Forcepoint

Issue Brief

# TIC 3.0

## Expanding the boundary without sacrificing security

The Trusted Internet Connection (TIC) initiative set out to greatly reduce the number of endpoints across Federal agencies – aiming to establish a secure perimeter to protect the nation's vital data. Since the early days of TIC, the Federal government has transformed how its employees work and how it meets its mission, largely propelled by far-reaching IT modernization initiatives, including Federal Risk and Authorization Management Program (FedRAMP), Federal Information Technology Acquisition Reform Act (FITARA), and the Modernizing Government Technology (MGT) Act. With transformation top of mind for agencies, TIC was due for an update.

Office of Management and Budget (OMB) Memorandum M-19-26[1] introduces the latest iteration, TIC 3.0, and updates expectations of the programs including a foundation for TIC to evolve as agencies continue to modernize and adopt new technologies. TIC 3.0 provides guidance for agencies via four use cases: traditional TIC, cloud, agency branch office, and remote users.

Previous TIC requirements have notoriously caused latency issues that occur when agencies attempt to access government data that is hosted off-premises or in the public cloud and mandated traffic run through that particular Enterprise Infrastructure Services (EIS) Managed Trusted Internet Protocol Service (MTIPS). As agencies move to the public cloud or rapidly adopt teleworking, TIC requirements for routing through a MTIPS provider resulted in inefficiencies, expensive private network bandwidth, latency, degraded end user experience, and lost productivity. With the new TIC 3.0 guidance, agencies can access cloud directly and securely.

TIC 3.0 Volume 2 Reference Architecture[2] notes strategic program goals to support the changing nature of Federal work and IT systems, including but not limited to:

- → **Boundary-Focused** – To support the increased use of cloud and mobile environments across agencies, TIC 3.0 adopts a flexible framework to address expanded network boundaries while prioritizing security. This includes dividing agency architectures by Trust Zones, looking beyond a traditional, singular physical network perimeter to establish zones within an agency environment, and corresponding security protections for each zone.
- → **Descriptive, Not Prescriptive** – Previous iterations of TIC focused solely on securing the physical agency network perimeter by limiting access points. This is no longer practical given the current state of Federal IT as a result of modernization efforts and broad cloud adoption. The updated reference architecture and use cases provide support for agencies and will continue to do so as IT evolves even further.
- → **Risk-Based to Accommodate Varying Risk Tolerance** – Not all Federal agencies have the same risk tolerance or security needs. Under TIC 3.0, agencies can assess their individual risk needs and look beyond the controls identified in TIC 3.0 as necessary.
- → **Environment-Agnostic** – As all agencies have varying level of risk tolerance and security needs, they all operate with unique missions, business needs, and resource availability. Therefore, TIC 3.0 supports vendor and technology-neutral terms, components, and definitions.
- → **Dynamic and Readily Adaptable** – The TIC PMO will provide continuous updates to use cases, core guidance, reference architectures, and capabilities to support the rapidly changing Federal IT environment.
- → **Automated and Streamlined Verification** – Previous TIC-related FISMA metrics and manual TIC Compliance Validation (TCV) has been replaced by automated metric collection with primary focus on security and availability

1 https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf
2 https://www.cisa.gov/sites/default/files/publications/Draft%20TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf

measures, leveraged by existing capabilities under the Continuous Diagnostics and Mitigation (CDM) program. The end goal is to track real-time, ongoing implementation of TIC capabilities across agencies.

A key strategic goal of TIC 3.0 is that agencies establish Trust Zones using designations like high, medium, and low to set security rules based on the sensitivity of data stored or processed. Trust Zones inherently go hand-in-hand with a Zero Trust architecture. Within a Zero Trust architecture, protecting data is a key component, and tracking who uses what data and how is essential. The previous perimeter approach allowed access based on implicit assumptions of trust. The Zero Trust architecture limits access only to what's necessary with a 'never trust, always verify' mindset. If a breach happens, the size and scope will be far less reaching with this approach. Data discovery and classification, data detection, deep forensics, analytics, and software-as-a-service (SaaS) application protection are integral components of Zero Trust. Agencies moving toward Zero Trust will be most successful using integrated security solutions that can adapt dynamically to risk and provide real-time reporting to generate actionable insights.

As Federal IT modernization efforts continue to progress, edge protection is also becoming increasingly important. Therefore, a key strategic goal of TIC 3.0 is to provide a flexible framework. No longer are Federal employees, applications, data, and systems located behind security gateways within the physical perimeter of an agency headquarters. Today's perimeter is much larger and more mobile. Protecting the edge means following employees, applications, data, and systems to the cloud – this is where a secure access service edge (SASE) comes in.

**In Gartner's "The Future of Network Security is in the Cloud[3]" analysts predict that "By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% in late 2018."**

As a result of the current extended telework posture, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released interim TIC guidance to help agencies leverage existing resources to secure their networks[4]. With the interim guidance, agencies can continue to connect to private agency networks and cloud environments in a secure manner, ensuring mission continuity.

