A Framework for Automated STIG Compliance for Navy Ships

Margaret L. Graves, Alan Shaffer and Gurminder Singh
Naval Postgraduate School, Monterey, California, USA

margaret.graves@nps.edu
alan.shaffer@nps.edu
gsingh@nps.edu

Abstract: Historically, U.S. Navy ships have faced challenges in meeting the requirements of Cybersecurity Inspections (CSIs), with persistent Security Technical Implementation Guide (STIG) compliance gaps as a major contributing factor. Ships have relied on manual remediation processes that are often time-consuming and error-prone, given IT staff and operational constraints. Existing STIG automation tools do not address unique afloat challenges, such as intermittent connectivity, diverse network architectures, integration with cyber-physical systems, and split authorities between ship and Program of Record (PoR) managers. Commercial tools like SteelCloud ConfigOS, Ansible Automation Platform, and Microsoft PowerSTIG demonstrate automation feasibility in traditional enterprise environments, but do not adequately accommodate maritime operational realities, where ships undergo extended periods of limited network connectivity. This research developed an automated STIG compliance toolkit framework to address maritime constraints by systematically analysing existing tools, identifying cybersecurity capability gaps, and deriving requirements from documented CSI deficiency patterns and operational constraints. The framework's modular design includes asset discovery with coverage validation, compliance assessment with baseline deviation detection, risk-stratified automated remediation, and human oversight through Information Systems Security Manager (ISSM) decision support, while respecting authority boundaries between shipboard IT teams and PoR managers. Validation of the framework employed requirements traceability analysis, mapping 48 requirements to design components, workflow analysis, tracking data flow through representative compliance scenarios, and engaged with experts at Naval Information Warfare Center Pacific cybersecurity specialists to evaluate operational feasibility. The results confirmed the framework's validity and practicality while revealing that organizational factors beyond technology, including formal sustainment authority assignment, improvements in PoR baseline documentation processes, and enhanced network inventory data quality, are essential to successful framework deployment. The framework provides a comprehensive requirements baseline, modular architecture supporting platform diversity, and authority-aware decision logic that preserves operational safety. Future work on this research will include developing a system prototype, integrating machine learning for predictive risk management, and expanding research to examine additional CSI improvement factors.

Keywords: Navy cybersecurity, STIG compliance, Automated remediation, Maritime operations, Risk management Framework, DevSecOps

1. Introduction

U.S. Navy ships continue to face persistent cybersecurity readiness challenges. Compliance with the Cybersecurity Inspection (CSI) Technology Area standards, shown in Figure 1, which includes evaluating STIG implementation, accounts for 60% of the CSI grade. However, fleet performance remains inadequate despite sustained efforts from operational commanders and program offices (Office of Compliance and Assessment, 2024; Naval Information Warfare Systems Command, 2024). Ships rely on manual STIG remediation processes that require excessive IT personnel hours, introducing human error, and that are unsustainable due to limited shipboard resources and high operational tempo.

The maritime environment presents unique cybersecurity challenges that set afloat platforms apart from shore-based enterprise networks. Ships often operate with intermittent satellite connectivity, which limits their access to shore-based cybersecurity support and results in bandwidth constraints for security updates (Commander U.S. Fleet Cyber Command, 2023). The diversity of fleet networks adds to remediation challenges, with ships operating different architectures, from modern Consolidated Afloat Networks and Enterprise Services (CANES) to highly heterogeneous legacy systems. Many shipboard systems operate for decades, leading to persistent vulnerabilities from outdated hardware and software (Akpan et al., 2022). These factors create an environment where shore-based cybersecurity tools may not fully address operational realities.

