ActiveShield-ZT: Presence-Bound Zero Trust for Naval Combat Data

Topic: DON26BZ03-NV059 — Real-time Zero Trust Data and Access Control for Combat Systems
Offeror: Groundbreaker Solutions LLC

1. Identification and Significance of the Problem

Naval combat systems depend on time-sensitive data flows across operators, sensors, mission applications, tactical services, shipboard infrastructure, and distributed cloud/fog environments. Existing access-control approaches remain too static, too perimeter-oriented, and too slow for combat scenarios where access decisions must be made continuously, close to the protected data, and under denied, degraded, intermittent, or limited-bandwidth operating conditions. A user, device, workload, or network location cannot be implicitly trusted merely because it previously authenticated or resides inside a nominally trusted network boundary.

Groundbreaker Solutions LLC will develop **ZT Active Presence**, a presence-bound Zero Trust access-control system that binds live operator presence, hardware-rooted wearable identity, workload identity, policy-as-code, micro-segmented data labels, AI-generated monitoring vectors, and tamper-evident audit evidence into one distributed authorization fabric. ZT Active Presence verifies access at every meaningful combat-data hop: read, write, sync, decrypt, cache, forward, export, release, and administrative override.

The innovation is a **PUF-native wearable active-presence authenticator** integrated with a cloud-to-fog Zero Trust software fabric. The wearable generates short-lived, signed presence assertions after local biometric verification. A .NET Presence Broker validates the assertion and issues a short-lived presence lease. Local policy decision points at cloud, regional, fog, and edge nodes evaluate that lease together with SPIFFE/SPIRE workload identity, data-compartment labels, policy epoch, revocation status, node posture, and AI-generated risk vectors. Policy enforcement points then allow, deny, degrade, revoke, or trigger a step-up presence check.

A Physically Unclonable Function, or PUF, derives a hardware-rooted device identity from naturally occurring microscopic manufacturing variations inside a silicon device. Because those variations are unique to each chip and are not practically copyable, the chip can reconstruct device-specific cryptographic material internally rather than storing an ordinary static secret in nonvolatile memory. In ZT Active Presence, the PUF is the root of trust for the wearable authenticator: it binds each issued device to a unique cryptographic identity and enables the wearable to sign short-lived presence assertions proving the authorized hardware, local biometric verification state, firmware measurement, nonce, timestamp, and anti-replay counter.

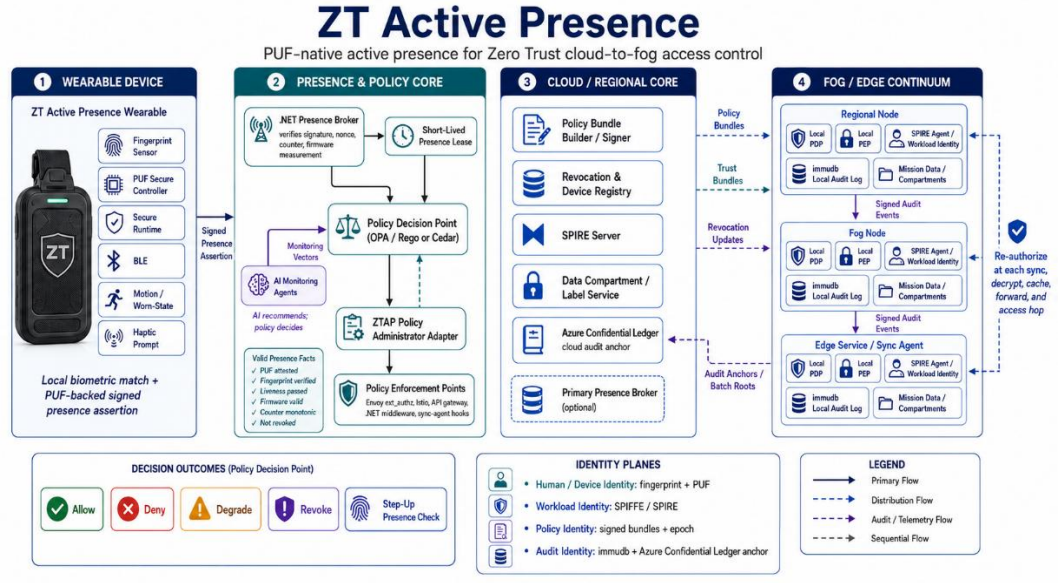
2. Technical Innovation and Navy Value

ZT Active Presence adds a missing high-assurance signal to combat-system Zero Trust architecture: **active operator presence**. Conventional authentication proves that a credential was presented. ZT Active Presence proves that an issued hardware authenticator is present, that the operator completed local biometric verification, that the device runtime is in an expected state, and that the resulting assertion is fresh, signed, and bound to anti-replay controls.

