

Naval Information Warfare Center (NIWC) Atlantic

Rapid Capabilities Cell (RCC)

Commercial Solutions Opening (CSO)

N65236-26-S-0001

Prototype Title: Project Sentinel: Joint-Service Offline Two-Person Integrity (J-SOTPI) for Tactical Systems

Area of Interest (AOI) Number: 26-A008

Command Focus Area: Battlespace Connectivity

Problem Statement:

In highly contested Joint All-Domain Command and Control (JADC2) environments, tactical systems cannot rely on external network reach-back or cellular signatures for authentication. Project Sentinel will validate an enterprise-grade software capability that enforces concurrent, hardware-validated dual-operator controls locally—ensuring that critical, single-point-of-failure actions cannot be executed single-handedly in disconnected space.

The Department of the Navy requires a prototype to demonstrate and validate an enterprise-level software capability for Two-Person Integrity (TPI) combined with Multi-Factor Authentication (MFA) for Privileged Access Management (PAM) within highly isolated, disconnected, and heterogeneous operational networks across Joint Force environments. We seek to prototype and scale a unified, non-cellular-reliant dual-authorization mechanisms to safeguard privileged functions—such as critical data deletion, privilege escalation, and network configuration changes—across diverse target systems (Windows, Linux, hypervisors, and network hardware). This effort seeks to evaluate a minimum viable product that enforces concurrent dual-operator authentication using dedicated physical hardware components (such as physical cryptographic tokens or smart cards, excluding mobile devices) in disconnected environments, ensuring critical system changes cannot be executed single-handedly. To ensure long-term supportability and integration, the technical response must explicitly define the physical hardware components required to support the solution, as well as the specific operating system and hypervisor versions supported (including legacy and modern Windows, Linux, VMware/vSphere, and Hyper-V distributions). Success will be measured by a 100% enforcement rate of concurrent, multi-factor dual-approvals under simulated disconnected-state operations, zero dependency on commercial cellular/internet networks, and documented cross-platform compatibility across all specified target systems.

Desired Solution:

Joint Force Application and Impact

A successful prototype of an enterprise-level, isolated TPI and PAM solution has critical operational significance and direct application across the Joint Forces (Navy, Army, Air Force, Marine Corps, and Space Force):

- **Multi-Branch Tactical Survivability:** In tactical operations across all service branches, critical mission-essential data (such as target tracks, cryptographic keys, and command-and-control software) is highly vulnerable to accidental deletion or unauthorized modification. Implementing dual-operator control ensures that no single point of failure or single unauthorized action can compromise critical operational systems, significantly bolstering tactical survivability and mission assurance during multi-domain operations.
- **Operational Readiness in Disconnected, Intermittent, and Limited (DIL) Environments:** Standard commercial Multi-Factor Authentication solutions depend heavily on internet connectivity and mobile phone networks for verification. For Navy afloat platforms, Army tactical command posts, and Air Force expeditionary airfields operating under emissions control (EMCON) or in disconnected environments, mobile phones represent an unacceptable electromagnetic signature and security risk. This capability provides a standardized, joint-service pathway to secure tactical systems using ruggedized, locally validated physical hardware components (e.g., YubiKeys, RSA tokens, smart cards) without external network dependencies.
- **Joint Interoperability and JADC2 Alignment:** Joint All-Domain Command and Control (JADC2) relies on the rapid sharing of secure data across heterogeneous tactical networks. Ensuring that unified, cross-platform security policies can be enforced concurrently on hypervisors (like VMware or Hyper-V) and network devices across different service branches enhances trust and secure data exchange during joint and coalition operations.
- **Supportability and Lifecycle Cost-Savings:** By requiring vendors to detail supported versions and provide long-term supportability plans for heterogeneous environments, the Joint Forces can adopt a highly sustainable software capability. This avoids the need for bespoke, siloed security solutions for individual combat systems, drastically reducing lifecycle sustainment, training, and configuration management costs across the Department of Defense.

Primary Attributes (Highly desired):

- **Access Control & Privilege Management**
 - **Concurrent Authorization:** The solution shall enforce concurrent authorization for privileged actions.
 - **Privilege Escalation Control:** The solution shall manage and control all escalations of user or system privileges.
 - **Account Lifecycle Management:** The solution shall provide capabilities to create, delete, and modify user and service accounts.