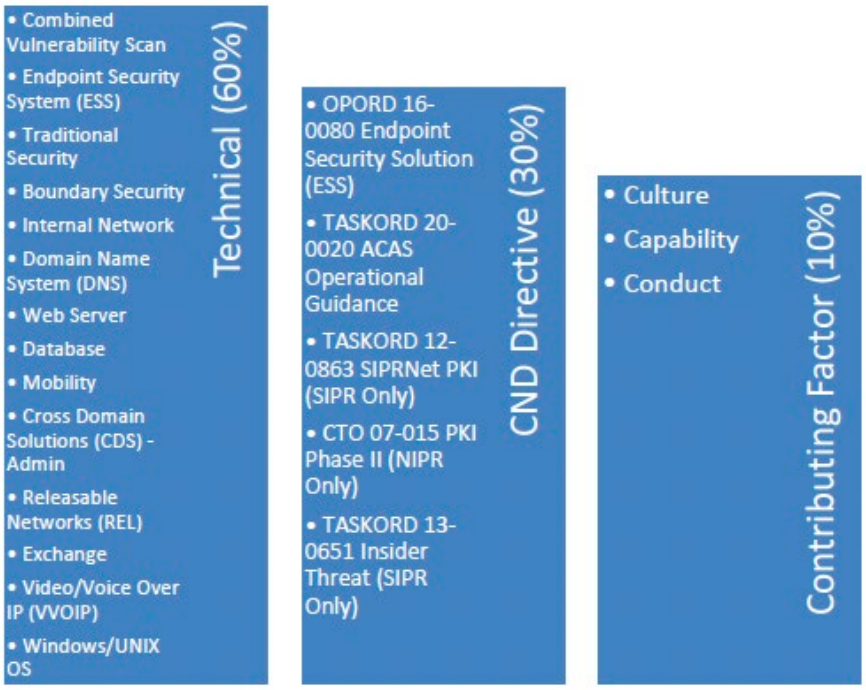

Figure 1: CSI Scoring Breakdown

Current STIG automation tools work well in onshore enterprise environments but lack adaptability to maritime constraints. Commercial products such as SteelCloud ConfigOS (SteelCloud, 2025), Ansible Automation Platform (U.S. Department of Defense, 2024), and Microsoft PowerSTIG (Microsoft, 2025a; Microsoft, 2025b) provide automated STIG remediation for enterprise networks with strong connectivity and centralized management. However, none of these tools comprehensively addresses the operational isolation, limited support infrastructure, and stakeholder complexities common to remote afloat operations. Additionally, fragmented authority between the ship's force and Program of Record (PoR) managers creates coordination issues that automated tools must account for (Naval Information Warfare Systems Command, 2024).

This research developed an automated STIG compliance toolkit framework specifically addressing maritime platform constraints and complexities. The framework combines asset discovery, compliance assessment, and automated remediation features, while maintaining human oversight for high-risk decisions and respecting authority boundaries between shipboard IT teams and PoR managers.

2. Background

The maritime operational environment imposes unique constraints on cybersecurity operations that distinguish afloat platforms from shore-based installations. This section examines these constraints and analyses current Navy cybersecurity tools to identify critical gaps that prevent effective STIG compliance aboard ships. Understanding these limitations provides the foundation for requirements of a STIG mitigation framework.

2.1 Maritime Cybersecurity Constraints

Maritime cybersecurity faces significant connectivity challenges. Ships depend on satellite communications with intermittent, high-latency links that limit bandwidth for security updates. Many shipboard systems are air-gapped to reduce threat exposure, including navigation, propulsion, and combat systems. While this isolation reduces external attack surfaces, it complicates routine compliance operations by requiring manual actions that can lead to human error (Pseftelis and Chondrokoukis, 2021).

U.S. Navy ships operate for decades, creating cybersecurity challenges as end-of-life and end-of-support systems still in use present ongoing vulnerabilities (Akpan et al., 2022). Fleet network diversity adds to these challenges, as ships run different architectures, from newer CANES installations to legacy Integrated Shipboard Network System, with specialized platforms needing unique configurations. This heterogeneity hinders standardized compliance methods and requires platform-specific STIG implementation strategies.

