BROCHURE

Connected Security

with TIC 3.0

Summary

For agencies looking to modernize their IT, cybersecurity is front and center – and increasingly, security must be connected to and built into government networks. The Government Accountability Office (GAO) continues to note in reports that ensuring the cybersecurity of the nation remains a high-risk issue for the United States. In part, Trusted Internet Connection (TIC) 3.0 is a major driver of this effort. Based on frameworks and input from the Office of Management and Budget (OMB), DHS's Cybersecurity and Infrastructure Security Agency (CISA), and General Services Administration (GSA), TIC 3.0 broadens the concepts of the TIC program to "accommodate cloud, mobile, and encrypted applications, services and environments. The program envisions a flexible perimeter that may protect diverse hosting environments, platforms, and services in contrast to the hard enterprise perimeter as previously implemented."

Supporting these efforts is the federal 2021 budget, which sets priorities for the year. It includes approximately $18.8 billion for cybersecurity efforts within government – with TIC and Federal Information Security Management Act (FISMA) compliance among them.

Further, the federal approach to cybersecurity will continue to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, with CFO Act agencies focusing the bulk of their spending on protection, identification, and response.

With draft TIC 3.0 guidance released in December 2019 and interim guidance released in February 2020, agencies are anticipating final drafts from CISA to publish summer 2020. Government leaders will have to understand the scope of these cyber program requirements as they make long-term plans, while simultaneously anticipating new policies to emerge – especially in the midst of rapid telework expansion. As CISA notes, unique challenges during this time include a greater chance of disruption, more endpoint devices connecting to the network, greater reliance on authentication mechanisms, and potential that more cybercriminals will look to exploit network vulnerabilities.

Agencies must ensure now they have the right security fundamentals – capabilities that are built-in and automated, and architectures that support a multi-boundary approach – while confirming that their response and recovery mechanisms are robust and ready for any disaster that comes their way.

Key considerations for TIC 3.0 implementation

Draft TIC 3.0 guidance is comprehensive and includes five volumes for agencies, including Reference Architecture, Security Capabilities, and Use Cases, to determine how to protect their environments to conform with their risk management strategy.

Notably, the Reference Architecture guide establishes the concept of trust zones, a discrete computing environment involved in information processing, storage, and/or transmission. This further supports TIC 3.0's goal of emphasizing a flexible perimeter and multiple levels of boundaries across distributed networks such as branch offices, remote users, and service providers. And, it will become ever more important as agencies maintain telework policies for their workforces.

Agencies can designate their own trust levels based on the control, transparency, sensitivity, and verification of the data. Zones should be tailored to each agency's environment and needs; however, CISA illustrates three trust zones (High, Medium, and Low) as an example. Policy enforcement remains up to each agency's discretion, allowing for flexibility for cloud adoption and other modernization initiatives.

- High trust: An agency has significant visibility into the environment – e.g., housed within an agency's on-premises network
- Medium trust: An agency has partial visibility into the environment – e.g., housed within an agency instance or cloud and mobile environment
- Low trust: An agency has limited visibility into the environment – e.g., fully maintained and managed by another entity Lumen was the first Managed Trusted
- Internet Protocol Services (MTIPS) provider to complete the TIC capability validation.

The new guidance on trust zones represents federal IT's shift toward zero-trust networking (ZTN), in line with industry best practices and as an acknowledgment that the enterprise perimeter is multi-boundary. It also aligns with NIST zero-trust architecture (ZTA) capabilities (encrypted traffic, default/deny, virtualization security, network and asset inventory) and supports the formalization of NIST ZTA as a complete enterprise solution. Moreover, CISA notes that it is developing a use case specifically on remote users, and is considering a use case for ZTA. The agency is coordinating with OBM, NIST, agencies, and vendors on ZTA and additional use cases ranging from the Internet of Things, partner networks, GSA Enterprise Infrastructure Solutions (EIS) Managed Security Service, and unified communications.

In light of these likely developments, agencies will seek to evolve to modern network architectures that support ZTA and continuous telework. Final guidance is forthcoming but CIOs will be set up for success if they modernize now and evolve their capabilities to stay ahead of emerging criteria via TIC 3.0 and other frameworks from OMB, CISA, and GSA. The TIC 3.0 Security Capabilities guidance outlines:

- Enterprise-level capabilities that outline guiding principles for TIC Use Cases ("Universal Security Capabilities")
- Network-level capabilities that inform technical implementation for relevant use cases ("Policy Enforcement Point Security Capabilities")

Uptake is at agencies' discretion. Decision-making criteria include technology maturity, sensor positioning (whether the capability is positioned to effectively measure performance and security), Policy Enforcement Point deployment, scope, and use case applicability. Agencies can then apply the various capabilities to protect dispersed assets and limit the potential impact of a cybersecurity event.

Regardless of an agency's current security posture and readiness for TIC 3.0, their network will serve as the foundation for their ability to modernize while managing risk. And yet, critical agencies may be underprepared; a 2019 GAO report found hundreds of security gaps and system architecture weaknesses at agencies possessing IT assets of high value.

