

How TIC 3.0 Will Enable Cloud, Remote Work

Early use cases create secure connections for branch offices and remote users.

[James Mersol](#)

Wed, 01/15/2020 - 16:21



Photo Credit: kanawatvector/iStock

As more and more federal agencies look to transition to the cloud, both to save costs by closing data centers and to give their employees greater freedom to work remotely, maintaining network security has been a stumbling block. Despite the security options that cloud providers offer, the transition still requires a rethinking of network architecture.

Up until last year, the previous guidance from the Office of Management and Budget on Trusted Internet Connections (TIC) assumed agencies' networks consisted almost entirely of desktop computers and fixed data centers. This assumption is not surprising, given that TIC 2.0 was released in 2008.

[Announced in September 2019](#), the TIC 3.0 guidelines aim to update that guidance for a federal IT environment that is increasingly mobile. The guideline documents are currently in draft as OMB and the Cybersecurity and Infrastructure Security Agency (CISA) seek public comment on both present-day use cases and how to ensure the guidelines can evolve alongside agency networks.

Rather than offer specific measures agencies must implement, the TIC 3.0 guidelines are designed to provide more abstract use cases, giving agencies the flexibility to adapt the program to their needs.

"These use cases we've recognized are very high level," said Sean Connelly, TIC program manager at CISA at ATARC's TIC 3.0 Briefing Jan. 15. "That's intentional to have a broad acceptance across the agencies ... to be able to support [a government-wide spectrum], we know the use cases could only go so deep. But we also recognize we have a gap to fill, and that's why we've come out with [use case] overlays."

Use cases currently outlined in the draft documents include connecting branch offices to headquarters and enabling cloud services in agency networks, Connelly explained. He mentioned that his office is working with GSA and OMB to explore potential use cases, such as the Zero Trust model, the "internet of things" and the GSA Enterprise Infrastructure Solutions acquisitions vehicle.

"This is a living document," said Connelly. "As we add more capabilities and find new objectives in the use cases, [the list of capabilities] will grow."

Connelly underscored that his office's main interest is in the "future of the enterprise." He envisions TIC 3.0 would allow agencies to move away from data centers and smooth the transition to a cloud environment.

TIC's previous iteration took over a year to finalize after the initial draft was published for comment. CISA is working to shorten the timeline this time around, Connelly said, and plans to publish the finalized documents in the next few months. He encouraged agencies interested in being early adopters to participate in pilot programs and promote what is working and what is not.

The National Oceanic and Atmospheric Administration was an early adopter of TIC 3.0 and is currently running four TIC access points in the continental U.S. and one in Hawaii, explained Deputy Director of Operations Chi Kang. Additionally, NOAA is sharing information with other agencies, including NASA, on TIC adoption procedures and architecture, especially regarding challenges with integrating TIC into legacy architecture.

The agency is also developing TIC use cases for mobile security, surrounding intelligent threat defense and heuristics for smartphones and other devices, Kang said. Like several other agencies, NOAA phones are currently government-furnished equipment, but many employees have expressed interest in using their own devices for work, he said. The use case, while still in its early stages, would allow NOAA to implement a "bring your own device" policy and share that procedure with other agencies.

The Department of State is another agency excited to adopt TIC 3.0, according to Gerald Karon, acting director of the department's Enterprise Network Management Office.

"TIC isn't for everything," Karon said, echoing what Connelly had said earlier. The new guidelines have helped the department find solutions for secure connections overseas, where the traditional secure network infrastructure may not exist at all.

Connolly added that the draft documents are [currently on GitHub and open for comment](#) until Jan. 31 and encouraged all agencies to respond to the request for comment either on GitHub or in an email to CISA directly.

[View printer friendly version](#)

[TIC](#)

[cloud](#)

[cisa](#)

[NOAA](#)

State Department
Standard