Cybersecurity responsibilities afloat are distributed among various stakeholders. The ship's force handles some systems, while program offices oversee others, requiring remediation strategies that respect these authority boundaries. The ship's crew records vulnerabilities using platform-specific plans of action and milestones (POA&M) for issues needing local remediation, while PoR-managed system vulnerabilities are escalated through multiple channels (Naval Information Warfare Systems Command, 2024). Even when PoR system managers issue patches, operational commanders might delay application due to concerns about mission-critical system stability. Although CANES offers a structured 30-day patch management cycle with patches accessible to the fleet, trend analysis shows limited patching across Navy ships (Office of Compliance and Assessment, 2024).

2.2 Current Tool Limitations

Navy ships use various tools for STIG compliance assessment, but these tools focus on noncompliance identification rather than remediation. Evaluate-STIG, developed by Naval Surface Warfare Center (Naval Sea Systems Command, 2020), provides automated STIG scoring and visual dashboards that display compliance status. Although it is not formally integrated into the CANES cybersecurity toolkit due to size constraints, Navy cybersecurity authorities actively promote its use over Security Content Automation Protocol for comprehensive compliance assessment (Office of Compliance and Assessment, 2024). The tool is used in all authorization and system reviews and validations for system authorization (Ireland, 2023). However, Evaluate-STIG does not enforce or remediate, limiting its utility to compliance verification and reporting.

The Assured Compliance Assessment Solution (ACAS) system, which uses Tenable technology with Nessus vulnerability scanners, is mandatory on board ships (Joint Force HQ-DoDIN, 2020). ACAS serves as the mandated enterprise vulnerability scanning tool for Department of Defense (DoD) systems, emphasizing network-wide vulnerability assessment rather than STIG compliance. Both Evaluate-STIG and ACAS provide vital visibility into system compliance, but do not provide automated STIG remediation.

Commercial STIG remediation automation tools exist but are not widely deployed in afloat environments. SteelCloud's ConfigOS automates STIG scanning, remediation, rollback, and reporting, but it requires enterprise licensing and formal deployment through Naval Systems Commands (SteelCloud, 2025). PowerSTIG leverages PowerShell Desired State Configuration to apply and monitor STIG controls on Windows systems, but it is limited to Windows environments (Microsoft, 2025a; Microsoft, 2025b). The Ansible Automation Platform enables Infrastructure-as-Code via reusable automation playbooks but depends on mature development pipelines and customized playbooks for each platform (U.S. Department of Defense, 2024).

These tools demonstrate that remediation automation is feasible and effective, but deployment barriers include platform specificity, tool fragmentation, and authorization requirements. Main limitations include the need for continuous connectivity, the assumption of a homogeneous network, and the absence of authority-aware decision logic for divided responsibilities between the ship and PoR managers.

3. Framework Design

The framework design process involved a systematic analysis of documented fleet challenges to identify technical requirements, which were then translated into a modular architecture adapted to maritime constraints. This section details the requirements definition approach, presents the system architecture with its six core components, and describes specific adaptations to address afloat operational realities.

3.1 Requirements Definition

The research team analysed authoritative sources to identify framework requirements, including Office of Compliance and Assessment (OCA) Waterfront Engagement Brief findings on documentation management issues where ships possessed required justification documents for PoR findings but did not provide them to OCA during assessments (OCA, 2024). The NAVWAR "Get Real, Get Better" artifacts documented program office shortfalls in resolving STIG findings for PoR systems in a timely manner (Naval Information Warfare Systems Command, 2024). The OCA CSI Planning Guide (Fleet Cyber Command, 2024) establishes that any DoD-published STIG applicable to inspected systems can be used during CSI evaluations.

The analysis uncovered recurring patterns: inconsistent STIG implementations across platforms, unclear configuration baselines, fragmented documentation between operational units and program offices, and ongoing delays in PoR system remediation. Naval Information Warfare Center Pacific cybersecurity personnel provided expert advice, highlighting key implementation factors. Subject matter experts stressed that gaps in baseline knowledge are a bigger obstacle than originally thought, noting that ships often operate without a full

understanding of approved operational baselines. This insight raised configuration discovery from a minor feature to a vital capability. Experts also pointed out that validating asset coverage is crucial, especially since scanning tools often miss systems due to network segmentation and offline status.

