World Wide Technology

Trusted Internet Connection (TIC) 3.0

TIC 3.0 Building Blocks

Federal agency IT and security teams need the right building blocks and tools to protect their systems as traditional network parameters disappear and threats increase as their TIC 3.0 journey continues.

Network connectivity is the foundational phase for agencies preparing for TIC 3.0. IT and security teams will need the right building blocks to accommodate a range of use cases. Operations teams will have to understand how network traffic and data transfers to and from remote offices and workers will perform in the new paradigm.

WWT can be your trusted solution provider to ensure your agency is ready to modernize its network architecture and lay the foundation for a Zero Trust strategy.

Overview

Trusted Internet Connection (TIC) 3.0 is needed now more than ever to strengthen cyber defenses in a world in which the network perimeter has become increasingly more amorphous, in alignment with guidance released by the Cybersecurity and Infrastructure Security Agency (CISA).

The transition to cloud and mobile environments, along with the increase in remote workers across the nation, heightens the need for cyber protection that can address agencies' distributed network requirements, including branch offices, remote users, and service providers.

TIC 3.0 is a response to the need for improved agility, security, connectivity, and visibility in federal government networks that can improve network performance and manageability, improve cybersecurity, increase operational effectiveness, and lay the foundation for implementing a Zero Trust strategy.

What's Driving the Need for TIC 3.0?

As Federal agencies have adopted cloud, mobile, and SaaS technologies as well as supported a larger remote workforce, their end users, applications, and data increasingly live outside of the traditional agency network boundary. TIC 2.0 and previous iterations of network architectures have focused on securing a physical, hub-and-spoke agency network perimeter leading to network bandwidth constraints, lack of agility, a degraded end user experience, and increasing costs.

The TIC 3.0 initiative aims to provide a more modern approach to network security and a better end user experience, giving agencies more flexibility to enforce security capabilities outside the traditional agency perimeter in these dispersed environments.

The WWT & Cisco Partnership

Our partnership with Cisco is rooted in our shared goal of driving value for our customers while helping them solve complex IT and business problems. Since first partnering more than 25 years ago, WWT has become Cisco's largest and most strategic global partner.

WWT and Cisco's shared holistic approach to security protects our customers' reputations, business assets and intellectual property, allowing them to achieve more effective outcomes and align security transformation to an enterprise architecture.

Together, WWT and Cisco collaborate on the latest best-of-breed technologies and multi-vendor solutions, aligning those with TIC 3.0 guidance to help agencies build a foundation for secure network access at the edge, and eventually transition to a Zero Trust architecture.

To learn more about WWT's Cisco capabilities, speak with an expert, or take advantage of one of our experiential interactive labs, please **contact us.**

The TIC 3.0 Experience with WWT

As federal agencies continue to rapidly expand their networks to meet new demands, they need an agnostic testbed for collaborative experimentation as they begin their journey from TIC 2.0 to TIC 3.0.

As noted by Sean Connelly, CISA's Program Manager for TIC 3.0, the latest guidance released to date is meant to serve as a starting point for agencies to help set the foundation for TIC 3.0 uses cases that will be a way for agencies to sponsor pilots and work with vendors on TIC solutions.

WWT has created a virtual environment specifically to address this need—to help them understand the differences between TIC 3.0 and previous iterations, along with why it is important to modernize—so that agencies can collaborate to design, build, educate, and deploy customized lab environments specific to their agency requirements.

The TIC 3.0 Architecture Lab is a capability of the Advanced Technology Center (ATC) designed to demonstrate how TIC 3.0 optimizes the end user experience, compared to that of TIC 2.0, providing customers an environment to gain hands-on experience to evaluate new cloud and infrastructure solutions for their respective TIC use cases.

The environment that supports the lab is a blend of physical and virtual infrastructure, purposely intended to highlight, and validate, the vast differences of prior TIC iterations and to create a realistic setting meant to help customers envision and evaluate their own TIC scenarios and flexible perimeters designed to protect diverse hosting platforms, improve security capabilities, optimize IT services, and ensure secure access to critical resources—all within an environment-agnostic approach.

With WWT's state-of-the-art TIC 3.0 Architectural Lab, agencies are able to better identify how TIC 3.0 can improve network performance and manageability, improve cybersecurity, and increase operational effectiveness.

WWT's TIC 3.0 Architecture Lab allows customers the ability to:

- Test network designs and the capability of SD-WAN to securely connect with the public Internet and cloud providers
- Work better remotely through the enablement of cloud adoption
- Experiment with trusted gateways for reliable bandwidth to locations CONUS and OCONUS
- Implement security in preparation for Zero Trust, across the entire data exchange from the laptop to branch offices, all the way to applications in the cloud
- Perform testing on end-user devices to simulate a remote user connection to the agency's traditional network, cloud, and the Internet
- Evaluate and optimize traditional TIC use cases
- Access TIC use cases to review results for environments with security requirements like their own
- Share and compare various TIC 3.0 solutions across agencies

Benefits to Federal Agencies

Access to Best-of-Breed Technology. Aligning the latest best-of-breed technologies and multi-vendor solutions with TIC 3.0 guidance will help agencies build a foundation for secure network access at the edge, and eventually transition to a Zero Trust architecture.

Remote Work Flexibility. TIC 3.0 provides the flexibility necessary to enable remote workers as well as the unified communications and collaboration tools they need to remain productive.

Improving IT Modernization. TIC 3.0 can improve network performance and manageability, cybersecurity, and operational effectiveness for federal government IT modernization.

Leveraging the Lab. This state-of-the-art collaborative environment provides agencies access to a secure integrated space with the ability to test and evaluate emerging technologies, shared services, and meet federal workforce expectations with simple, seamless access to applications and data.

Related Resources

TIC 3.0 Thought Leadership

The Transition to TIC 3.0: Ensuring Agency Readiness for Network Modernization

WWT-ATARC TIC 3.0 Webinar Recording

TIC 3.0: Ensuring Agency Readiness for Network Modernization

TIC 3.0 Architecture Lab

Meet the Experts at WWT

Eric Lundblad
Regional Manager
Federal Law Enforcement

Matt Oberhofer
Systems Engineering Manager
Federal Law Enforcement

Tim Robinson, D.Sc.
Practice Manager
Public Sector Security

Ryan Friel
Senior Consulting Solutions Architect, Federal Civilian

Steve Hollar
Practice Manager
Connectivity

Michael Pfeiffer
Cloud Networking Architect

David Vasek
Principal Solutions Architect