FEDERAL ARCHITECTURE ALIGNMENT GUIDE

Total Access Control (TAC) and CISA TIC 3.0

How TAC delivers Policy Enforcement Point security capabilities for the Trusted Internet Connections 3.0 trust-zone model — particularly the Remote User and Branch Office use cases that define modern federal access.

Audience	Framework	Version
Federal agency CISOs, network architects, TIC / zero trust program leads	CISA Trusted Internet Connections (TIC) 3.0	v1.0 — 2026

TAC Scope in TIC 3.0. TIC 3.0 is a federal architecture program overseen by CISA, OMB, and GSA. It is descriptive, not prescriptive — agencies have significant discretion in how they meet each security capability. TAC delivers the **Policy Enforcement Point (PEP) capabilities for the access path**: authentication, authorization, encryption, zone-boundary enforcement, and access logging — the strongest fit being the Remote User and Branch Office use cases.

TIC 3.0 also spans PEP capabilities TAC does **not** provide — email protection, DNS filtering, web content inspection, intrusion detection and prevention, and data loss prevention. CISA telemetry-sharing obligations remain an agency responsibility; TAC produces the access telemetry that supports them but does not transmit to CISA on the agency's behalf.

Overview

The most fundamental change in TIC 3.0 is the shift away from a single physical network perimeter toward trust zones — logical boundaries defined around applications, services, and environments rather than the agency's physical network edge. As agencies adopt cloud and support remote users, traffic no longer flows through one consolidated access point, so security must be enforced at the boundary of each zone.

TIC 3.0 organizes this through a Security Capabilities Catalog — Universal capabilities that apply across the enterprise, and Policy Enforcement Point (PEP) capabilities that secure traffic between zones — applied within use cases such as Traditional, Branch Office, Remote User, and Cloud. TAC is purpose-built to be a Policy Enforcement Point at the boundary of a trust zone: its reverse proxy authenticates, evaluates, and authorizes every request crossing into a protected zone on a single encrypted port, regardless of where the user or application sits.

ACCESS CONTROL & IDENTITY PEP — PRIMARY COVERAGE

Authentication & Authorization

TIC 3.0 SECURITY CAPABILITY	HOW TAC DELIVERS
Authentication	Every user and entity is authenticated before crossing into a protected zone. TAC federates with Active Directory, LDAP, SAML, OIDC, RADIUS, and SQL identity sources, and enforces MFA — FIDO2, hardware tokens, push, OTP, SMS, and more — on every session.
Authorization & access control	Per-user, per-application, per-protocol authorization is enforced at the proxy on every request. Access decisions reflect identity, device posture, and policy — not network location.
Least privilege / segmentation	Each protected application is its own trust zone, reachable only by authorized identities meeting policy. There is no flat network behind TAC for an attacker to traverse.
Hardened access path	TAC exposes a single encrypted inbound port (TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules). All other inbound ports to the protected zone are closed.

CONNECTION & DATA PROTECTION PEP — PRIMARY COVERAGE

Encryption & Boundary Enforcement

TIC 3.0 SECURITY CAPABILITY	HOW TAC DELIVERS
Encryption in transit	All traffic crossing the zone boundary through TAC is encrypted end-to-end, protecting data in transit between the user and the protected application.
Zone boundary enforcement	TAC is the enforcement point at the boundary of each trust zone. Every request is inspected, authenticated, and authorized before it reaches anything inside the zone; unauthorized traffic is dropped at the proxy.
Application-layer enforcement	As a reverse proxy, TAC enforces policy at the application layer — including for legacy, thick-client, RDP, SSH, and forms-based applications — without modifying those applications.

LOGGING & TELEMETRY — PRIMARY COVERAGE

Audit & Visibility

TIC 3.0 SECURITY CAPABILITY	HOW TAC DELIVERS
Logging & auditing	Every authentication, authorization decision, session, and policy event at the zone boundary is logged with full attribution — a high-fidelity record of all access crossing into protected zones.
Telemetry for CISA reporting	TAC logs export to SIEM, where agencies aggregate the telemetry TIC 3.0 expects them to share with CISA. TAC produces the access telemetry; the agency's reporting pipeline transmits it.

Strongest Fit: Remote User & Branch Office Use Cases

Remote User Use Case. TAC authenticates remote users, evaluates device posture, and brokers access to agency applications on a single encrypted port — no VPN, no open inbound ports, no agent required. Remote users reach only the applications they are authorized for, with policy enforced on every request, exactly as this use case envisions.

Branch Office Use Case. For remote offices accessing agency resources, TAC enforces the trust-zone boundary without backhauling traffic through a central access point. Each branch reaches protected applications through the same identity-, posture-, and policy-based enforcement, regardless of where those applications are hosted.

> **Out of Scope — PEP capabilities TAC does not provide.** TIC 3.0's Security Capabilities Catalog spans Policy Enforcement Point areas beyond access control — including email protection (anti-phishing, anti-spam), DNS filtering, web content inspection and filtering, intrusion detection and prevention, and data loss prevention. TAC does not provide these. It secures the access path into trust zones and produces access telemetry; agencies combine TAC with email, DNS, content-inspection, and IDS/IPS tooling to address the full catalog. Universal capabilities such as the agency's overarching security policy, incident response program, and contingency planning are organizational responsibilities outside any access control platform.

A Natural Fit for Federal Cloud Migration and Zero Trust

TIC 3.0 was designed to help agencies securely adopt cloud and support remote work — and to establish a foundation for zero trust. TAC advances all three at once. Because TAC abstracts application location, an agency can migrate a workload from a data center to the cloud without changing access policy or disrupting users: the trust-zone boundary moves with the application, and the user experience is unchanged.

The same enforcement that satisfies TIC 3.0 PEP capabilities also advances the agency's zero trust posture under OMB M-22-09 and NIST SP 800-207. The access decisions, authentication records, and audit telemetry are shared evidence across all three.

PEP Capability Coverage Summary

PEP / CAPABILITY AREA	WHAT TAC ADDRESSES	TAC COVERAGE
Access & Identity PEP	Authentication, MFA, authorization, least-privilege segmentation, single-port hardening	Primary
Connection & Data PEP	Encryption in transit, zone-boundary enforcement, application-layer policy	Primary
Logging & Telemetry	Full access logging + SIEM export for agency CISA reporting	Primary
Email / DNS / Content / IDS	Not provided — addressed by complementary tooling	Out of scope
Universal program capabilities	Agency security policy, incident response, contingency planning	Out of scope

Next Steps

Map your trust-zone architecture against the TIC 3.0 Security Capabilities Catalog. Identify where TAC delivers the access-path PEP capabilities for your Remote User and Branch Office use cases. **Request a TIC 3.0 walkthrough** at portsys.com/contact or info@portsys.com — a PortSys specialist will work through your environment and produce a prioritised plan.