The Phase I system integrates five technical advances:

1. **PUF-backed active presence.**
   The Phase I wearable prototype uses an LPC55S69-EVK-based surrogate device with a PUF-capable secure controller, fingerprint verification path, BLE transport, haptic prompting, motion/worn-state sensing, and 3D-printed badge/belt-pack enclosure. The wearable signs short-lived presence assertions and never exports raw biometric information.
2. **Presence leases as Zero Trust policy inputs.**
   The .NET Presence Broker verifies signed wearable assertions, validates nonce freshness, checks monotonic counters, confirms device registry and revocation status, evaluates firmware measurement state, and issues broker-signed presence leases.
3. **Deterministic policy-as-code decisions.**
   OPA/Rego serves as the primary policy engine. Cedar remains available as an alternate compact authorization language for constrained environments. AI agents generate monitoring and risk vectors only; the policy engine makes final deterministic decisions.
4. **Every-hop enforcement across cloud, regional, fog, and edge nodes.**
   Envoy external authorization, Istio external authorization, API gateway hooks, .NET middleware, and sync-agent enforcement points enforce decisions before data access, synchronization, caching, decryption, forwarding, export, privileged release, or administrative action.
5. **Tamper-evident local and cloud audit.**
   immudb instances at edge and fog nodes retain local immutable audit evidence during normal and DDIL operation. Azure Confidential Ledger anchors signed batch roots, policy epochs, and audit receipts in the Phase I Azure Commercial demonstration environment.

ZT Active Presence does not replace Navy identity systems, PKI, CAC/PIV workflows, or workload identity platforms. It strengthens them with a presence-native authorization layer that continuously verifies live operator participation for actions requiring human control while preserving machine-to-machine authorization for authorized shipboard synchronization.



3. Technical Approach and Architecture

ZT Active Presence consists of four integrated layers.

Layer 1 — Wearable Active-Presence Device.

Groundbreaker will fabricate and deliver ten LPC55S69-EVK-based badge/belt-pack engineering prototypes to the Navy in the Phase I Base. Each unit will include a PUF-capable secure controller, fingerprint sensor/module, secure firmware path, BLE transport, motion/worn-state input, haptic prompt, local status indicators, and 3D-printed wearable enclosure. The device will generate signed presence assertions containing device identity, biometric verification status, firmware measurement, nonce, monotonic counter, and timestamp.

Layer 2 — Presence and Policy Core.

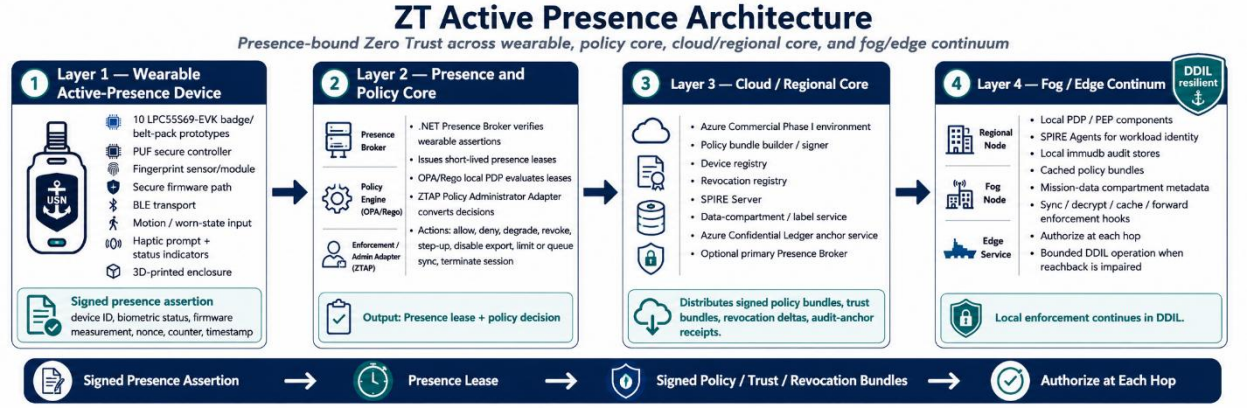
The .NET Presence Broker will verify wearable assertions and issue short-lived presence leases. The local policy decision point will evaluate these leases using OPA/Rego. The ZTAP Policy Administrator Adapter will convert policy decisions into operational actions: allow, deny, degrade, revoke, issue step-up prompt, disable export, strip fields, limit sync, queue sync, or terminate a session.

Layer 3 — Cloud / Regional Core.