Federal agencies are always at risk of data breaches and security incidents, but this is magnified in the current extended telework posture. As users and data are moving between on-premise and cloud, maintaining effective data protection is crucial. Threat actors continue to evolve to identify any available point of entry to breach.

Forcepoint can help agencies meet the new standards required by TIC 3.0 – Forcepoint's products are purposely designed to support ongoing IT modernization. Forcepoint seeks to transform cybersecurity by focusing on what matters most – people's behavior as they interact with critical data and systems. This human-centric approach to cybersecurity frees employees to innovate by understanding the normal rhythm of user behavior and the flow of data in and out of an agency network. Forcepoint behavior-based solutions adapt to risk in real time and are delivered via a converged security platform to protect network users and cloud access, prevent confidential data from leaving the corporate network, and eliminate breaches caused by insiders.

3 https://security.umbrella.com/gartner-future-of-network-security-report-gated
4 https://www.cisa.gov/sites/default/files/publications/CISA-TIC-TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf

A recent real-world example shines a light on remote work challenges considering current events. A Forcepoint customer supporting multiple government agencies with sensitive mission requirements needed to rapidly transition to a remote work environment.

Some of the challenges the customer was facing included:

- → Complex VPN management
- → A lack of or inefficient one-to-many device provisioning
- → New time-consuming firewall deployments
- → Maintaining policy consistency across firewalls
- → Deploying software updates at a large scale
- → Having a unified view of all firewalls and VPN tunnels

Forcepoint helped this customer leverage small office and remote office appliances to connect 400 remote workers to critical business applications and functions, at a low cost, and while enforcing enterprise security. The solutions helped combat the overload and strain on the network caused by increased usage of VPN connectivity caused by the expanded remote workforce. The customer deployed a small desktop firewall that was configured with policy-based and rule-based protocols and distributed these to remote employees for a full VPN mesh architecture. Benefits as a result included: fewer planned maintenance occurrences, fewer unplanned outages, fewer cyberattacks and breaches, faster deployment times, overall lower total cost of ownership, end-user internet performance improvement, and a reduction from days to hours in planned maintenance, unplanned outages, and incident response time.

Forcepoint has been a leader in the Federal market for many years and provides agencies the end-to-end, human-centric security architecture required to meet their unique security challenges and mission goals, with a full and integrated portfolio to aid agencies in modernizing their networks as they evolve to new TIC 3.0 use cases, including:

- → **Dynamically connect direct-to-cloud and site-to-site**

  As agencies modernize their networks to support cloud initiatives and meet TIC 3.0 guidance, Forcepoint can help eliminate single points of failure, reduce networking costs, increase capacity, security, and improve quality of service. Forcepoint uniquely combines enterprise software-defined wide-area network (SD-WAN) connectivity with the most secure and efficient next generation firewall (NGFW) available and is centrally managed, even at cloud scale. This helps agencies connect and protect users and Federal data throughout data centers, edge, branches, and the cloud – all with the industry's #1 security, manageability, and availability. With Forcepoint's renowned Sidewinder proxy technology at its core, it offers high availability and centralized management which combines NSS Labs' top-rated security for mission-critical networks and applications. Forcepoint SD-WAN, firewall, and intrusion prevention solutions work seamlessly with cloud-based web security and cloud access security broker (CASB) services to provide unrivaled protection for users and data as they move about the internet.

- → **Implementing Trust Zones**

  As agencies look to implement Trust Zones or Zero Trust, additional controls are necessary to manage residual risk. Forcepoint can help with full and integrated security solutions that can adapt dynamically to risk and provide real-time reporting that generates actionable insights. Forcepoint Edge Protection solutions enable cost-effective network protection against advanced threats, while securing remote users with Zero Trust direct-to-cloud connectivity. Unlike point product vendors, Forcepoint's full and integrated security portfolio helps agencies implement a practical approach to Zero Trust.

→ **Evolving to risk-based architectures**

Forcepoint's risk-adaptive protection solutions enable agencies to support their risk tolerance goals by continuously assessing risk and automatically providing proportional enforcement that can be dialed up or down. This solution integrates Forcepoint Behavior Analytics, Data Loss Prevention (DLP), and Insider Threat products and helps to provide agencies with options for both monitoring and enforcement. Intelligent analytics combined with individualized policy enforcement helps support the CDM and TIC 3.0 missions. These risk-adaptive capabilities, together with Forcepoint NGFW, CASB Email Security, and Web Security solutions, are included on the CDM Approved Product List to protect sensitive networks and data – wherever they are accessed and wherever they reside. Only Forcepoint can provide agencies the end-to-end, human-centric security architecture required to address their unique risk tolerance while enabling mission goals.

Forcepoint's solutions are cloud first, hybrid-ready and provide unified cloud and network security for real-world architectures: cloud, on-premise, and everything in between to address and help to support TIC 3.0 advanced security measures across branch offices, remote users, cloud and other service providers, mobile devices, and more. Download the latest TIC 3.0 white paper to learn more about TIC 3.0 use cases Forcepoint can help support.

Forcepoint

**forcepoint.com/contact**

## About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.