The requirements definition produced 48 detailed requirements organized into seven functional categories (data processing, baseline detection, asset coverage, decision support, automated remediation, escalation and coordination, documentation and reporting) and five non-functional categories (maritime environment, platform diversity, performance, security and authorization, sustainment). Each requirement traces to specific framework components, allowing verification of architectural completeness.

3.2 System Architecture

The proposed toolkit uses a modular design that follows a six-step process, balancing automation with human oversight, as shown in Figure 2. The process gathers IT input sources from Evaluate-STIG and manual assessments, parses and identifies findings while performing automated system discovery, allows the Information Systems Security Manager to review and make decisions, executes automated remediation, reviews unresolved issues, and exports reports for inspections.

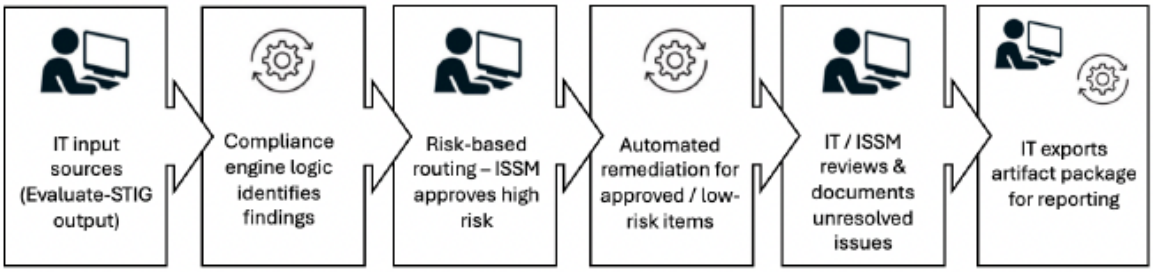

Figure 2: STIG Toolkit Workflow

Figure 3 shows the main system components and how they interact. The input parser imports data from various IT compliance sources, accepting Evaluate-STIG results and STIG Viewer files while also performing asset discovery validation to ensure thorough coverage. The parser checks discovered assets against trusted network sources, including switch Address Resolution Protocol tables, Dynamic Host Configuration Protocol lease tables, and documented IP allocation plans, to identify systems that haven't been scanned.

The compliance engine acts as the analytical core, containing a knowledge base of STIG requirements and applying rule-matching logic to compare parsed findings against established baselines. During analysis, the engine automatically discovers configurations by scanning system registries, configuration files, network settings, and service configurations to create current "as-built" baselines that support risk assessment decisions. The compliance engine correlates findings from multiple sources using Control Correlation Identifiers as defined by DISA (Defense Information Systems Agency, 2025).

A key function is baseline deviation detection, which prevents the toolkit from remediating findings necessary for system operation. Using the discovered configuration data and previous remediation results, the engine classifies findings as either PoR baseline requirements (do not remediate), approved exceptions with entries to the POA&M (for tracking only), or remediable findings (safe to fix automatically).