The Azure Commercial Phase I environment will host the policy bundle builder/signer, device registry, revocation registry, SPIRE Server, data-compartment/label service, Azure Confidential Ledger anchor service, and optional primary Presence Broker. The regional core will distribute signed policy bundles, trust bundles, revocation deltas, and audit-anchor receipts.

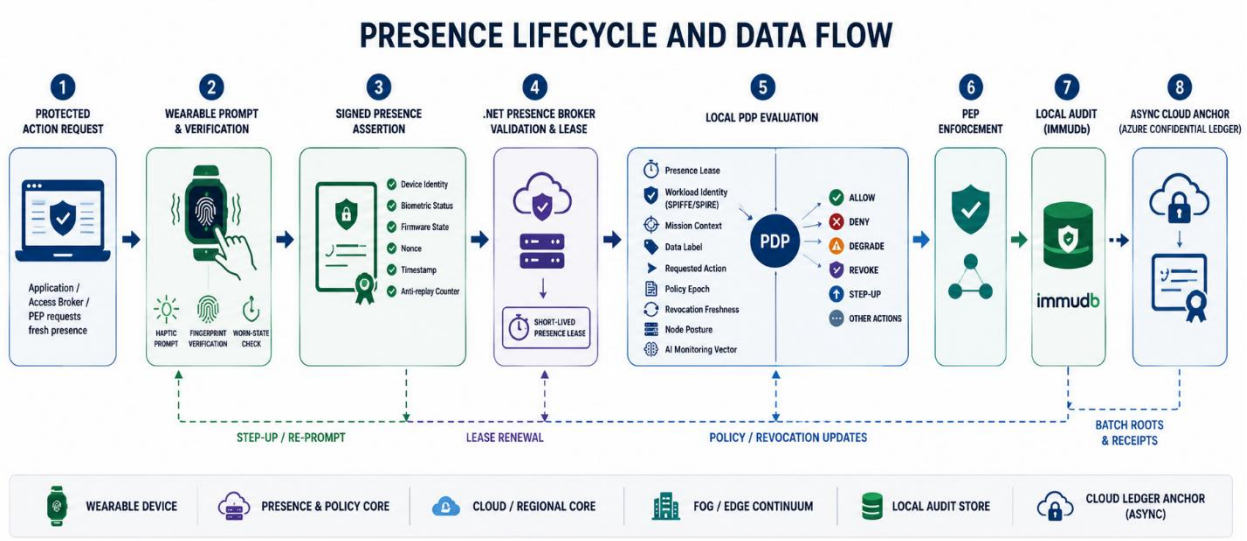
Layer 4 — Fog / Edge Continuum.

Regional nodes, fog nodes, and edge services will run local PDP/PEP components, SPIRE Agents for workload identity, local immudb audit stores, cached policy bundles, local mission-data compartment metadata, and sync/decrypt/cache/forward enforcement hooks. The system will authorize at each hop and continue operating in bounded DDIL modes when cloud or regional reachback is impaired.



