1.0 Project Title

Technica Continuous Monitoring and Risk Assessment Automation.

1.1 Background / Problem to be Addressed

Modern applications are evolving faster, growing more complex, and becoming increasingly distributed. The Navy faces many challenges in securing, operating, and defending their complex cyber landscape, but the current implementation of the Navy's Risk Management Framework (RMF) is labor intensive, time consuming, and expensive. The manual and siloed approach to RMF increases operational risk as the attack surface continually evolves and expands. When you need to operate at the speed of war, relying on humans and manual RMF activities is too time intensive and reactive.

These factors increase the meantime to identify and repair problems. Technica understands how imperative it is that personnel responsible for securing, operating, and defending the cyber environment have the necessary capabilities to accurately assess the cybersecurity posture with speed, provide a true understanding of the operational risk of cybersecurity exploitation or the resultant operational risk to platform (*ship, sub, aircraft, building, etc.*), missions, and Navy/Joint operations, including operations in cyberspace. Given the complexity of the cyber domain, there is a need to introduce more automation to permit operators near real-time understanding of the cyber battlespace or to provide them with the ability to operate and maneuver networks to minimize the attack surface exposed to adversaries.

1.2 Topic

This document is Technica's response to a Request for White Paper for the prototype project topic 22-PAC-0230 ConMon and Risk Assessment Automation.

1.3 Participants

Technica is a non-traditional small business contractor with 30 years' experience supporting the Department of Defense in various branches with cybersecurity, data, network management, and artificial intelligence solutions. Integral to the company's success is a dedicated Independent Research and Development (IR&D) group that explores and delivers solutions to support DoD missions. Technica will manage the project, integrate, and secure technology components to provide a continuous monitoring and automated RMF capability powered by Artificial Intelligence/Machine Learning (AI/ML) technology.
Technica's integrated solution is powered by Digitate's **ignio™,** commercial off-the-shelf (COTS), AI/ML technology. Digitate has earned 80+ patents over the past five years, helping 200+ customers overcome IT Operations challenges with security compliance, predictive, prescriptive, and preventative capabilities, including problem analysis, root cause analysis, recommended fixes, and automated actions for healing issues with cyber infrastructure.

1.4 Project Milestones

Milestone	Post-award delivery	Deliverables
Technical Approach Validation	30 days	Capabilities Document
Technical Plan Validation	60 days	System Design Document, Test Plan
Capability Demonstration	90 days	Demonstration
Prototype	180 days	Fully integrated capability
Closeout	190 days	Test report

1.5 Outline of Technical Strategy and Key Innovations

Technica acknowledges and understands the Navy's need to shift its RMF implementation from a manual stand-alone, paper-based validation approach to one that is fully integrated and synchronized with daily operations and maintenance, configuration control, and operations. Ensuring a positive security posture with a minimal attack surface goes beyond the identification and reporting of exploitable vulnerabilities. Non-compliant configurations, insufficient capacity, anomalous behavior, or degraded performance can be precursors to a security breach. Investing in a comprehensive prepare-and-protect approach to cybersecurity is more resilient to attack and positions the Navy to better isolate and recover from attacks when they do occur. By understanding the entire cyber landscape, context, and normal behavior, Technica's solution will identify, report on, and rapidly respond to events that jeopardize operational security and increase risk.

Relying on manual data processing, reporting, and remediation is not sustainable. By leveraging AI/ML technology for IT Operations (AIOps), Technica will deliver a cost-effective solution that significantly reduces data overload on operators, using automation tools to do more with less. AIOps technology can aggregate data from siloed tools, automatically reduce data noise, detect correlated anomalous patterns, verify compliance, and create timely and actionable reports at machine speed that shorten time to identification and resolution – dynamically in real-time without requiring human supervision. Employing AIOps technology will significantly increase the Navy's confidence in the ability of the operational system to meet the mission, to maneuver the network as necessary, and to optimally minimize the attack surface.

AIOps. AIOps is the overarching technology that coalesces the data and activities in cyber operations and cybersecurity, presented in a single view for situational awareness that fosters collaboration, and a single control point. Technica will integrate full-stack, domain-agnostic AIOps technology with the Government's existing systems to supplement and enhance processes and procedures through advanced analytics and automation. This results in an integrated network command and control capability that permits the Navy to operate, defend, and maneuver the network during daily operations at the system, enclave, platform, shore, and Fleet enterprise levels.

