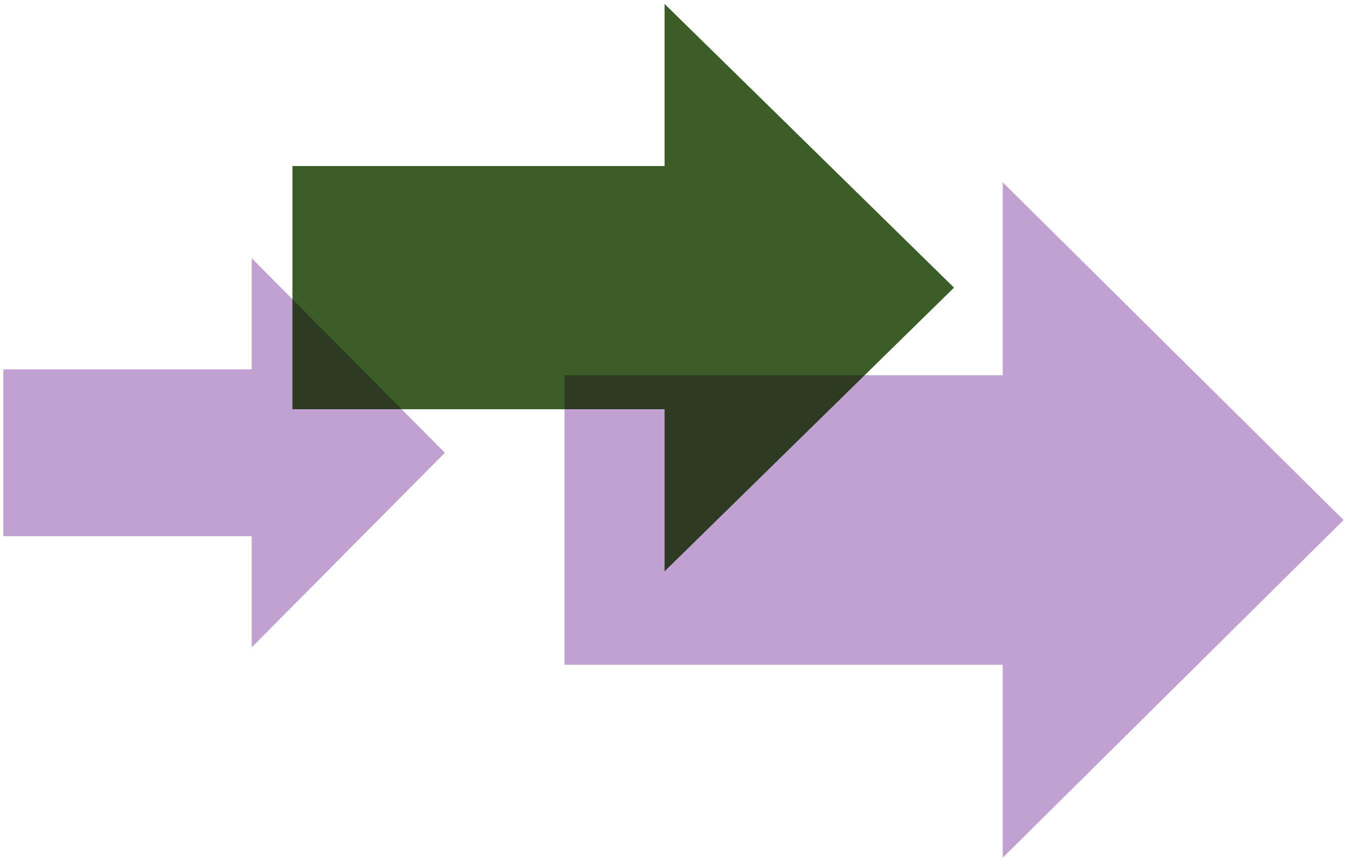

TIME FOR MODERN, SECURE NETWORKS: THE TIC 3.0 INITIATIVE

zscaler aws govloop

EXECUTIVE SUMMARY

Months after the publication of the Trusted Internet Connections (TIC) 3.0 policy, users still have questions. Despite the release of broadly defined use cases, employees across large and small federal agencies remain uncertain about the viability of their current network connections and the future of cloud computing security models.