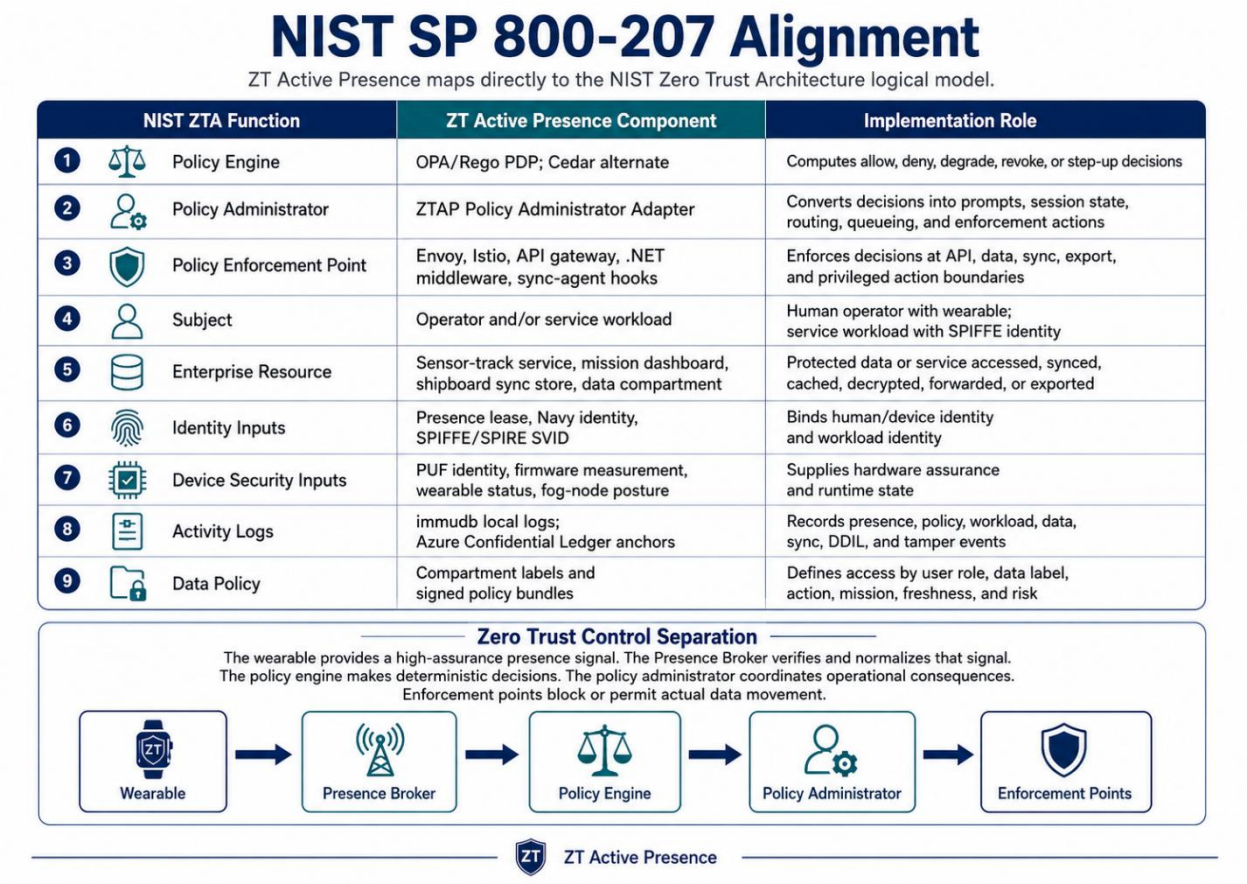
3.1 Presence Lifecycle and Data Flow

A protected action begins when an application, access broker, or PEP requests fresh presence. The wearable prompts the operator through haptic feedback, performs local fingerprint verification, and signs a PUF-backed presence assertion containing device identity, biometric verification status, firmware state, nonce, timestamp, and anti-replay counter. The .NET Presence Broker validates the assertion and issues a short-lived presence lease. The local PDP evaluates the lease together with SPIFFE/SPIRE workload identity, mission context, data label, requested action, policy epoch, revocation freshness, node posture, and AI monitoring vector. The PEP enforces the result and records the event locally in immudb. Azure Confidential Ledger anchoring occurs asynchronously through signed batch roots and receipts, keeping cloud ledger writes off the critical access path.



