical engineers, Keith said.

That's why Keith's office has created a Cyber Workforce Development Management Program to identify and define those missing cyber position requirements and goals, as well as a Cyber Training Academy to provide its employees with baseline that can transfer across VA and other agencies.

"I'm about federal national standards," Keith said. "How do we leverage this across the board?"

Sharing information and services across agencies is also necessary for critical cyber support, said Janet Vogel, CISO at the Department of Health and Human Services. With 416 potential threats a minute, addressing traffic as effectively as possible is one of her agency's top priorities, she said.

Vogel noted the value of adopting a continuous diagnostics and mitigation program from the Department of Homeland Security, which has allowed the agency to respond very quickly to those incoming threats.

Still, many agencies are largely unaware of available shared services, like LookingGlass and Einstein, noted National Institutes of Health CISO Jothi Dugar. Dugar suggested that educating agencies and their personnel of what's available to them could advance agencies' security efforts.

She also suggested that educating potential applicants on the breadth of careers available to them in the field matters equally as much for attracting a diverse workforce.

"The beauty of security is that you can get it from all kinds of different angles," Dugar said. "Even if you're an art major or an English major, you need to be able to communicate. You need to be able to speak the language of the person you're speaking with."

Moreover, public-private partnerships can help achieve these goals, said VA CISO Paul Cunningham.

"If somebody thinks there's a barrier to come into cybersecurity, whether it's a diversity issue or maybe a geographical issue, we need to look to see how to remove that barrier so it's not there," he said.

[View printer friendly version](#)

[cybersecurity](#)

[health](#)

[HHS](#)

[CDM](#)

[FDA](#)

[veterans affairs](#)

[Standard](#)