- Critical Data Protection: The solution shall have controls to prevent and audit the deletion of critical data across applications, operating systems, and storage.
- System Configuration Control: The solution shall manage and audit all configurations and changes to system and network settings.
- Integration & Interoperability
 - Change Management Integration: The solution shall integrate with existing Change Management (CM) controls through a Privilege Access Management (PAM) framework.
 - Multi-Factor Authentication (MFA) Support: The solution shall support all MFA methods currently deployed in the Navy, including Smart Card, Yubikey, RSA SecurID, and biometrics (excluding cell phone-reliant methods).
 - Third-Party Identity Integration: The solution shall demonstrate the ability to leverage and integrate with third-party Identity and Access Management (IDAM) solutions.
 - DoD Operating System Compatibility: The solution shall integrate seamlessly with common Department of Defense (DoD) operating systems.
- Operational Resilience & Logging
 - Hybrid Environment Functionality: The solution shall be enforceable on networked systems and maintain full functionality on stand-alone systems.
 - Disconnected/Degraded Operations: The solution shall remain functional and effective in disconnected, denied, or degraded network environments.
 - Administrative Log Retention: The solution shall maintain and retain comprehensive logs for administrative use, review, and auditing.

Secondary Attributes:

- Usability & Administration
 - Administrative Ease-of-Use: The solution shall demonstrate a user-friendly interface and streamlined processes for system administrators.
 - Proven Test Case Effectiveness: The solution's effectiveness must be demonstrable in a pre-defined test case that will be provided in Phase 2 Pitches.
- Integrates and leverages available infrastructure to the maximum extent.
- Ease of scalability. Does the system/technology perform and adapt automatically to different variations within the operating environment. For example, how well will the solution work as a highly available, independent, de-centralized capability with graceful degradation?
- Architecture & Scalability
 - Infrastructure Utilization: The solution shall integrate with and leverage available infrastructure to the maximum extent possible.

- Legacy System Integration: The solution must be easily integrated into existing legacy Naval platforms with minimal dependencies on specific hardware or extensive software packages.
- Environmental Adaptability & Scalability: The solution shall perform and adapt automatically to variations in the operating environment, demonstrating high availability and graceful degradation as an independent, decentralized capability.
- Advanced Audit Logging: The solution shall feature built-in audit logging capabilities that can also be integrated with third-party logging and monitoring services.

Prior Demonstration and Experience:

Preference may be given to companies that can provide evidence of quickly scalable solutions with a minimum Technical Readiness Level (TRL) of 7. Companies must demonstrate their solution in an unclassified environment as part of Phase 2. Proposers are encouraged to highlight prior experience in conducting integration and capabilities in an operational environment.

DOD Contract Security Classification Specification (DD254):

Due to the accelerated nature of the CSO timeline, the Government is requiring offerors to demonstrate the required facility clearance level at time of submission of the Solutions Brief. The contractor shall possess a Top Secret (TS) Facility Clearance with eligibility for Sensitive Compartmented Information (SCI) access to perform under this Area of Interest. Solution Briefs must contain the Cage Code for the prime contractor that would be identified on any resulting agreement. NIWC Atlantic will use the cage code provided in the Solution Brief to determine if contractor facility clearance requirements are met. Contractors that do not hold the appropriate level may not be considered for a Phase 2 Pitch.

Solution Briefs:

Interested companies shall submit a solution brief within the vulcan platform (Vulcan-sof.com) no later than 2359 Eastern Daylight Time (EDT) August 12, 2026. Solution briefs shall not contain CUI and shall meet the requirements specified in CSO N65236-26-S-0001 paragraph 7.2. In addition, the solution brief shall detail how the nontraditional business participation as defined in CSO N65236-26-S-0001 paragraph 6.2 will be met. If proposing a teaming partner to meet nontraditional requirements, that teaming partner must be identified by name in the solution brief and their cage code provided for verification. If an offeror is proposing to meet the requirements by providing a cost share, this must be explicitly stated in the solution brief.

Late submissions will not be considered.

The Government reserves the right to limit the number of entities invited to pitch based on the evaluation consideration in accordance with CSO N65236-26-S-0001 paragraph 7.2.2. Solution Briefs that are selected for the Phase 2 Pitch will be notified in writing as soon as practicable.

Pitch:

The Government anticipates hosting virtual pitches for this AOI.

Tentative dates for the pitches will be 21 August 2026 and 25 August 2026. Solution Briefs that are chosen for the Phase 2 Pitch will be notified in writing as soon as practicable. The pitch session will be centered on a demonstration of the solution. The pitch must present a complete solution and outline a credible pathway to address the full problem set.

Point of Contact:

Questions related to this AOI can be submitted to Jessie Rehwoldt:

jessie.m.rehwoldt.civ@us.navy.mil. Solutions Briefs emailed directly to Jessie Rehwoldt will not be accepted for this AOI. Solutions briefs must be submitted via the Vulcan platform to be evaluated.

Potential for Follow-On Production Contract:

Companies are advised that any prototype other transaction agreement awarded in response to this AOI may result in the direct award of a follow-on production agreement without the use of further competitive procedures.

Enclosures:

See Enclosure 1 of the RCC CSO N65236-26-S-0001 for the TS/SCI DD254 applicable to this AOI.