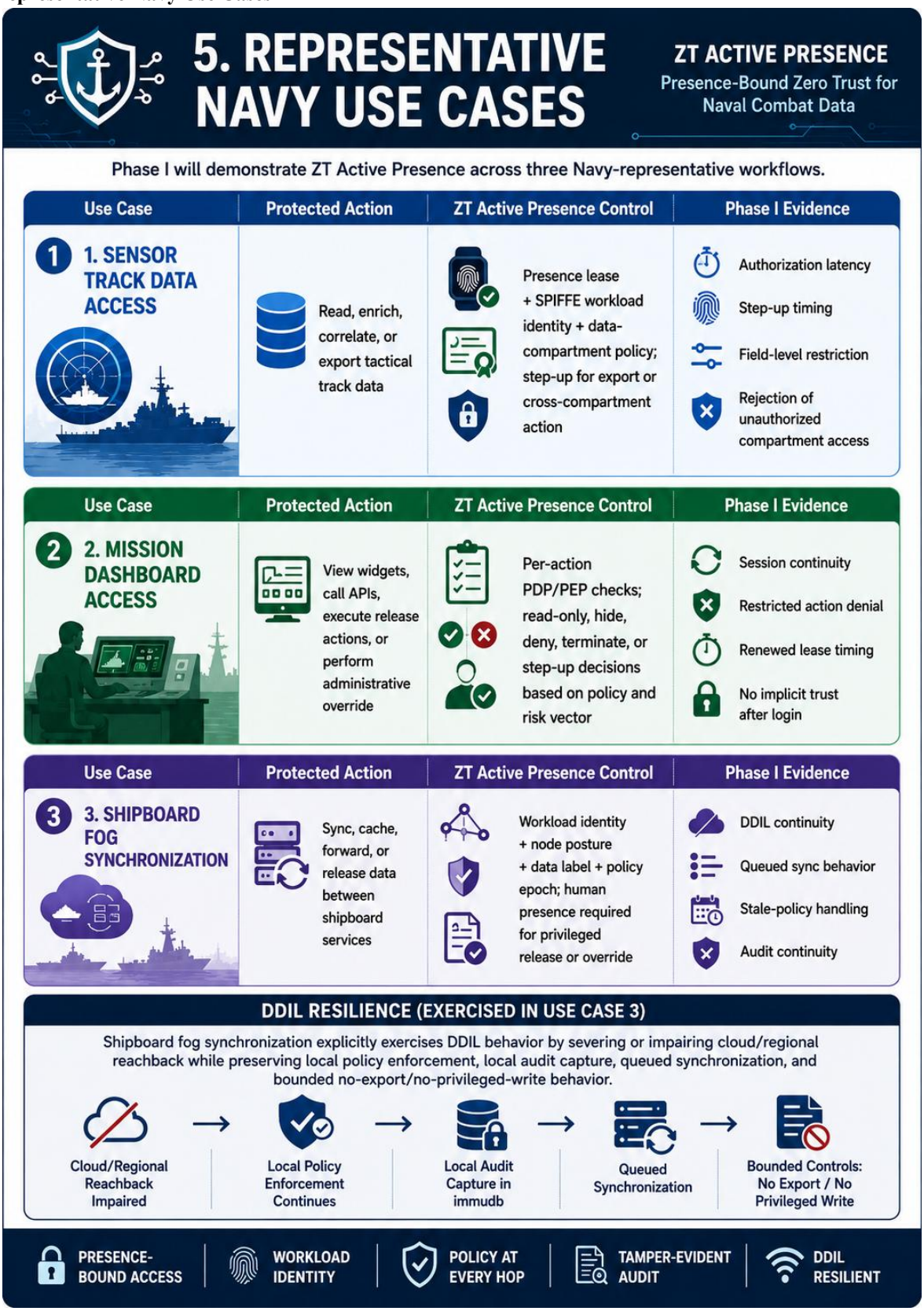
4. NIST SP 800-207 Alignment

ZT Active Presence maps directly to the NIST Zero Trust Architecture logical model.



This separation preserves the correct Zero Trust control model: the wearable provides a high-assurance presence signal; the Presence Broker verifies and normalizes that signal; the policy engine makes deterministic decisions; the policy administrator coordinates operational consequences; and enforcement points block or permit actual data movement.

5. Representative Navy Use Cases



6. Phase I Base Work Plan and Deliverables

The Phase I Base is a six-month feasibility effort. It includes delivery of ten wearable engineering prototypes to the Navy and a working cloud/fog/edge software testbed.

Base Task	Work Performed	Deliverables
Task 1 — Architecture and mission baseline	Finalize protected-resource model, trust boundaries, assertion schema, presence lease schema, policy inputs, compartment labels, and DDIL rules	Architecture package, NIST mapping, data-flow diagrams, testbed design
Task 2 — Wearable prototype fabrication and delivery	Build, provision, and deliver ten LPC55S69-EVK-based badge/belt-pack surrogate prototypes with PUF-rooted identity, local fingerprint verification path, BLE transport, haptic prompts, firmware measurement reporting, and signed assertion output	Ten Navy-delivered engineering prototypes; provisioning records; device enrollment package
Task 3 — Presence Broker and device registry	Implement .NET Presence Broker, device registry, nonce service, revocation service, counter replay guard, firmware measurement policy, and lease issuer	Broker source/configuration package, API definitions, registry and revocation workflow
Task 4 — Policy-as-code PDP and PA adapter	Implement OPA/Rego policy bundles for sensor-track access, mission dashboard access, shipboard fog sync, step-up, degrade, revocation, and stale-policy behavior; evaluate Cedar as alternate compact authorization language	Policy bundle library, policy test cases, PA adapter
Task 5 — PEP, workload identity, and fog testbed	Integrate SPIFFE/SPIRE workload identity across regional, fog, and edge services; implement PEPs at API ingress, dashboard service, track-data service, and sync-agent boundaries using Envoy/Istio or .NET middleware	PEP reference integrations, SPIFFE/SPIRE configuration, fog/edge testbed
Task 6 — Tamper-evident audit and cloud anchoring	Deploy immudb at edge and fog nodes; batch, sign, and anchor audit roots to Azure Confidential Ledger without uploading raw mission data	Local audit store, cloud-anchor demonstration, receipt verification workflow
Task 7 — Modeling, simulation, and feasibility testing	Execute the three mission flows under nominal, adversarial, and DDIL conditions; inject latency, jitter, partial disconnects, stale policy, stale revocation, revoked devices, stale leases, forged workload identity, replay attempts, and audit-chain verification events	Metrics package, demonstration dataset, Phase I final report, Phase II recommendations