Propelling federal cybersecurity forward

What's needed to fill these gaps and guide organizations on adapting TIC 3.0 to their own needs is cybersecurity capabilities that are built-in and network-based. As evidenced by OMB, CISA, GSA, and the White House's priorities, security cannot be an afterthought.

In enforcing TIC 3.0's trust zones, NIST's zero-trust architecture can provide the foundation. The emphasis of the model is on authentication, authorization, and shrinking implicit trust zones while minimizing temporal delays in authentication mechanisms. Importantly, the approach is tailored. The Department of Justice serves as one example.

The department established the goal to focus on ZTN and identity and access management pilots in fiscal year 2020 to minimize data breaches and adapt to cloud-hosted assets, and is now doubling down on authentication and virtual private network bandwidth amid the need to enable remote work for employees' health and safety.

As shown, the network includes connectivity, cloud, and security solutions and is the foundation of digital transformation. Therefore, it is essential for agencies to start their digital transformation not with advanced applications and capabilities, but with foresight into securing the network that will enable them.

Lumen provides the modern network foundation for TIC 3.0

Modernization requires agencies to think comprehensively about security and resilience. They must securely connect a massive dispersed workforce, proactively monitor, and effectively defend against evolving security threats – while also protecting mission-critical systems.

A trusted partner understands these needs and has the ability to augment an agency's risk management program and existing staff. It can help CIOs navigate competing priorities between security and operations, and help CISOs establish consistent policies and procedures on standardized technology. Moreover, it can provide agencies with the power that comes from accessing enterprise-grade risk data.

Lumen is one of the largest and most deeply peered internet protocol (IP) backbones in the world, giving us expansive, near-real-time visibility to reduce the overhead of threat identification and eradication. Given the global nature of the Lumen backbone and deep network peering, our visibility provides increased opportunities to observe advanced threats, resulting in shortened response times and advanced analysis surrounding reportable events.

The technologies Lumen uses to protect ourselves also protect our customers. By modeling threat behaviors, understanding motivations, using attacker techniques as a kernel for research and analysis, and ultimately implementing disruption efforts, we built one of the world's most advanced threat research teams – Black Lotus Labs (BLL). Through our continued investment in our BLL division, Lumen harnesses the power of our global visibility to disrupt malicious actors.

Our view of security services for the federal government, and specifically our approach to TIC 3.0, is consistent in that we prioritize 1) Security-at-scale and 2) Security "baked in" instead of "bolted-on." We firmly believe that Departments and Agencies (D/As) need to have visibility and the ability to act to orchestrate protections across multiple use cases. Lumen's TIC 3.0 solution will not provide siloed support for a single use case. It will be a comprehensive, compliant and defined EIS and WAN complementary solution for all use cases based on Internet connectivity. A user must be able to figuratively travel between "use cases" by literally moving between a remote/home-based site and a branch office – all while using multiple applications, some of which are housed in the cloud and some of which are in a dedicated data center. This interaction must be seamless.

Lumen also provides managed services and consulting expertise to tailor access policies to agencies' missions and structure – meaning that IT leaders have a trusted partner every step of the way and as guidance evolves. Our heritage of supplying security services to the government speaks for itself.

- Lumen was the first Managed Trusted Internet Protocol Services (MTIPS) provider to complete the TIC capability validation. Engineered for scalability and growth, our MTIPS infrastructure allows agencies to physically and logically connect to the public Internet in full compliance with TIC.
- Lumen is a premier provider of EINSTEIN 3 Accelerated (E3A) services and E3ASE; continually adding capabilities and providing recognized operational support for this mandated program.
- The Department of the Interior is partnering with Lumen to modernize the core of its network. Together, they are implementing MTIPS and ZTN solutions that meet strict government security requirements.

Finally, Lumen understands that cybersecurity, cloud services, and TIC 3.0 must work hand in hand to support long-term government transformation. We engage in public-private partnerships – including with DHS' National Risk Management Center, National Cybersecurity and Communications Integration Center, and National Coordinating Center – to protect the resiliency of the federal cyber ecosystem. Lumen's decades of experience with government customers and breadth in providing cybersecurity services that are backed by DHS provide public sector leaders the assurance that their networks remain protected and adaptable for the future.

Let Lumen help you modernize with built-in security.

Lumen is invested in collaborating with federal agencies to solve their IT challenges and meet their missions. With our comprehensive approach to network-based cybersecurity, we provide the right solutions, right now – propelling agencies into the future of federal IT.

Disclaimer

This document is provided for informational purposes only and may require additional research and substantiation by the end user. In addition, the information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. Lumen does not warrant that the information will meet the end user's requirements or that the implementation or usage of this information will result in the desired outcome of the end user. This document represents Lumen's products and offerings as of the date of issue.

lumen.com/public-sector

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.

LUMEN®