Through continuous monitoring and assessment of the risk of vulnerability exploitation, our approach automatically identifies potential and current issues, correlates vulnerability data with CVEs, CVSS scoring, security controls, DISA Security Technical Implementation Guides/Security Requirements Guide (STIGs/SRGs), and Security Content Automation Protocol (SCAP) to provide a comprehensive risk assessment. Based on correlated results, the system can provide recommended corrective actions for operator disposition or automatically take corrective action with operator approval. Our solution will interrogate external systems for context-based information, vulnerability exposure items, and security controls to build and maintain a security profile, including exceptions, for each cyber asset.

Technica's solution provides a detailed analysis report of identified vulnerabilities and non-compliant configurations that compromise system security. The control configurations can be customized to the application stack and pre-tested to avoid the risk of breaking production applications. Technica's solution for the Navy will enable automated and proactive organizational/mission risk analysis and inform system security, information security, and risk-management decisions per resource, platform, and mission. Our solution includes innovations in four key strategic areas that cover the following:

Knowledge Engineering:

- Automatic Entity Relation (ER) model generation
- Knowledge Acquisition for ER model Generation
- Knowledge Acquisition through Log Analysis

Machine Learning:

- Prediction of failures by estimating Normal Behavior of jobs in future and its cause of correlated alerts
- Preventive and predictive alerts for cyber systems
- System and Method for analysis of cyber production service support metrics

Intelligent Automation:

- Answering the What, When, and Why of Automation
- Fault detection and localization in data centers
- Prioritization, reporting, and remediation

AI & Reasoning:

- Management of vast number of alerts by alert suppression and aggregation
- Construct and leverage comprehensive blueprint of enterprise cyberspace and operations
- Automated Ticket Analysis
- Automatic generation and execution of service operation, based on ER model

Continuous Monitoring and Assessment. Relying on human capital to maintain a positive security posture for an increasingly complex cyber environment, compounded by the vast number of tools required to secure, operate, and defend cyber assets, is not sustainable. Our solution capitalizes on AIOps technology with intelligent automation to unify and process data across silos of tools to advance continuous monitoring and risk assessment from a labor-intensive, static, and tool-centric approach to a dynamic data-centric one. It provides a systematic approach to correctness and completeness of the compliance verification process to ensure a positive security posture with a minimal attack surface. This technology can be incorporated into the DevSecOps lifecycle to ensure compliance as a cyber capability progresses through its path to production.

Technica's solution will seamlessly integrate into the existing cyber environment to permit the Navy to operate, continuously monitor and analyze cyber operations and performance, and identify and mitigate vulnerabilities. The system will "learn" cyber operations and deliver the ability to self-heal incidents using machine learning and closed-loop automation that incorporates compliance verification. The system will use diagnostic analytics to identify the probable cause of issues based on learned behaviors that consider seasonality, periodicity, and configuration exceptions. Incorporating all aspects of cyber operations and cybersecurity provides a comprehensive and holistic solution because operations and security are synergistic. This will reduce Mean Time to Repair (MTTR) and move the Navy from a reactive monitor and respond security model to a proactive prepare and protect model.

The following are the key compliance features of Technica's solution:

- Supports various industry security benchmarks as well as DoD-specific controls
- Supports 30+ technology versions for compliance auditing
- Detects 5500+ types of vulnerabilities across supported technologies
- Provides the facility to add and manage exceptions across the vulnerabilities profile
- Offers automatic remediation support for ~1000 vulnerabilities
- Provides the flexibility to add or edit security controls to manage exceptions
- Provides extensible reporting capabilities for exporting to other DoD-compliant systems, such as eMASS

Innovative Results. Using relationship inference through its powerful algorithm, Technica's solution provides real-time context-based observability and risk assessment across Navy platforms. The necessary application dependency mapping and service topologies required for effective analytics are extracted from existing tools, data stores, system logs, Security Information and Event Management (SIEM) systems, vulnerability scanning tools, or directly from managed cyber resources. The context-based information will be available to external systems through APIs for actionable insight, compliance status, and risk posture. By harnessing machine learning techniques and automation, the Navy can reduce the high-volume, low-complexity human-intensive tasks such as resolving frequent problem patterns, performing impact analysis on configuration changes, assessing risk, generating status and compliance reports, and optimizing capacity for a more proactive operation.

