Next-Gen Cybersecurity Must Account for Complexity and Variability

A revolution in remote work and internet of things necessitates cybersecurity measures that cover the corresponding risk.

Adam Patterson
Thu, 09/03/2020 - 14:36

The abrupt mass shift to remote work amidst COVID-19 and ongoing adoption of "internet of things" capacities have presented newfound challenges for protecting sensitive data, adaptations that have required an evolution in cybersecurity methods to ensure federal systems are properly safeguarded.
Much of this has emerged from the publication of the third Trusted Internet Connections (TIC) initiative that updates security standards to accommodate the increasingly dynamic nature of federal IT systems that rely on mobile devices and IOT. The newly published TIC 3.0 provides guidance for federal agencies looking to protect the integrity of their networks when users are geographically dispersed and using either mobile or personal devices.

“Agencies are allowing more branch offices to connect to cloud environments," said Sean Connelly, TIC program manager at the Cybersecurity and Infrastructure Security Agency, during the GovernmentCIO Media & Research [CyberScape virtual event Wednesday](#). "These are alternative ways to secure their data and have their users access their data … We have interim telework guidance, and we’re looking to release that before the end of the year."

“TIC 3.0 is less about the specific interconnectivity of the network segments, and it’s more about the data integrity, data security and resiliency of the entire system including the network,” added John Fanguy, chief technology officer at Micro Focus Government Solutions.

Much of the evolving federal cybersecurity paradigm rests on the merging of previously separate areas of data protection, including a newfound merging of privacy and security standards designed to simplify information management in a remote work environment.

“We've found that many privacy controls can be joined with security controls; they’re dual use. These new controls that are in the catalogue will be supporting our cybersecurity framework and privacy framework, and we are confident that privacy controls are so comprehensive that they will be able to cover things like GPR requirements and things of that nature,” said Ronald Ross, cybersecurity fellow at the National Institute of Standards and Technology.

One of the priority frontiers of federal cybersecurity development rests on the broader public sector cloud development program, with extant cloud migration having allowed for a much smoother transition to remote work.
“Moving to the cloud is another big decision we made prior to COVID. Because we moved to the cloud, it allowed us the flexibility to surge really quick,” said Timothy Amerson, director of infrastructure operations security management at the Department of Veterans Affairs.

Ross seconded this assessment, noting that the migration to the cloud and subsequent adaptation of federal cybersecurity standards has helped smooth this transition.

“Cloud has been a huge investment on the federal government’s part. We’ve also invested in mobile technologies and the TIC initiative. All of these allowed our federal workforce to become comfortable with telework since well before the pandemic,” Ross said. "Federal employees get fully loaded laptops, and mobile devices come with controls that are in the [NIST Special Publication] 800-53."

In evaluating the federal IT landscape, panelists recognized that management and reduction of complexity is a newfound security challenge government agencies will need to address.

“It’s going to take some discipline to understand the things you’re bringing into your network, and what are the parts of this large system I’m building,” Ross said. "You have to almost analyze each device and each component on its own. ... Our challenge as cybersecurity professionals is to show mission owners how to make this technology work for you so it can support your mission and do it in a way that is within their risk tolerance."

Despite the challenges at hand, the officials expressed confidence that the federal government would be able to adapt existing capacities around managing and reducing this newfound complexity.

“Agencies can move a lot of that complexity to the cloud ... with platform as a service, software as a service, and infrastructure. All of those things have been tested and can provide a high level of assurance for agencies to move some of that outside the fence. And for whatever stays in the fence, they can reduce that complexity and use behavioral analytics so every device and component you know has been approved,” Ross said.

View printer friendly version
Federal Cybersecurity