ZERO TRUST ALIGNMENT GUIDE

Total Access Control (TAC) and the NSA Zero Trust Security Model

How TAC advances Zero Trust maturity across the access-centric pillars of the NSA's Zero Trust Security Model — User, Device, Application & Workload, and Network & Environment — under the principle of "never trust, always verify."

Audience	Framework	Version
Federal CISOs, NSS / DoD / DIB security teams, zero trust program leads	NSA Zero Trust Security Model (7 pillars)	v1.0 — 2026

TAC Scope in the NSA Zero Trust Model. The NSA Zero Trust Security Model is maturity guidance — a series of Cybersecurity Information Sheets describing how to advance capability across seven pillars over time — not a certification or pass/fail standard. TAC delivers **primary coverage** in the four access-centric pillars: User, Device, Application & Workload, and Network & Environment.

TAC plays a **supporting** role in the Data, Visibility & Analytics, and Automation & Orchestration pillars: it controls access to data-bearing systems, generates access telemetry, and exposes a policy engine and API — but it does **not** classify or encrypt data at rest, perform analytics-driven threat detection, or act as a SOAR platform. TAC contributes to a Zero Trust architecture; it does not, by itself, constitute one.

Overview

The NSA structures its Zero Trust Security Model around seven pillars: User, Device, Application & Workload, Network & Environment, Data, Visibility & Analytics, and Automation & Orchestration. The NSA publishes detailed Cybersecurity Information Sheets for each, describing how to mature capability from a traditional perimeter posture toward a fully realized Zero Trust architecture. The guidance is intended primarily for National Security Systems (NSS), the Department of Defense (DoD), and the Defense Industrial Base (DIB), and shares its foundations with NIST SP 800-207.

No single product spans all seven pillars. TAC is an access control platform; its strength is concentrated in the four pillars where Zero Trust is fundamentally an access problem — verifying the user, evaluating the device, controlling access to each application and workload, and segmenting the network environment to curtail lateral movement. This guide maps TAC to those pillars and is explicit about where TAC only plays a supporting role.

PILLAR 1 — PRIMARY COVERAGE

User

NSA CAPABILITY	HOW TAC DELIVERS
Identity verification & authentication	Every user is authenticated before reaching any resource. TAC federates with Active Directory, LDAP, SAML, OIDC, RADIUS, SQL, and custom identity sources — including multiple directories simultaneously — without requiring migration to a new identity provider.
Multi-factor authentication	All seven MFA methods are included in the base licence: FIDO2/WebAuthn, SafeLogin, TOTP, push, SMS, OTP, and hardware tokens, plus third-party integration with Duo, RSA, Swivel, and biometric factors. MFA is enforced on every session.
Least-privilege access	Access is granted per-user, per-application, scoped to exactly what each identity is authorized to reach. Users see only the resources their current authorization permits — nothing more.
Continuous authentication	Authorization is re-evaluated throughout the session, not just at login. If identity context changes, access can be revoked mid-session. Removing a user at the identity source cuts off all access in moments.
Non-human identities	Service accounts, devices, and AI agents are governed as first-class identities under the same policy engine as human users — a requirement as automation expands inside Zero Trust environments.

PILLAR 2 — PRIMARY COVERAGE

Device

NSA CAPABILITY	HOW TAC DELIVERS
Device posture evaluation	TAC evaluates device posture at access time — certificate presence, OS version, patch level, antivirus state, firewall status, disk encryption, domain join, and geolocation — and enforces policy based on the result.
Continuous device validation	Posture is validated continuously throughout the session. If a device falls out of compliance mid-session, access is revoked immediately rather than at next login.
No agent requirement	Device posture is assessed without mandating an endpoint agent on every device, reducing deployment friction for contractors, partners, and unmanaged endpoints that must still meet posture requirements.

PILLAR 3 — PRIMARY COVERAGE

Application & Workload

NSA CAPABILITY	HOW TAC DELIVERS
Granular application access control	TAC's reverse proxy sits in front of every protected application and enforces identity-, posture-, and policy-based access on every request. No user reaches an application without passing TAC's policy decision first.
Protection from unauthorized users	Applications are never directly exposed. They sit behind TAC's single encrypted port, invisible and unreachable to unauthenticated users — the core aim of the NSA Application & Workload pillar.
Coverage for legacy & thick-client apps	TAC protects modern web apps, legacy web apps, thick-client applications, RDP, SSH, and forms-based authentication apps — with no application modification. Legacy workloads that cannot adopt modern auth are brought under Zero Trust policy.
Location-independent enforcement	Policy is enforced identically whether a workload runs on-premises, in a private cloud, or in a public cloud. Migrating a workload does not change its access policy or the user experience.