Open Architecture and Interoperability. By combining best-of-breed solutions and best practice approaches, Technica's IR&D team creates Reference Architectures for the target requirements. While a given proprietary technology/vendor may be selected as a component of a Reference Architecture, Technica seeks to facilitate the interchange of vendor technologies by making sure the vendor solution adheres to open standards/open interfaces as much as possible. **Figure 1** provides a Reference Architecture of the solution for the Navy's Continuous Monitoring and Risk Assessment Automation prototype project.

Data Hub. The Technica-developed data hub is a critical platform component for ingesting, transforming, enriching, and filtering data between providers and consumers. It includes features that abstract the data interface details from the data store to enable a highly flexible and scalable pipeline. The data hub centralizes and offloads the burden of data integration to provide a more rapid and scalable data environment by enabling other technology components to focus on their core competencies and not worry about the changing interfaces as they evolve. It will be the integration point with the Navy's cyber operations Data Analytic Fabric (DAF).

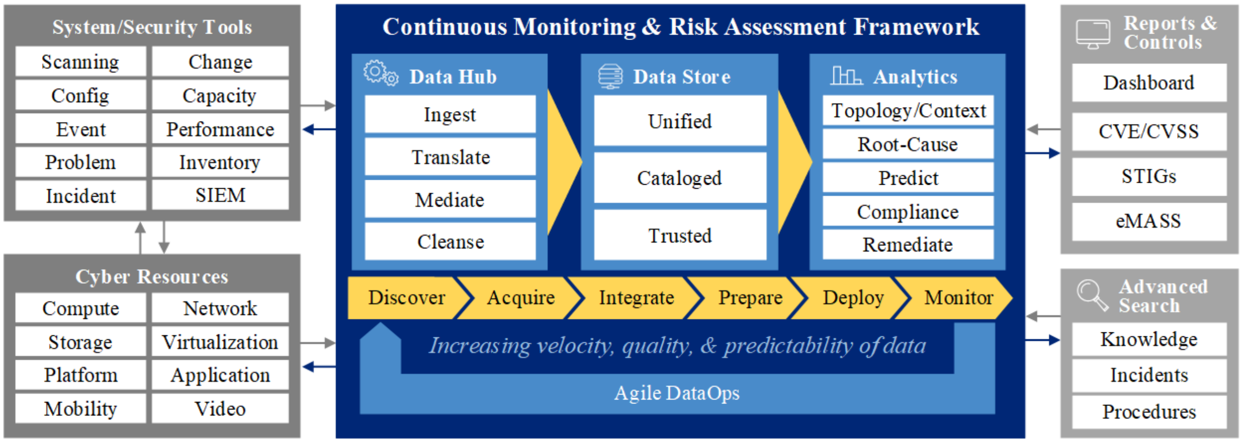

Figure 1. Technica's Reference Architecture for Continuous Monitoring and Risk Assessment.

The Technica Agile Continuous Improvement Process. The Technica Team has broad experience evaluating and adopting new and innovative technologies. Our staff will apply the strength of our Agile Technology Evaluation, Capability Development, and Integration Process. We have honed this process over three decades supporting the DoD and developed a standard operating procedure. This investigative workflow defines and executes data-centric use cases to support the rapid and continuous adoption of emerging technical capabilities amid ever-evolving requirements. Working with the Navy, Technica will:

- Apply a value-driven use case lifecycle methodology for delivering a solution aligned with mission objectives to provide clarity and certainty of realizing customer expectations.
- Define data-centric use cases, build components, test prototypes, and evaluate alternative approaches through rapid iterations of user stories and reprioritization of the product backlog.
- Integrate Navy personnel into the solution development for faster responsiveness to changing conditions.
- Allow stakeholders to make decisions early to mitigate risk to project costs and schedule.
- Apply a "fail fast" mindset to minimize project risk when identifying, evaluating, and adopting innovative technologies. When a workaround cannot be established, the investigation is terminated, and resources are redistributed to the next priority in the product backlog.