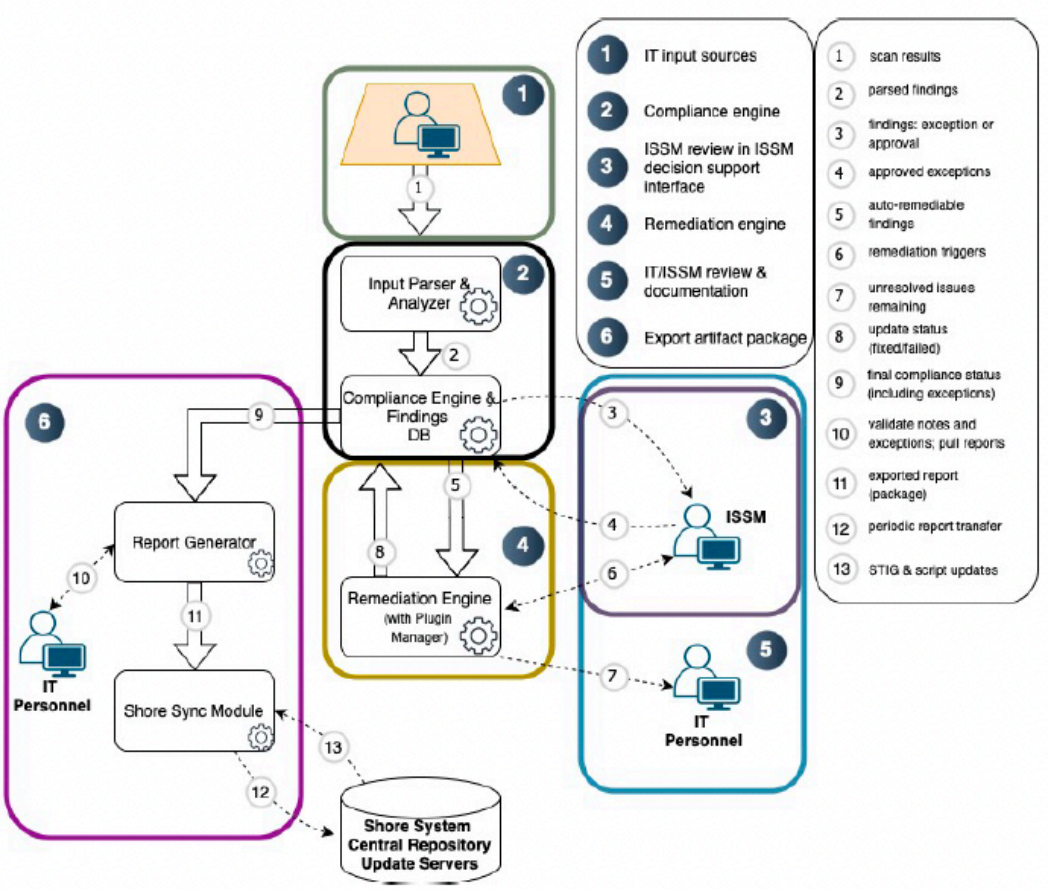

Figure 3: Detailed STIG Toolkit Control Flow

The Information Systems Security Manager (ISSM) decision support interface incorporates human oversight by displaying findings organized by category and risk level, with clear visual cues that distinguish PoR baseline findings from remediable issues. This enables ISSMs to approve automated remediations only for genuine security problems while maintaining necessary operational configurations and preserving command authority as required by Navy regulations (Department of the Navy, 1990).

The remediation engine performs authorized configuration changes using a modular plugin system. The Plugin Manager chooses suitable remediation tools based on system details and STIG type, supporting PowerSTIG for Windows (Microsoft, 2025a), Ansible for Linux (U.S. Department of Defense, 2024), and custom scripts for specialized systems. The engine features automated rollback functions and detailed logging, recording both success and failure statuses while conducting post-change verification.

The report generator produces comprehensive artifact packages, including STIG checklists, remediation logs, and exception documentation that adhere to DoD reporting standards (Fleet Cyber Command, 2024; Joint Task Force Transformation Initiative, 2018). The shore synchronization module handles asynchronous data exchange with shore-based systems during connectivity windows by uploading compliance results and downloading STIG updates using bandwidth-efficient compression and differential updates while operating in default offline mode.

3.3 Adaptation to Afloat Constraints

The framework addresses maritime constraints with specific design adaptations. Its modular, plugin-based design supports various network configurations, where modules focus on particular systems while keeping a standardized core (Seferagić et al., 2021). Containerized deployment ensures consistent operation across different environments by packaging all dependencies into portable images, addressing legacy system compatibility and complying with Navy cybersecurity accreditation practices using DoD Iron Bank hardened base images (DoD Chief Information Officer, 2025).

The framework includes pre-positioned remediation libraries with local repositories of STIG content and remediation scripts prioritized by historical findings, with updates synchronized during connectivity windows.