That was the focus of a GovLoop roundtable event held in January in collaboration with Zscaler and Amazon Web Services (AWS), featuring TIC 3.0 policy leaders and representatives from several agencies across the federal government.

TIC 3.0 is the latest update to an initiative first designed to consolidate the number of network connections and attach defense and monitoring solutions to the security perimeter. The new policy reflects the evolution of enterprise security, which emphasizes the protection of data rather than the dissolving or constantly shifting perimeter.

Rather than directing agencies to shut down the perimeter, the policy provides them with a framework for defining different zones of trust within their environment – and it recognizes that agencies need the latitude to interpret TIC 3.0 based on the requirements of their specific environments.

The hope is that agencies won't have to bend over backward to satisfy TIC anymore. Instead, they can leverage the new use cases to find better ways to extend services to the distributed enterprise — remote offices and individuals working outside the traditional network perimeter — and provide a secure way to adopt technologies like cloud, mobility and the Internet of Things (IoT).

In this report, we provide a recap of the roundtable discussion, plus other sources to help you understand the evolution of the TIC policy.

Featuring insight from:

Sean Connelly
TIC Program Manager, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)

Jim Russo
Technical Director, Enterprise Infrastructure Solutions (EIS) Program, General Services Administration (GSA)

John MacKinnon
Global Telecommunications Partner Development Manager, Worldwide Public Sector, AWS

Stephen Kovac
Vice President of Global Government and Compliance, Zscaler

THE NEED-TO-KNOW CONCEPTS

Trusted Internet Connections Initiative

The Office of Management and Budget (OMB) launched the TIC initiative in 2007 with the intention of defending the federal government's network security through enhanced monitoring and fewer external connections. The government designated TIC Access Providers (TICAPs) to offer central gateways for single or multiple agencies' external network connections.

Fact: ***In January 2008, more than 4,300 external connections were linked to federal networks. TIC set a target of fewer than 100 total.***

TIC 2.0

TIC 2.0 came out as a follow-up in 2012, providing a new architecture for agencies to follow. Additionally, TIC 2.0 established security policies of "default deny, permit by exception" and implemented further requirements for TICAPs. TIC 2.0 still stands as the traditional — and standard — use case for TIC.

TIC 3.0

Released in 2019 as the new standard, TIC 3.0 adds three new use cases to the framework of the previous initiative, which remains the "default" use case. Addressing the use of the cloud and supporting remote offices and mobile users, TIC 3.0 allows agencies to define different trust zones in their environments, depending on the specific requirements of a given use case. "**To promote flexibility while maintaining a focus on security outcomes, the capabilities used to meet TIC Use Case requirements may be separate from an agency's existing network boundary solutions,**" TIC 3.0 guidance states.

Fact: ***TIC 3.0 was in development for more than three years. Additional pilots are still underway to finalize other potential use cases.***

Cloud Smart

The Cloud Smart policy, released in 2017, is an administration priority to prepare agencies for cloud transitions with a three-pronged approach of security, procurement and workforce. Cloud Smart specifically called out the need to update TIC: "With the proliferation of private-sector cloud offerings, the emergence of software-defined networks, and an increasingly mobile workforce, the TIC model must compete with newer, more flexible solutions that provide equal or greater security, or it must evolve as well."

Enterprise Infrastructure Solutions

Designed to help agencies upgrade their infrastructures, the $50 billion telecommunications EIS contract gives agencies access to managed security services known as Managed Trusted Internet Protocol Services (MTIPS), which are compatible with the TIC initiative.