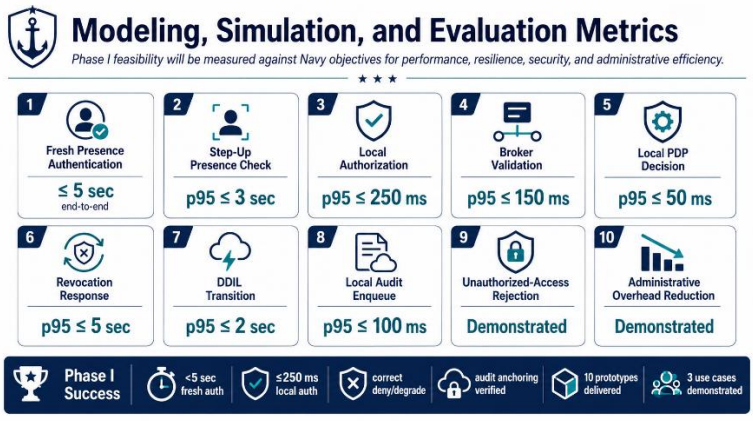
Base deliverables: ten ZT Active Presence wearable engineering prototypes delivered to the Navy; architecture package; data-flow diagrams; .NET Presence Broker; OPA/Rego policy bundle library; PEP integration examples; SPIFFE/SPIRE deployment configuration; immudb edge/fog audit implementation; Azure Confidential Ledger anchor demonstration; modeling and simulation results; Phase I final report.

7. Phase I Option Work Plan

The Phase I Option is a six-month bridge exercised upon Phase II selection. It does not repeat Base feasibility work. It converts Phase I results into a Phase II-ready technical baseline.

Option Task	Work Performed	Deliverables
Option Task 1 — Phase II system design freeze	Convert EVK-based wearable and software testbed into Phase II design specifications	Custom PCB requirements, component trade study, enclosure update, battery/power plan, provisioning architecture
Option Task 2 — Security hardening package	Finalize threat model, cryptographic protocol, enrollment/revocation workflow, secure firmware update concept, key-management plan, stale-mode profile, and DDIL security rules	Threat model, crypto specification, secure update plan, compromise-response workflow
Option Task 3 — Combat-system integration package	Define Phase II interfaces for sensor-track access, mission-dashboard control, and shipboard fog synchronization	Interface control documents, data-label model, PEP placement plan, audit event model
Option Task 4 — Expanded modeling and simulation	Extend the simulation campaign across longer outages, stale revocation, policy-bundle aging, workload identity rotation, audit-anchor backlog, and multi-node fog sync	Expanded M&S report, DDIL transition evidence, updated metrics
Option Task 5 — Phase II execution package	Prepare build, test, and transition materials for the prototype effort	Acceptance criteria, test matrix, transition roadmap, Phase II prototype build plan

8. Modeling, Simulation, and Evaluation Metrics



Phase I will measure feasibility against the Navy's stated objectives for faster authentication, reduced latency, reduced unauthorized access risk, lower administrative overhead, NIST alignment, and degraded-environment resilience.

Measurement	Phase I Target	Measurement Method
Fresh presence authentication	≤ 5 seconds end-to-end	Nonce challenge → local fingerprint check → wearable assertion → broker validation → lease issuance → PDP/PEP enforcement
Step-up presence check	p95 ≤ 3 seconds	Haptic prompt → renewed assertion → renewed lease → policy decision
Local authorization with valid lease	p95 ≤ 250 ms	PEP request → local PDP evaluation → enforcement result
Broker validation	p95 ≤ 150 ms	Signature, counter, nonce, registry, revocation, and firmware-state validation
Local PDP decision	p95 ≤ 50 ms	OPA/Rego evaluation over lease, SPIFFE identity, data label, mission context, and risk vector
Revocation response when connected	p95 ≤ 5 seconds	Revocation update receipt → session degrade or terminate
DDIL degraded-mode transition	p95 ≤ 2 seconds after freshness threshold	Detect stale policy or stale revocation → shift to bounded degraded mode
Local audit enqueue	p95 ≤ 100 ms	Event creation → local immudb write queue; cloud anchoring remains asynchronous
Unauthorized-access rejection	Demonstrated across test cases	Reject stale lease, replay, revoked device, forged workload identity, expired policy, and unauthorized compartment
Administrative overhead reduction	Demonstrated workflow reduction	Signed policy bundles, automated device registry, automated revocation, and audit verification workflow

Phase I success is achieved when the testbed demonstrates fresh presence authentication under five seconds, local authorization with a valid presence lease at p95 ≤ 250 ms, correct denial of stale/replayed/revoked credentials, correct DDIL degrade behavior, verifiable local-to-cloud audit anchoring, and delivery of ten wearable prototypes across the sensor-track, mission-dashboard, and shipboard fog-sync workflows.