Role-Based Access Control separates shipboard administrative privileges among stakeholders, enabling complete automated remediation for Navy-administered systems while providing scanning and reporting only for program office-managed systems.

Technical challenges require targeted mitigation strategies. For legacy system integration across diverse platforms, the modular plugin architecture allows custom development for platform-specific needs, while plugin isolation helps prevent compatibility issues. During extended deployments, offline STIG updates are supported by local repository management with prioritized caching and differential updates, ensuring critical content delivery during brief connectivity windows. Performance optimization includes multi-threaded architecture for concurrent processing and database indexing on frequently queried fields for rapid analysis of thousands of findings (PostgreSQL Global Development Group, 2025). Security accreditation requirements are met through phased implementation, starting from minimal-authorization proof of concept, advancing to containerized deployment, and finally integrating with Platform One for Authority to Operate coverage (Joint Task Force Transformation Initiative, 2018; Department of Defense Chief Information Officer, 2025).

4. Validation

Validation of the framework employed three complementary methods suitable for conceptual architecture research: requirements traceability analysis to verify completeness, workflow analysis to demonstrate logical consistency, and expert consultation to assess operational feasibility. This approach establishes framework soundness without requiring prototype implementation or operational fleet data.

4.1 Requirements Coverage Assessment

Requirements traceability analysis creates formal links between documented CSI deficiency root causes and derived system requirements. The research team developed a Requirements Traceability Matrix that consolidates 48 detailed requirements into seven functional categories (data processing, baseline detection, asset coverage, decision support, automated remediation, escalation and coordination, documentation and reporting) and five non-functional categories (maritime environment, platform diversity, performance, security and authorization, sustainment), demonstrating comprehensive coverage of identified fleet compliance challenges. Each requirement is linked to specific framework components and referenced sections, enabling systematic assessment of design coverage.

The analysis identified five key dependencies beyond technical design: PoR baseline documentation requiring program office involvement in documenting approved configurations, network inventory data quality greatly influencing asset discovery accuracy, formal sustainment agreements assigning Program Manager Warfare-130 responsibility for core toolkit maintenance while Systems Commands maintain platform-specific plugins, uncertainty in the authorization timeline for containerized deployments adding schedule risk, and PoR coordination channels requiring established communication mechanisms and tracking systems. These dependencies are not flaws in the framework but realistic factors that require organizational coordination alongside technical development.

4.2 Workflow Analysis

Workflow analysis examined three representative compliance scenarios derived from documented CSI deficiency patterns. The bulk Windows Group Policy Object remediation scenario demonstrated an end-to-end data flow from input through remediation and documentation, confirming that the architecture supports high-volume, low-risk remediation. The workflow revealed dependencies, including PoR baseline database accuracy, plugin compatibility across finding types, network stability during multi-host remediation, and ISSM confidence in bulk approval decisions.

The PoR baseline configuration scenario evaluated the framework's ability to distinguish between operationally necessary configurations and actual security vulnerabilities. The baseline detection logic effectively categorized findings into documented baselines marked "do not remediate," flagged high-risk systems without baseline matches for manual review, and findings suitable for automated remediation. The scenario's success relies heavily on the accuracy of the PoR baseline database, dependable system identification through hostname conventions and network topology, ISSM's understanding of baseline justifications, and OCA inspector acceptance of documented baseline rationale.

The external authority escalation scenario demonstrated the toolkit's ability to identify findings that require program office intervention. The process of generating the escalation package compiles details of technical findings, system identification and authorization boundaries, impact assessments, recommended remediation

approaches, and POA&M templates with PoR designated as the responsible party, in accordance with DoD Risk Management Framework requirements (Joint Task Force Transformation Initiative, 2018). This workflow introduces structured escalation processes that are currently absent in fleet operations but relies on accurate system ownership data, established communication channels, timely PoR responses, and tracking mechanisms for long-term issue resolution.