1.6 Significant Materials and Equipment Required

Technica's solution is a software and process deliverable designed to work in conjunction with the Navy's legacy and future systems via API interfaces. There are compute and storage requirements for data processing and network requirements for connectivity between data providers and consumers. As a purely software-based solution that can operate on virtualized infrastructure, Technica will leverage the virtualized infrastructure within its IR&D lab. During the design phase of the project, Technica will define capacity and network details for a Navy production deployment. Technica does not expect any extraordinary requirements in this regard. Commercial technology integrated into our solution is licensable, and any fees required for the prototype project will be included in the final proposal.

The capacity requirements that Technica anticipates leasing for the prototype project include 92 virtual cores, 192GB memory, 3,238GB storage. To maximize functional density within constrained spaces, Technica will investigate ways to reduce the solution's footprint during the prototype development phase without sacrificing performance.

1.7 Technical Maturity

Digitate's **ignio™** software is commercially available and used in a wide range of industries, including Banking and Finance, Energy and Utilities, and Telecommunications and Retail at a current Technology Readiness Level (TRL) of 8. Technica's data hub draws on Technica's agile development approach and years of technology and data integration for the Federal Government for an overall delivered system TRL of 7 before the transition to Plan of Record (POR).

1.8 Intellectual Property/Data Rights Assertions

It is anticipated that upon award, Technica and the Government shall enter a mutually agreeable contract that would provide the acceptable limited, unlimited, or other requisite license or ownership rights in any work product, deliverables, works for hire, or third-party products, as applicable, to provide the Government with adequate rights for the scope of sustainment/maintenance activity, including without limitation the creation of derivative works for such purposes. Except as to such mutually agreed rights in the foregoing, to the extent that Technica utilizes any of its or its suppliers' and subcontractor's property and derivatives thereof (*including but not limited to computer software, APIs, algorithms, technical data, data rights, patents, trade secrets or other intellectual property*) in performing under the contract, such property remains the property of Technica or such licensors.

1.9 Success Metrics

Technica will develop and integrate proven commercial technology that will deliver the following improvements for securing, operating, and defending the Navy cyberspace. Our operating assumption is that baseline metrics of current processes are available from the Government. Technica, operating in cooperation with the Government, may need to modify these success metrics pending the availability of data and customer input.

Use Case	Success Criteria	Target Improvement
Event management	Detect and suppress "false" alerts by aggregating and correlating associated alerts	90% noise reduction measured by the number of false alerts reported
Health check	Perform non-functional health checks on application and associated technology stack, and display/send results	50% reduction of manual effort, measured by person-hours
Self-heal	Detect actionable alerts and perform automated remediation	80% MTTR improvement measured by person-hours
Compliance	Improve security compliance of audited systems	85%+ compliance level

1.10 Implementation and Transition

Upon completion of this project, Technica will deliver a TRL 7 system capable of transition to POR in 9-12 months. The transition is comprised of the following steps:

Remediation / Improvements Based Upon Lessons Learned: The Navy will review the final prototype for how well it meets requirements as defined. While Technica expects to meet ALL baseline requirements, we expect requests for some configuration, reporting, action alert, or interface improvements.

RMF/ATO Process: Technica will secure all system components according to DoD Security Requirements Guides and DoD Security Technical Implementation Guides. Technica will prepare Risk Management Framework (RMF) packages sufficient to gain official Authority to Operate (ATO) from the Government, and work with the appropriate organizations to list it on an Approved Product List, such as the Department of the Navy Application and Database Management System (DADMS), to certify secure operations and interoperability of the system for use by other DoD entities.

Commercialization: All Federal agencies and commands subject to the mandates of RMF with complex, extensive networks and/or data center environments are potential customers for this effort. The United States Government Manual lists 96 independent executive units and 220 components of the executive departments. An even more inclusive listing comes from USA.gov, which lists 137 independent executive agencies and 268 units in the Cabinet. This universe is the Total Addressable Market. The Serviceable Addressable Market is a subset of these larger agencies, limited by Technica personnel but more likely budget constraints. The actual Service Obtainable Market (SOM) would be Federal agencies with a need for secure, RMF-compliant systems. The complexity and scale of security compliance is proportional to the agency size. The primary DoD services, DISA, Federal health care, DHS, law enforcement and Treasury are all target Federal organizations that will have a need for a proven solution. These agencies may be considering competing solutions. A critical competitive advantage of this system is proven history in a certified Government environment and lessons learned with the Navy.