PILLAR 4 — PRIMARY COVERAGE

Network & Environment

NSA CAPABILITY	HOW TAC DELIVERS
Curtailing lateral movement	Because access to each resource is brokered individually through TAC, a compromised credential or endpoint cannot move laterally to other systems. There is no flat network to traverse — every hop requires a fresh policy decision.
Macro- and micro-segmentation	TAC enforces logical segmentation by identity and policy rather than network topology. Each application is its own segment of one, reachable only by authorized identities meeting posture requirements.
Reduced attack surface	TAC's reverse-proxy architecture requires only a single encrypted inbound port (TLS 1.2 or TLS 1.3 with FIPS 140-2 compliant cryptographic modules). Every other inbound port is closed, eliminating the unauthenticated remote-exploitation attack surface.
Encrypted access paths	All access is encrypted end-to-end through the single TAC port, protecting traffic against interception and tampering across the network environment.

Supporting Pillars — Honestly Scoped

TAC supports the remaining three pillars but does not fully deliver them. Each requires capabilities beyond an access control platform. The tables below state exactly what TAC does — and does not — contribute.

PILLAR 5 — SUPPORTING COVERAGE

Data

NSA CAPABILITY	HOW TAC DELIVERS
Access control to data-bearing systems	**Supports.** TAC controls who can reach the applications and systems that hold data, applying identity, posture, and policy to every access path. It governs the door to the data.
Data classification, tagging & labelling	**Out of scope.** TAC does not classify, tag, or label data. These are functions of data governance and DLP tooling. TAC can enforce access policy informed by classifications applied elsewhere.
Encryption of data at rest	**Out of scope.** TAC encrypts data in transit on the access path. Encryption of data at rest is a function of the storage and application layers, not the access control platform.

PILLAR 6 — SUPPORTING COVERAGE

Visibility & Analytics

NSA CAPABILITY	HOW TAC DELIVERS
Access & authentication telemetry	**Supports.** Every authentication, authorization decision, session, and policy event is logged with full attribution — a rich, high-fidelity source of access telemetry for the visibility pillar.
SIEM integration	**Supports.** TAC logs export to SIEM for centralized correlation, retention, and reporting alongside telemetry from other sources.
Analytics & AI-driven threat detection	**Out of scope.** TAC does not perform native behavioral analytics or AI-driven anomaly detection. It enforces configurable policy rules and feeds its telemetry to the analytics platforms that perform detection.

PILLAR 7 — SUPPORTING COVERAGE

Automation & Orchestration

NSA CAPABILITY	HOW TAC DELIVERS
Policy-driven automated enforcement	**Supports.** TAC's policy engine automatically enforces access decisions and can automatically revoke access when identity or posture conditions change — automation at the access decision point.

NSA CAPABILITY	HOW TAC DELIVERS
API-driven integration	**Supports.** TAC exposes an API that orchestration and automation platforms can use to integrate access control into broader security workflows.
Security orchestration (SOAR)	**Out of scope.** TAC is not a SOAR platform. It does not orchestrate cross-tool incident response playbooks. It integrates with orchestration platforms as the access-control enforcement point within them.

Built on the Same Foundation as NIST 800-207

Shared principles. The NSA Zero Trust Security Model and NIST SP 800-207 share the same core principles: never trust, always verify; assume breach; enforce least-privilege access; and make access decisions dynamically based on identity, device, and context. The NSA's pillar-based Cybersecurity Information Sheets translate those principles into specific maturity guidance — but the underlying architecture is the one NIST defines.

Direct architectural fit. TAC implements the NIST 800-207 logical model directly: a policy decision point and policy enforcement point that sit between every user and every resource, evaluating identity, device posture, and policy on every request. That architecture is exactly what the NSA's User, Device, Application & Workload, and Network & Environment pillars call for as organizations mature beyond a perimeter model.

Shared evidence. For organizations working toward both NSA Zero Trust maturity and NIST 800-207 alignment, the evidence is shared. The same access enforcement, authentication records, and audit telemetry serve both.

Pillar Coverage Summary

PILLAR	WHAT TAC ADDRESSES	TAC COVERAGE
User	Identity verification, MFA (7 methods), least privilege, continuous auth, non-human identities	Primary
Device	Posture evaluation, continuous validation, no-agent option	Primary
Application & Workload	Reverse-proxy access control, legacy/thick-client coverage, location independence	Primary
Network & Environment	Lateral-movement curtailment, segmentation, single-port attack-surface reduction	Primary
Data	Access to data-bearing systems (not classification or at-rest encryption)	Supporting
Visibility & Analytics	Access telemetry + SIEM export (not native analytics / AI detection)	Supporting
Automation & Orchestration	Policy automation + API (not SOAR orchestration)	Supporting

Next Steps

Map your current Zero Trust posture against the NSA pillars. Identify where TAC advances maturity in the User, Device, Application & Workload, and Network & Environment pillars. **Request a Zero Trust walkthrough** at portsys.com/contact or info@portsys.com — a PortSys specialist will work through your environment and produce a prioritised plan showing exactly where TAC contributes to your maturity goals.