9. DDIL Operations, AI Boundaries, and Audit Assurance

ZT Active Presence is designed for DDIL environments: denied, degraded, intermittent, and limited-bandwidth conditions. In DDIL mode, authorization decisions remain local to the fog or edge node using signed policy bundles, cached trust material, SPIFFE/SPIRE workload identity, local revocation deltas, local data-compartment labels, and immudb audit stores. The system does not require continuous cloud reachback to enforce policy. When connectivity is impaired, ZT Active Presence applies bounded stale-mode rules: low-risk local reads may continue where policy permits; export, privileged writes, cross-compartment release, and administrative override require fresh presence and acceptable revocation state; and all decisions are captured locally for later synchronization and Azure Confidential Ledger anchoring.

The degraded-mode policy profile includes normal mode, impaired mode, stale-revocation mode, disconnected mode, expired-presence mode, high-risk anomaly mode, and recovered mode. In normal mode, policy, revocation, and presence are fresh. In impaired mode, local authorization continues with bounded policy staleness. In stale-revocation mode, privileged writes, export, release, and cross-compartment sync are denied. In disconnected mode, operation becomes local-only with no external export, queued sync, and full audit capture. In expired-presence mode, sessions degrade or revoke. In high-risk anomaly mode, the system requires step-up presence or denies the action. In recovered mode, the system synchronizes audit batches, anchors roots, refreshes bundles, and reconciles queued sync operations.

AI is constrained to monitoring and risk vectors only. Fog-based monitoring agents analyze telemetry such as access cadence, unusual data-compartment requests, workload behavior, sync-path anomalies, failed presence checks, device motion anomalies, policy staleness, revocation-feed staleness, and abnormal degraded-mode usage. The agents emit normalized vectors such as operator risk, workload risk, sync-path risk, node-health status, policy age, and recommended step-up indicator. OPA/Rego remains the decision authority. AI does not grant access, override policy, or directly actuate the PEP.

ZT Active Presence records the evidence necessary to reconstruct who accessed what, from which device, through which workload, under which policy epoch, and with what enforcement result. Edge and fog immudb instances store full local events, including wearable boot and firmware measurement, presence assertion verification, lease issuance, PDP decision, PEP enforcement, workload identity, data label, sync/cache/decrypt/forward/export/deny events, AI monitoring-vector summaries, degraded-mode transitions, and audit-anchor batch construction. Azure Confidential Ledger stores signed batch roots, not raw combat data. Each anchor includes event range, batch ID, policy epoch, first event hash, last event hash, immudb root hash, signing workload identity, and receipt metadata.

10. Risks and Mitigations

Risk	Mitigation
EVK-based wearable is not production form factor	Phase I uses engineering surrogate prototypes to prove the PUF-backed active-presence assertion workflow; Option freezes the custom PCB and enclosure baseline for Phase II
Operator friction from repeated prompts	Policy uses short-lived leases and adaptive step-up only for sensitive actions, not fixed high-frequency prompting for every read
Revocation delay during DDIL conditions	Fast revocation deltas are separated from slower policy bundles; stale revocation denies privileged writes, export, release, and cross-compartment sync
AI explainability concerns	AI produces monitoring vectors only; OPA/Rego policies make deterministic, inspectable decisions
Policy inconsistency across fog nodes	Signed bundles, policy epochs, local freshness checks, and explicit stale-mode rules bound eventual consistency risk
Audit overhead affects access latency	Full events remain in local immudb; Azure Confidential Ledger receives signed roots asynchronously
Integration complexity	Phase I uses standard, composable components: .NET, OPA/Rego, Envoy/Istio/.NET middleware, SPIFFE/SPIRE, immudb, and Azure Confidential Ledger

11. Key Personnel, Facilities, and Human-Subjects Boundary

Jason L. Lind, Lead Investigator, is the founder and principal architect of Groundbreaker Solutions LLC and will lead the technical execution of ZT Active Presence. He brings more than 25 years of software architecture and systems engineering experience, including 24+ years of .NET full-stack development, 10+ years of Azure cloud delivery, and extensive work across secure web systems, distributed application architecture, identity integration, policy-driven workflows, and applied AI prototypes. His recent work includes ASP.NET Core, Blazor, MAUI, Azure SQL, Azure App Service, Azure Functions, Entra External ID, SignalR, PostgreSQL, Python/Streamlit simulation tools, and AI-enabled document and workflow systems. For this effort, Mr. Lind will direct the overall system architecture, .NET Presence Broker implementation, cloud/fog/edge testbed integration, policy-as-code design, prototype evaluation, and Phase II technical baseline.