4.3 Expert Consultation

Consultations with Naval Information Warfare Center Pacific cybersecurity subject matter experts (SME) provided an operational feasibility assessment of the framework architecture. Experts reviewed the modular architecture concept and identified key operational considerations during development of the framework. A design debate arose regarding the necessity of human oversight in the remediation workflow, with SMEs initially suggested full automation without ISSM approval, arguing that required reviews could reduce efficiency and hinder adoption. However, the final framework intentionally maintains the ISSM decision support interface, aligned with Navy operational principles where commanding officers remain responsible for all matters affecting their command (Department of the Navy, 1990), and Office of the Chief of Naval Operations cybersecurity policy explicitly assigns ISSM responsibility for the security of information systems (U.S. Navy, 2018). When automated remediation affects mission-critical systems, the framework ensures that commanding officers remain accountable for operational outcomes, regardless of whether a human or technical tool made the decision.

Expert consultation revealed that baseline knowledge gaps pose a more significant implementation barrier than initially assessed, with ships often operating without a comprehensive understanding of approved operational baselines. This insight elevated configuration discovery from a supplementary feature to a core capability, indicating the toolkit must actively document system states and build institutional knowledge rather than assuming complete baseline documentation exists. Experts also identified asset coverage validation as essential, noting scanning tools frequently miss systems due to network segmentation and offline status, creating false confidence about assessment completeness. The consultation highlighted that sustainment authority requires a formal organizational assignment, recommending PMW-130 manage core toolkit sustainment while SYSCOMs maintain platform-specific plugins and baseline exceptions.

5. Conclusions

This research developed an automated STIG compliance toolkit framework to address ongoing Navy shipboard cybersecurity compliance challenges through risk-stratified automation. The framework incorporates existing Navy cybersecurity tools, while maintaining human oversight for high-risk decisions, balancing automation efficiency with operational command authority requirements.

Validation through requirements traceability analysis, scenario-based workflow analysis, and cybersecurity subject matter expert consultation demonstrates the framework's logical soundness and operational feasibility. The analyses showed that successful implementation requires concurrent attention to organizational factors beyond technical architecture, including formal sustainment authority assignment, PoR baseline documentation processes, and network inventory data quality improvements. These findings indicate that while the toolkit architecture incorporates essential technology capabilities for enhanced fleet compliance, achieving measurable CSI improvements depends on addressing organizational coordination and data quality challenges.

The framework offers Navy leadership a clear path toward improved fleet cyber readiness. Key contributions include a detailed requirements baseline based on documented fleet cybersecurity challenges, a modular architecture that supports diverse shipboard environments while maintaining standardized core functions, risk-stratified automation that ensures operational safety through baseline deviation detection and ISSM oversight, and authority-aware decision logic that respects stakeholder boundaries between the ship's force and PoR managers. Detailed implementation specifications, including parsing algorithms, database schemas, and remediation logic, are available in the full thesis manuscript.

Future work in this area will include developing prototypes to validate framework performance against actual CSI benchmarks. Other work will include integrating machine learning algorithms to shift the framework from reactive compliance checking to predictive risk management (Yang et al., 2024), exploring integration with Navy zero-trust architecture initiatives (Department of Defense Chief Information Officer, 2022) to support continuous device posture assessment, and investigating additional factors contributing to CSI compliance gaps. These factors include the effectiveness of ISSM training, the adequacy of shore-based support structures,

and mechanisms for knowledge transfer between ships. The persistent nature of Navy cybersecurity compliance challenges and the operational costs of manual processes justify continued investment in framework development, testing, and fleet integration. Each research effort helps improve and sustain fleet cyber readiness through scalable, sustainable automation that respects operational realities.

Acknowledgements

The authors wish to thank cybersecurity subject matter experts at the Naval Information Warfare Center Pacific for their valuable operational insights and technical validation of the framework architecture. Special appreciation goes to the CANES program representatives for their expertise on shipboard IT infrastructure and operational constraints.

Ethics Declaration: Ethical clearance was not required for this research.