Zero Trust

Zero trust is a security strategy based on a "never trust and always verify" mentality, and it emphasizes the constant protection of data instead of stagnant defense of the perimeter. As TIC continues to evolve to meet the times, a zero trust use case is in its future, officials say.

A NEW ERA FOR TIC: 5 TAKEAWAYS

The evolution of the TIC program – from TIC 1.0 more than 10 years ago to TIC 3.0 today – reflects how technology often moves in unexpected ways.

For example, early in the roundtable discussion about TIC 3.0, TIC Program Manager Sean Connelly reminded everyone about why TIC came about back in the mid-2000s. OMB had asked agencies to report their total number of internet connections.

No one had done such a count before, so OMB officials weren't sure what to expect. But they were still surprised.

"The number that came back was well over 4,000 connections – that was well above what anyone thought," said Connelly, whose position sits in CISA. "We realized that we had to get some way to control this."

The surge in cloud usage came as yet another surprise because cloud was just emerging as a viable platform when OMB issued the first TIC policy in 2007.

It's easy to forget that there was a time when people saw the cloud as having limited potential in government, according to Stephen Kovac, Vice President of Global Government and Compliance at Zscaler, a cloud-based information security company.

"In 2008, 2009, the key thing we did on the internet was surf, and check email," Kovac said. "I remember I used to call on [agencies], and people would say, 'I'm never going to put my data on the internet and the cloud. No way!'"

The roundtable discussion, which primarily involved representatives from federal civilian agencies, covered a wide range of topics, from the continued relevance of the original TIC vision to the uncertainty and excitement about how the program will evolve. **Here are five big takeaways.**

1 Legacy TIC Still Matters

For many years, feds have spoken about TIC in somewhat disparaging terms, given its incompatibility with the widespread adoption of cloud and emerging technology solutions. But one roundtable participant from a civilian agency reminded folks that TIC was an important breakthrough and provided a standard approach to securing internet traffic.

"When TIC came along, it just enabled us to do what we needed to do," the attendee said. "It helped us because we actually had the staff, the funding and the whole nine yards to funnel traffic in through the edge."

That said, the TIC model had its drawbacks, noted John MacKinnon, Global Telecommunications Partner Development Manager for the Worldwide Public Sector at AWS.

"We had an information superhighway – and a two-lane dirt road feeding that superhighway," MacKinnon said. "You are not going to have a great user experience in that environment."

Connelly added that the goal of TIC 3.0 is not to replace traditional TIC but to extend secure connectivity to more distributed environments.

"The guidance coming out from Federal [Chief Information Officer] Suzette Kent was, 'Get TIC out of the way for my users going to the cloud.' These use cases are just different examples of how agencies can connect the user systems to the cloud.

"Your traditional TIC, TIC 2.0, is still the primary solution. We've talked to a lot of agencies over the last month, and they're still interested in the traditional TIC being their primary architecture, and that's completely fine. What we're doing, though, with TIC 3.0 is providing alternatives for agencies to use."

2 No More `Easy Button′

One challenge for many agencies is that as TIC evolves and security gets built into solutions, the cost of security becomes more difficult to pinpoint.

For example, in the Networx contract, security typically was "bolted on" after a solution – an "easy button" approach to security, according to Jim Russo, Technical Director for EIS at GSA.

> "It was just that, an easy button. It was, 'OK, buy your transport,' and then, 'Oh here's the security, we just slip that on.' You didn't even have to buy it from the same provider. It was essentially a one-size-fits-all solution, and there was a cost for that investment," Russo said.
>
> "But with Enterprise Infrastructure Solutions, we started moving past that to a package-based solution – I wouldn't go so far as to say DevSecOps, but we did try to boil in security on a service-by-service basis where it makes sense. Agencies still have the ability to go buy everything separately and integrate themselves with an enterprise solution that includes cybersecurity."

