Remote work is changing the way federal agencies think about cybersecurity. Now federal agencies are shuffling their cyber priorities to address new challenges brought on by the COVID-19 pandemic.

If federal agencies focus on just two things in their cybersecurity strategy, they should be zero trust and edge security, according to federal IT leaders at multiple virtual events last week.
“We have the ability now to work from anywhere, and in some ways the imperative given the current situation, but I also think that's going to drive long-term change for how we do work,” said Kevin Stine, chief of the applied cybersecurity division at NIST's Information Technology Laboratory. “Increased emphasis on the endpoint and protecting that data, whether it's on your local network or sitting on a laptop at your house, those are the types of capabilities I think we had a decent understanding of, but really need to ramp up our understanding and make sure the capabilities we have in place match the actual current environment.”

Because remote work is such a dynamic environment, federal agencies should be adaptable and flexible about how they think about cybersecurity and IT operations, especially when working with the private sector.

“The threat environment changes very rapidly,” Stine said at a Cyber Best Practices NextGov event. “Given this, we like to encourage folks to focus on outcomes as opposed to fine-grained contractual requirements that dictate a solution when there could be multiple solutions or approaches from a security perspective. I think that's allowed innovation to flourish.”

Robert Costello, executive director of enterprise networks and technology support at Customers and Border Protection, said the agency thinks about edge security and IT operations in terms of the end user first.

“Our job as federal employees is to be effective,” he said at an AT&T event on edge security. “I have to understand while I may not be out there, what it's like to be a border patrol agent with limited or no connectivity. They don't care if it's 4G or 5G as long as they're getting the connectivity they need. Do you have the connectivity to do your mission?”

Costello also encouraged federal agencies to “partner closely with your CISO” and break down organizational silos within their IT departments to allow a closer-knit relationship between software developers and security professionals.

“I have the privilege right now of leading a software shop, but I'm merging it a little bit with our infrastructure shop because the application is now the network and the network is now the application,” Costello said. “We need to drive that from the top down.”
Because of the rapidly evolving threat environment, federal cyber leaders at CISA and the GSA recommend agencies adopt a zero trust approach to cybersecurity. Zero trust is an IT mindset uniquely suited for telework.

“When the pandemic hit ... we did migrate off a legacy service provider to zero trust,” Costello said.

Allen Hill, acting deputy assistant commissioner for category management at the General Services Administration, thinks agencies need artificial intelligence and automation to improve cybersecurity.

“Agencies need to build on a zero trust architecture,” he said at the AT&T event. “We need our networks to be smart with security built in them, not on them. This is why automation of a secure network is so important.”

Daniel Ragsdale, assistant director for cyber in the Office of the Director of Defense Research and Engineering at the Defense Department, said agencies should think about zero trust as a way to be “threat-informed.”

“Zero trust doesn't mean no trust, there has to be some root of trust,” he said at the NextGov event. “On the device itself, there are some hardware issues we have to be cognizant of. There are vulnerabilities that can exist with regard to firmware — that's another attack surface. And then the applications.”

The reason zero trust is so important comes down to the fallibility of human employees. Humans will make mistakes, and compromise network security. Zero trust accounts for that, he said.

In a telework environment, shifting to a zero trust architecture might be the single most important move a federal agency can make to dramatically improve its cybersecurity.

“We can have a nearly perfectly secure stack from the hardware on up through the application, but we will still have end users susceptible to manipulation; they will make mistakes,” Ragsdale said. “All of us have received information through these mediums that prompt an emotional response, and sometimes our judgment is not where it needs to be.”

View printer friendly version
Federal Cybersecurity
GSA
CBP
DOD
NIST
Zero Trust
edge security
Standard