AI Declaration: The authors used Anthropic's Claude Sonnet 4 to aid in developing technical specifications during the framework design phase. The tool helped develop database schemas, generate pseudocode for parsing and compliance algorithms, and convert conceptual requirements into detailed technical specifications. All specifications were validated against Defense Information Systems Agency STIG documentation, Navy cybersecurity policies, and DoD security standards. Cybersecurity subject matter experts from Naval Information Warfare Center Pacific reviewed the technical approach for feasibility and operational suitability. All research methodology, gap analysis, requirements definition, and evaluation of existing tools represent original analytical work, with AI serving only as a supporting tool to translate our analyses into technical specifications, rather than as a primary source of content.

References

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S. and Michaloliakos, M. (2022) "Cybersecurity Challenges in the Maritime Sector", Network, Vol 2, No. 1, pp 123–138.

Commander, U.S. Fleet Cyber Command (2023) OPERATION NEPTUNE IRONCLAD, Naval Message, 141215Z APR 23.

Defense Information Systems Agency (2025) Control Correlation Identifier (CCI) List, [online], https://public.cyber.mil/stigs/cci/

Department of Defense Chief Information Officer (2022) DoD Zero Trust Strategy.

Department of Defense Chief Information Officer (2025) Platform One Iron Bank Repository, DoD Enterprise DevSecOps, [online], https://p1.dso.mil/ironbank

Department of the Navy (1990) United States Navy Regulations, SECNAV M-5210.1, Washington, DC.

Fleet Cyber Command, Navy Space Command, Joint Force Headquarters – Cyber (Navy) (2024) CSI Planning Guide, Washington, DC.

Ireland, D. (2023) RMF Tool Automation Training, NAVSEA RMF Intelink, May.

Joint Force HQ-DoDIN (2020) Joint Force HQ-DoDIN Task Order 20-0020: Assured Compliance Assessment Solution (ACAS) Operational Guidance.

Joint Task Force Transformation Initiative (2018) Risk management framework for information systems and organizations: a system life cycle approach for security and privacy, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-37r2.

Microsoft (2025a) Desired State Configuration (DSC) Overview, [online], https://learn.microsoft.com/en-us/powershell/scripting/dsc/overview

Microsoft (2025b) Microsoft GitHub PowerStig, [online], https://github.com/microsoft/PowerStig

Naval Information Warfare Systems Command (2024) Get Real, Get Better Integrated Cyber Defense Artifacts.

Naval Sea Systems Command (2020) NSWC Crane employee creates software automation tool that improves efficiency, [online], https://www.navsea.navy.mil/Media/News/Article-View/Article/2267419/

Office of Compliance and Assessment, U.S. Fleet Cyber Command (2024) OCA CSI Waterfront Brief, Washington, DC.

PostgreSQL Global Development Group (2025) PostgreSQL 14 Documentation: Chapter 19. Server Setup and Operation, [online], https://www.postgresql.org/docs/14/runtime.html

Pseftelis, T. and Chondrokoukis, G. (2021) "A Study about the Role of the Human Factor in Maritime Cybersecurity", Spoud. J. Econ. Bus., Vol 71, No. 1–2, pp 55–72.

Seferagić, A., Haxhibeqiri, J., Pilozzi, P. and Hoebeke, J. (2021) "Multimodal Network Architecture for Shared Situational Awareness amongst Vessels", Sensors, Vol 21, No. 19, p 6556.

SteelCloud (2025) ConfigOS Automates STIG and CIS Compliance, [online], https://www.steelcloud.com/configos-cybersecurity/

U.S. Department of Defense (2024) DoD Enterprise DevSecOps Fundamentals, ver. 2.5.

U.S. Navy (2018) U.S. Navy Cybersecurity Program, OPNAVINST 5239.1D, 18 July.

Yang, H., Zhu, J. and Li, J. (2024) "Cybersecurity and Risk Prediction Based on Machine Learning Algorithms", Appl. Math. Nonlinear Sci., Vol 9, No. 1.