Another factor, Russo said, is that with TIC 3.0, agencies might add secure capabilities that weren't even an option before, which makes cost comparisons difficult.

"Let's say you have a TIC 3.0 solution, and it's based on a [software-defined wide area network]," Russo said. "How do you compare that to what you had before, when you just had on-premises networks that were more or less static?"

That lack of clarity on costs can be a challenge for senior executives, said Connelly. It's not that the savings aren't there; it's just that you can't always get at them by comparing line items.

"One thing at the [chief information officer] and chief information security officer level is they want to know the cost difference," Connelly said. "OK, here's my old solution, here's my new solution, what's the cost savings and what's the changes? That's what's hard to articulate from the TIC perspective."

3 The Value of Use Cases

As part of the TIC 3.0 rollout, CISA is supplementing the core guidance with use cases that show how agencies can deploy TIC 3.0 to meet more particular requirements, such as support for remote offices or the adoption of cloud-based services.

The idea is to show agencies how to meet such a requirement while giving them the latitude to decide how they might apply that approach to their particular environments. That latitude requires a different mindset than a traditional mandate, Connelly said.

Some roundtable attendees worried that the lack of regular use cases would mean that the TIC solutions they piloted might become unusable as TIC 3.0 continues to roll out. Connelly emphasized that the new use cases were different from those in previous TIC models – as now, agencies define their own trust zones.

No longer are use cases prescriptive. Instead, now there's room for interpretation. And, of course, TIC 2.0 is still viable.

"My expectation is that the agencies will build interpretations of those use cases," Connelly said. "But there's no approval process, right? It's an agency interpretation; there's broad interpretation authority."

Use cases also could play a role in the acquisition process, said Russo, affecting how agencies define requirements and how vendors propose solutions.

> "On the agency side, your ask is a little different," Russo said. "It's not going to be as simple as picking services off menus. It's, 'I need to do this; here's my use case. Now, how do you guys solve it?' Then we give industry the place to create the solution set."

With the new TIC 3.0 model, Connelly said, agencies should be able to come together from similar situations and field shared solutions.

4 Get Ready for Zero Trust

Security experts have noted that TIC 3.0, with its focus on assigning trust scores to users and defining more granular “zones of trust” within a network, provides some building blocks for a zero trust architecture.

Zero trust, which was first defined by an analyst at Forrester Research in 2010, assumes that unauthorized users or systems are bound to get on a network, so it’s important to put security at the level of individual datasets, applications and other resources.

Connelly noted that interest in zero trust was high, although not all agencies were quite ready for it yet. He said:

“I have to be careful when I talk about zero trust in terms of TIC because there are some agencies that want to turn the whole architecture over to zero trust. From a TIC perspective, we need to be inclusive of the technology from 1999, if you will, and also from 2029. But we will have a zero trust use case coming out at some point.

“One thing to understand is that, typically, we only have one or two agencies doing a pilot for a use case. But there’s so much interest in zero trust, I expect we’ll have many agencies doing a zero trust pilot.”

One way to implement zero trust is to “separate the meat and the milk,” said MacKinnon. At any given time, an agency is likely being inundated with traffic from hostile actors, whether they are cybercriminals, nation-states or political hacktivists. So, how can they deflect these attacks while safeguarding user experience inside the system?

The goal is to focus on this traffic at the edge, via the cloud, and not let it reach the data center.

“I don’t want to have that stuff sitting in the same data center as mission-critical [assets]. Because if somebody overwhelms the firewalls and all the stuff is in there, then the fox is in the henhouse. This is another case for zero trust,” MacKinnon said. “In a traditional cybersecurity approach, I check your ID at the front door, then I let you go anywhere in my house. Wouldn’t it make any more sense for me to check your ID at the [network’s] edge with two-factor authentication, and then only allow you to go to the things I give you access to?”