Mr. Lind is a U.S. Air Force veteran with avionics backshop experience and a long-running focus on cybersecurity, Zero Trust architecture, AI governance, and mission-oriented software systems. He has authored technical work on Zero Trust architecture, cognitive cyberwar, organizational systems, and goal-oriented governance, and has supported prior federal concept development efforts involving AI orchestration, cyber operations, data analytics, and secure system modernization. His background bridges hands-on engineering and proposal-level systems thinking, making him well suited to lead a Phase I effort that must deliver working wearable prototypes, a measurable cloud/fog/edge authorization testbed, and a credible transition path toward a Navy-relevant Phase II prototype.

Jack R. Driscoll, Hardware Lead, is Chief Engineer at Groundbreaker Solutions LLC and will lead hardware integration, wearable prototype fabrication, RF/BLE communications, and device-validation activities for ZT Active Presence. Mr. Driscoll brings deep experience in RF and wireless-network engineering, including low-latency and high-reliability Wi-Fi, LTE, 5G, and mesh-network topologies for contested, infrastructure-poor, and DDIL environments. His background in signal propagation, interference mitigation, antenna/link-budget design, network-security protocols, and embedded Linux systems directly supports the Phase I requirement to deliver ten wearable engineering prototypes that can communicate securely with a cloud/fog/edge Zero Trust testbed.

For this effort, Mr. Driscoll will oversee integration of the LPC55S69-EVK-based wearable surrogate hardware, BLE transport, fingerprint module interface, haptic prompt, motion/worn-state inputs, enclosure packaging, provisioning workflow, and bench-validation process. He also brings experience with edge AI, RF-signal identification, ROS2-based autonomy stacks, mesh routing protocols, Jetson-class edge compute, and field-deployed DevSecOps workflows, giving the team practical depth across embedded systems, resilient communications, and maintainable prototype platforms. His role is central to reducing hardware risk in Phase I and translating the EVK-based badge/belt-pack prototype into a Phase II-ready production-representative wearable design.

Groundbreaker Solutions LLC is a U.S.-owned small business focused on secure software architecture, applied AI, cloud/fog systems, Zero Trust design, and mission-oriented prototype development. The company specializes in translating complex operational requirements into working technical demonstrations that combine modern software engineering, identity architecture, policy-driven workflows, data integration, and fieldable prototype concepts. Groundbreaker's recent work spans .NET, Azure, Blazor, MAUI, Python simulation tools, AI-enabled workflow systems, secure identity integration, distributed application modernization, and proposal-driven federal technology concepts involving cyber operations, AI orchestration, data analytics, and secure system design.

The Phase I work does not require Government Furnished Equipment. The representative testbed uses simulated sensor-track services, simulated mission-dashboard services, and simulated shipboard fog-sync services to demonstrate feasibility without requiring access to classified combat-system infrastructure during Phase I.

Fingerprint testing is limited to engineering verification of device, software, and access-control function. The effort does not constitute human-subjects research. The system does not study human subjects, collect biometric research datasets, or draw generalizable conclusions about human behavior. Biometric information is used only to demonstrate local device verification and is not exported from the wearable.

12. Phase II Transition and Commercialization

Phase II will mature ZT Active Presence from Phase I surrogate prototypes and representative software testbed into a Navy-relevant prototype environment. Phase II will replace simulated data adapters with representative combat-system data interfaces, refine the wearable into production-representative hardware, harden provisioning and revocation workflows, expand policy libraries, increase DDIL test coverage, integrate with Navy hosting expectations, and test against operational scenarios with simulated cyberattacks and stress conditions.

The Phase I Base delivers the working evidence: ten wearable prototypes, Presence Broker, PDP/PEP fabric, workload identity, audit chain, Azure anchor, performance metrics, and three Navy workflow demonstrations. The Phase I Option delivers the Phase II-ready design baseline: hardened security architecture, interface control documents, custom hardware specification, expanded simulations, acceptance criteria, and transition roadmap.

ZT Active Presence has direct Navy relevance and strong dual-use potential. The same architecture applies to civilian environments that require high-assurance access to sensitive data and privileged operations, including energy operations, healthcare systems, financial services, private banking, critical infrastructure, secure legal document access, industrial control environments, and executive-level privileged access. Commercial adoption will emphasize the same value proposition demonstrated in Phase I: short-lived active-presence leases, deterministic policy-as-code, workload identity, fog/edge authorization, tamper-evident audit, DDIL resilience, and degraded-mode controls.