

Trusted Internet Connections (TIC) 3.0

TIC 3.0 provides federal guidance to secure and monitor agency network connections across cloud and on-premises environments.



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

What it is

At a glance

PUBLISHER

Cybersecurity and Infrastructure Security Agency (CISA)

TYPE

Architecture / Technical Model

VERSION

3.0

EFFECTIVE

July 31, 2020

DOMAIN

Cybersecurity

FAMILY

NIST Special Publications

REGION

United States

INDUSTRY

Government & Public Sector

ADOPTION MODEL

Regulatory Compliance

IMPLEMENTATION COMPLEXITY

High

Source: <https://www.cisa.gov/trusted-internet-connections>

Why it matters

- **Enable dynamic security oversight** Provide agencies with flexible, risk-based monitoring and enforcement for a variety of cloud, on-premises, and hybrid environments.
- **Strengthen compliance support** Facilitate alignment with federal mandates and OMB policies, helping organizations demonstrate adherence to security and privacy requirements.
- **Enhance operational resilience** Improve network segmentation and traffic visibility, reducing the risk of widespread disruption from cyber incidents or infrastructure outages.
- **Improve incident detection and response** Increase the ability to rapidly identify, contain, and remediate security events across distributed and diverse network perimeters.

How SmartSuite supports TIC 3.0

TIC Capability Library

Structure TIC 3.0 security capabilities and use cases with mapped controls and responsible owners.

Network Architecture and Trust Zone Governance

Document network boundaries, trust zones, and security architecture aligned with TIC guidance.

Traffic Monitoring and Security Visibility

Track monitoring controls, telemetry collection, and inspection capabilities across network environments.

Security Policy and Access Control Management

Manage policies governing network access, routing, and traffic filtering requirements.

Vendor and Network Service Oversight

Track telecommunications providers and managed services supporting federal network infrastructure.

TIC Security Posture and Federal Review Readiness Reporting

Provide dashboards summarizing TIC capability implementation, security posture, and readiness for federal security reviews.

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

Official resources

CISA Trusted Internet Connections (TIC) 3.0 Core Guidance

Provides the primary framework documentation for secure federal network architecture.

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

CISA TIC 3.0 Security Capabilities Catalog

Describes the security capabilities required under the TIC 3.0 framework.

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

CISA TIC 3.0 Program Guidebook

Outlines implementation guidance and best practices for TIC 3.0 adoption.

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

Frequently asked questions

What is TIC 3.0 used for?

TIC 3.0 is designed to enhance the security of federal network architectures by providing guidance on securing external network connections, including cloud, remote, and hybrid environments. The program aims to modernize and adapt federal cybersecurity postures to evolving threats and technologies while maintaining effective risk management principles.

Is TIC 3.0 required for U.S. federal agencies?

Yes, TIC 3.0 is a mandatory federal guideline for executive branch civilian agencies as directed by the Office of Management and Budget (OMB). Agencies must follow TIC 3.0 requirements as part of their broader Federal Information Security Modernization Act (FISMA) obligations.

What is the scope of the TIC 3.0 program?

TIC 3.0 applies to all federal agency network architectures managing or transmitting federal information, whether hosted on-premises, in the cloud, or via third parties. It covers agency-managed connections, service provider-managed environments, and any use case involving sensitive government data transfer.

What key concepts or artifacts are required by TIC 3.0?

TIC 3.0 mandates the development of security capabilities, architectural diagrams, and documentation of trust zones and trust boundaries. Agencies must create TIC use case documents, security capability matrices, and implementation summaries to demonstrate compliance.

How does implementation of TIC 3.0 work for agencies?

Agencies implement TIC 3.0 by assessing their network environments, identifying applicable TIC use cases, and mapping required security capabilities to their technical and business needs. Agencies are encouraged to tailor security controls based on risk assessments while adhering to CISA guidance and OMB mandates.

How does TIC 3.0 relate to other federal cybersecurity frameworks?

TIC 3.0 aligns with frameworks such as NIST SP 800-53 and FISMA requirements, and it complements federal initiatives like Zero Trust Architecture (ZTA). TIC 3.0 provides architectural context for deploying control baselines and integrating with broader federal cybersecurity policies.

What are the ongoing compliance requirements for TIC 3.0?

Ongoing compliance with TIC 3.0 involves continuous risk assessment, updating architectural documentation, monitoring security capabilities, and periodic reporting to CISA. Agencies must demonstrate active risk management, keep use case documentation current, and participate in regular audits or assessments.

How would SmartSuite support TIC 3.0?

SmartSuite would help organizations manage TIC 3.0 compliance by enabling centralized tracking of TIC use cases, risk registers, and security controls. It supports evidence collection for audits, facilitates control mapping and implementation management, and provides reporting tools for audit readiness and ongoing compliance oversight.

License included / downloadable: Yes TIC 3.0 is published by CISA and is publicly available on CISA's website. License included with platform

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