NavigateCyber and Risk Management Framework (RMF)

Executive Summary

There is a need for reliable and trustworthy RMF automation technologies that can enhance the efficiency and effectiveness of critical technical and business cybersecurity compliance operations. Automation of cyber compliance would transform manual cyber compliance processes into automated operations. Implementing automated cyber compliance software within federal agencies would optimize limited labor hours and dollars, providing capabilities to the agencies. Cyber compliance software will not only conduct repetitive tasks but can incorporate machine learning that would enable intelligent automation at scale.

Navigate Cyber is an AI-enabled automated software platform developed by AiComply that realizes an efficient RMF project management tool that automates the RMF process steps and decreases the time and cost required to achieve compliance and re-certification. Navigate Cyber is a cost-competitive service offering that enables organizations to achieve cybersecurity compliance and approvals in record time. It is a cloud-based, automated analytical tool that delivers cybersecurity adherence. Navigate Cyber enables faster Authority to Operate (ATO) compliance, certification, and continuous cyber readiness. aiComply's Navigate Cyber offering integrates with existing processes, procedures, and tools already used by the DoD, such as eMASS, magnifying their power. Navigate Cyber supports content development for eMASS verification artifacts, such as the System Security Plan (SSP), Continuity of Operations Plan, and other compliance documentation. Navigate Cyber does not aim to re-create the wheel and replace eMASS as the cybersecurity content management tool for all the DoD's Information Systems. Instead, Navigate Cyber augments and enhances eMASS by delivering consistent, error-free artifacts for ingestion and dissemination.

Overview

NavigateCyber is a Generative artificial intelligence (AI)-enabled automated platform that realizes an efficient RMF project management and decreases the time and cost required to achieve compliance and re-certification. NavigateCyber's Intelligent Automation capability will be able to process Tactics, Techniques and Procedures that describe the current threat landscape, hardware and software configuration, and control information from prior packages to realize automated security control prioritization and inheritance. It is an automated analytical tool that delivers cybersecurity adherence on-premises or in the cloud. NavigateCyber enables faster ATO compliance, certification, and continuous cyber readiness thoroughly through human and AI teaming. NavigateCyber uses machine learning to realize intelligent automation of cybersecurity compliance workflows developed by our RMF subject matter experts. Intelligent Automation represents a suite of technologies that would transform manual processes in preparing ATO packages into automated operations at scale and optimize limited labor hours and dollars. This approach will provide DHA with metrics that provide insights into both platforms' cost efficiency and effectiveness and will help agencies make an informed decision on deploying NavigateCyber for enhanced productivity. Intelligent Automation is recommended to deliver these results in a net-zero footprint. Net-zero, meaning cost efficiencies and process effectiveness, are used to save labor hours and dollars to pay for the ATO projects. NavigateCyber's Command Center is interoperable with popular identity management, vulnerability scanning, auditing tools, data sources, and connectors to ingest policy documents. The Command Center provides visibility into the entire ATO process for all packages across units and improves efficiency in processing the ATO packages.

Impacts of the Proposed Solution

- Conduct issue and risk management and remediation of cybersecurity vulnerabilities with automated plans of action and milestones that are easy to understand and transferable to similar systems.
- Interoperable with identity management, domain controller, vulnerability scanning, and auditing tools.

- Modular and flexible to adapt to the agency's process.
- RMF Command Center is a dynamic dashboard that allows stakeholders to track the status of all outstanding packages and packages up for recertification and identify bottlenecks to processing existing packages.
- Aid the agencies in improving processes to ensure device and associated systems cyber hardening. Provides automated recommendations for state-of-the-art remedial measures.
- Generates and downloads preformatted risk management reports for compliance, eliminating the current service-oriented model of manually generating reports, which can be error-prone.
- Agencies no longer depend on human input for organizational processes and system operations. This automation reduces errors, speeds up compliance and certification, and ensures continuous cyber readiness.
- Navigate through the challenges of cyber readiness, compliance, and certification.
- Aid in achieving faster compliance faster and staying compliant.

Impacted RMF Steps

1. **Automated Preparation**: We have developed an automation engine that can extract information about organization policies and procedures, software BOM, hardware BOM, and network topology that will be needed for subsequent steps.
2. **Automated Categorization**: We leveraged popular inventory management tools to gather information related to computing devices, software, and networking resources, which will include enumeration, location, and interconnectivity information. We developed AI techniques that provide a comprehensive and holistic view of all the assets in the organization, security boundaries, and interconnection.
3. **Automated Control Selection**: We have developed AI algorithms to analyze the organization's document artifacts, policies, and procedures and automatically select the

desired security controls for every package. This approach reduces the reliance on humans to provide input on their organization's processes and system operation.

4. **Automated Implementing Controls**: We developed large language models (LLMs) that would provide a guidebook on implementing the controls in the infrastructure for compliance. The LLM model is trained on the organization's policies, procedures, and system information and will balance the tradeoff between efficiency and speed. In addition, the LLM model can provide specific configuration changes that need to be made to services to ensure the controls will be implemented accurately.

5. **Automated Assess Controls**: We have developed AI algorithms that correlate the scan results with the control expectation. Based on the assessment provided by our AI algorithms, we automatically label the control as compliant or non-compliant. We developed AI-based validators to ensure all resources are configured according to the compliance requirement. We created AI techniques to quantify and classify the risks and provide the relevant information needed for POA&Ms.

6. **Automated Monitor Controls**: We execute the AI model to ensure that all controls remain validated periodically to identify any delta change in the inventory. We developed AI techniques that ensure we only target control selection on the upgraded infrastructure. We will incorporate an AI-based anomaly detection technique to monitor for any drift in controls' behavior automatically.