Zero Trust's Role in TIC 3.0 Strategies

The COVID-19 pandemic-induced telework prompted federal agencies to build off TIC 3.0 guidance and explore zero trust to maximize network security.

To support these efforts, CISA TIC Program Manager Sean Connelly said the agency will release telework-specific TIC 3.0 use cases, which he described as “upcoming” in an ATARC webinar earlier this month.
“There’s a number of items we want to tackle — [software-as-a-service] and [platform-as-a-service] use cases, email-as-a-service, and also zero trust,” Connelly said during the event. “Everyone wants to leap forward to zero trust so we're looking forward to what we're doing to support that also. Our major focus right now is on the architecture and getting the use cases out the door.”

Sara Mosley, strategic architect at the Department of State, sees TIC 3.0 and zero trust as facets of a new security philosophy cut and polished by the pandemic.

“There are synergies there between TIC 3.0 and zero trust architecture,” Mosley said during the event. “The difference is TIC 3.0 is a mandate. We have to work through the implementation and make sure we meet the mandate. In terms of zero trust, it's more an objective for most of us. It's kind of the panacea. In some cases it's become a marketing term. For us at State, we're trying to identify basic requirements that we see as far as what zero trust is. We've got some examples right now of implementation [of TIC 3.0] that have some of the characteristics of zero trust.”

The proper approach to zero trust, she added, is through data.

"We need to move closer to the data," she said. "How do we get closer to data and start now breaking down specific data requirements that we can now adjust our architecture to meet those zero trust mandates? We can't do it all at the same time, it's just not going to happen. What is our most critical data, the most sensitive, and start with those applications that are related to that data."

Trafenia Salzman, a security architect at the Small Business Administration (SBA), agreed. SBA is working on both TIC 3.0 and zero trust implementation.

“Look at your data because zero trust moves more toward your data as opposed to your physical perimeter,” Salzman said. “From there, look at your identity, who's accessing it, from there your network, and from there your assets (like monitors and computers). That's how I would move into zero trust.”

When modernizing IT infrastructure, federal agencies should keep TIC 3.0 guidance and zero trust principles in mind — especially when drawing up contracts with private-sector vendors.
“We’ve been promoting this idea of modernization in three main areas,” said Justin Morgan, solutions architect at General Services Administration. “Transition your traditional [time-division multiplexing] (TDM) circuits to ethernet, move from legacy voice to IP voice as a service, and get a better idea of your traffic patterns and inventory. What you have, where you’re going, and how that all fits together. When you’re architecting a new network, now would be the good time to look at TIC 3.0 or zero trust because you’re looking at your environment holistically. Try to lay that out in your solicitations.”

For federal agencies considering a zero trust approach, Mosley advised taking it slow, and implementing in phases.

“Some of the challenges we’re seeing is integration,” she said. “Really looking beyond the network — as an IT and network person, you’re looking at your stack to check protections. ... The awareness has to be up the stack at the application level, at the user level, you need to understand how the user works.”