SmartSuite

Framework / Cybersecurity / Other

Trusted Internet Connections (TIC) 3.0

TIC 3.0 is the federal civilian network security initiative set by OMB M-19-26 (2019) and documented by CISA: trust zones, policy enforcement points, security capabilities and use cases.



What it is

Trusted Internet Connections (TIC) 3.0 is the network security initiative for U.S. federal civilian agencies that OMB Memorandum M-19-26 (September 12, 2019) directed and that the Cybersecurity and Infrastructure Security Agency (CISA) documents in the TIC 3.0 Core Guidance. M-19-26 rescinded M-08-05 (November 20, 2007), M-08-16, M-08-27 and M-09-32, the memoranda that had required agency traffic to flow through a physical TIC access point, and gave agencies one year to update their network and system boundary policies and to identify which TIC use cases they allow (section E).

At a glance

PUBLISHER
Cybersecurity and Infrastructure Security Agency (CISA), under OMB Memorandum M-19-26

TYPE
Architecture / Technical Model

VERSION
TIC 3.0 Core Guidance (Program Guidebook v1.2, July 2025; Security Capabilities Catalog v3.2, December 2024; Cloud Use Case v1.0, April 2023)

EFFECTIVE
September 12, 2019 (OMB M-19-26); core guidance v1.0 July 2020

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: cisa.gov/resources-tools/programs/trusted-internet-connections-tic

Why it matters

- **Cloud and remote access without a backhaul** M-19-26 section C lets traffic bypass a TICAP or MTIPS access point when the alternative controls in a TIC use case are in place, which removed the policy barrier to IaaS, SaaS, PaaS and remote-user architectures.
- **One vocabulary for architectures** Trust zones, policy enforcement points, security patterns, use cases and overlays (Guidebook section 6.1) give agencies, CISA and vendors a common way to describe and compare a network design.
- **Rigor set by risk, not by a fixed list** The catalog dropped the Critical/Recommended prioritization of TIC 2.x; agencies decide the level of each capability per trust zone and document the residual risk they accept (Guidebook sections 4 and 6.1).
- **A catalog already mapped to NIST** Every capability in the Security Capabilities Catalog carries NIST Cybersecurity Framework category mappings, updated to CSF 2.0 in version 3.2, so TIC evidence reuses the agency's CSF and SP 800-53 work.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports TIC 3.0

Security Capabilities Catalog Library

Load the universal (3.UNI) and PEP (3.PEP) capabilities with their NIST CSF 2.0 mappings, the use cases they apply to, an owner and an implementation status.

Trust Zone and PEP Register

Record each trust zone with its designated trust level, the policy enforcement points that serve it and the security patterns between zones, linked to the capabilities applied at each PEP.

Use Case Adoption and Compensating Controls

Track which of the Traditional TIC, Branch Office, Remote User and Cloud use cases the agency allows under M-19-26 section E, the boundary policy update and the compensating controls for residual risk.

Network Connection Inventory

Keep the M-19-26 section E inventory of connections with service provider, cost, capacity, traffic volume, logical and physical configuration and topology in IT Asset Management (ITAM).

Vendor Overlays and FedRAMP Status

Hold each provider's TIC overlay mapping and FedRAMP authorization status in Third Party Risk Management, with the capability gaps the overlay reveals (Guidebook sections 7 and 9).

Telemetry and FISMA Reporting

Evidence that telemetry reaches CISA for each use case (Guidebook section 10), CISA Services coverage and the TIC posture reported through FISMA, assembled from the same records.

Common framework mappings

CIS Controls v8.1 | FedRAMP Rev. 5 | FIPS 140-3 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2 | GovRAMP

Official resources

TIC 3.0 Core Guidance Documents (CISA)

CISA's page listing the core guidance volumes and the use cases with their PDF links.

cisa.gov/resources-tools/resources/trusted-internet-connections-tic-30-core-guidance-documents

TIC 3.0 Security Capabilities Catalog v3.2 (CISA, December 2024)

CISA's announcement of version 3.2 of the catalog of security capabilities, updated for the NIST CSF 2.0 mappings.

cisa.gov/news-events/news/updated-tic-30-security-capabilities-catalog-scc-v32

TIC 3.0 Program Guidebook, Version 1.2 (July 2025)

Volume 1 of the TIC 3.0 core guidance: program structure, roles and the July 2025 revision history.

cisa.gov/sites/default/files/2025-07/CISA%20TIC%203.0%20Program%20Guidebook.pdf

Frequently asked questions

What did OMB M-19-26 change about the TIC initiative?

M-19-26 (September 12, 2019) rescinded M-08-05, M-08-16, M-08-27 and M-09-32, which had required agency traffic to flow through a physical TIC access point (section B). It made DHS, through CISA, define TIC requirements in use cases whose alternative controls let traffic bypass a TICAP or MTIPS (section C), set up a pilot and approval process with OMB, GSA and the Federal CISO Council (section D), and gave agencies one year to update their boundary policies and name the use cases they allow, tracked through FISMA reporting (section E).

What are the five TIC 3.0 security objectives?

Section 5 of the Program Guidebook and section 3 of the Security Capabilities Catalog list them: Manage Traffic; Protect Traffic Confidentiality; Protect Traffic Integrity; Ensure Service Resiliency; and Ensure Effective Response. Traffic means data in transit between trust zones or stored at either. Each objective stands alone, agencies apply them at a level commensurate with the resources protected, and the guidebook maps them to the six NIST CSF 2.0 Functions.

Updated Oct 15, 2026 - © 2026 SmartSuite Inc. All rights reserved.

What are trust zones and policy enforcement points in TIC 3.0?

A trust zone is a discrete computing environment designated for information processing, storage or transmission whose trust level the agency sets; a policy enforcement point (PEP) is a security device, tool, function or application that enforces security policies (Guidebook Appendix C). TIC 3.0 disperses security capabilities across multiple PEPs close to the data instead of concentrating them at a TIC access point, and a security pattern describes the end-to-end data flow between two zones (section 6).

Which TIC 3.0 use cases exist, and must an agency use them?

CISA has published the Traditional TIC, Branch Office, Remote User and Cloud use cases; the Cloud use case (April 2023) completed the initial set that M-19-26 Appendix A listed. Traditional TIC remains the default for scenarios no other use case covers. Agencies choose and may combine use cases to suit their risk tolerance, and where a use case does not address residual risk they must apply compensating controls, with their senior officials accountable for risk management (CISA program page; Guidebook section 9).

What is in the Security Capabilities Catalog, and which version is current?

Volume 3 indexes universal security capabilities, which are enterprise-level and expected in every use case, and PEP security capabilities grouped into Files, Email, Web, Networking, Resiliency, DNS, Intrusion Detection, Enterprise, Unified Communications and Collaboration, Data Protection, Services and Identity (sections 4.1 and 4.2), each mapped to NIST CSF categories. Version 3.0 (April 2023) added five universal capabilities and the Services and Identity groups; version 3.2 (December 2024) updated the mappings to CSF 2.0 and is the current edition.

License included / downloadable: Yes The TIC 3.0 core guidance, use cases and catalog are published free by CISA as TLP:CLEAR documents on cisa.gov, and OMB M-19-26 is a public memorandum on whitehouse.gov; the platform links to the official texts.

Full framework page and mappings: smartsuite.com/frameworks/us-cisa-trusted-internet-connections-tic-3-0-federal-network-security