5 Input, Please

Connelly closed out the roundtable by asking participants — and by extension, agencies across government — to get engaged with the discussion of TIC 3.0. In particular, CISA wants comments on the larger vision of TIC 3.0, he said, not just the specifics.

“Some people tend to use feedback to argue about something in the documents themselves – like, ‘Is internet spelled with a big I or small I?’ or “What’s the comma here mean?’

“What I’m really more interested to hear is more the programmatic stuff, how you’re going to use TIC 3.0. And even after the comment period closes, we’ll still talk to you. We are always talking to agencies one on one.”

Note: ***CISA and OMB were working on the TIC 3.0 policy for three years before finalizing it in late 2019. At the start of the decade, TIC 2.0 had a yearlong period before the use cases were finalized following their pilots. Connelly said not to expect that long of a turnaround this time around.***

THE FINAL WORD

Following the roundtable discussion, GovLoop caught up with Sean Connelly, the TIC program manager, to share some of his own takeaways.

Are there important elements of TIC 3.0, or TIC in general, that you don't want agencies to overlook?

Right now, there's still a lot of emphasis on the traditional TIC access point even though we moved toward TIC 3.0. And the reason you want to focus on traditional TIC access points to begin TIC 3.0 is, as we start to move away from that, agencies might forget about or stop using that traditional TIC access point, but it's still there. We've talked to a lot of agencies that still look at traditional TIC as their access point, so that's still a very viable solution for agencies to use. I talked to some agencies who said they're all in on zero trust or all in on this alternative use case. That's fair if it works for them, but also some agencies are perfectly comfortable using that traditional TIC access point.

What would you want attendees of the roundtable to take away from the event?

From TIC 1.0 to TIC 2.0, it was a few years between them, but it's been seven or eight years since TIC 2.0 came out, so it's been a large shift to TIC 3.0. Obviously, federal IT has improved. Cloud is a lot more relevant in ways that it wasn't seven or eight years ago. It's just these alternatives that are available for agencies to consider. It's a huge leap forward in terms of federal IT cybersecurity, but again, it really is up to agencies for how they want to adopt it. …

Last thing I'll wrap up with, with the roadshows and at a lot of events like yours, we've talked about the guidance itself, the structure of the documents. And I understand the importance of agencies having to build out architectures, but I think what we recognize is that in the federal enterprise of tomorrow, we know there's going to be more work performed off the enterprise network than on it. We know there's going to be more workloads running in the cloud than through traditional data centers, and more traffic in the cloud than in the data center itself. What's exciting to me is how we're moving the program forward to support those enterprise solutions of tomorrow.

How Zscaler Helps

Zscaler is built to help you move to the cloud securely while delivering a better user experience. With Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), agencies can safely connect their users and customers no matter the device, application or location. Unlike traditional approaches based on hardware appliances, Zscaler cloud-based solutions are fully scalable.

ZIA was the first TIC 3.0-approved secure internet and web gateway solution. By helping agencies go directly to the cloud and securely move mission-critical traffic, it removes latency from the process that regularly slows when using a traditional TIC solution or MTIPS. ZPA provides seamless and secure zero trust access to internal applications for authorized users. Traffic does not traverse the open internet, bypassing the need to go through the TIC. Zscaler is ready for agencies' transitions to the cloud under the new use case, leaving latency and static perimeters in the past.

Learn more at www.zscaler.com/government.

How AWS Helps

AWS is designed to meet the needs of government agencies on their cloud journeys. Authorized as FedRAMP-High, the AWS Cloud can service a variety of government missions securely on an affordable and service-based plan.

More than 5,000 government agencies already depend on AWS cwommercial-level clouds, selecting from either AWS GovCloud (U.S.) or more tailored offerings. Now, TIC 3.0 allows many more agencies to continue moving to the cloud securely and efficiently. After going to the AWS Cloud, agencies receive access to machine learning, mobility and citizen-facing services.

Learn more at aws.amazon.com/government-education/government

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop