2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

May 20, 2025

Re: Software Fast Track (SWFT) - Automation & Artificial Intelligence (AI)

To: Ms. Leanne Condren

Electronic Delivery: whs.mc-alex.ad.mbx.eosd-psb-branch-mailbox@mail.mil and leanne.m.condren.civ@mail.mil.

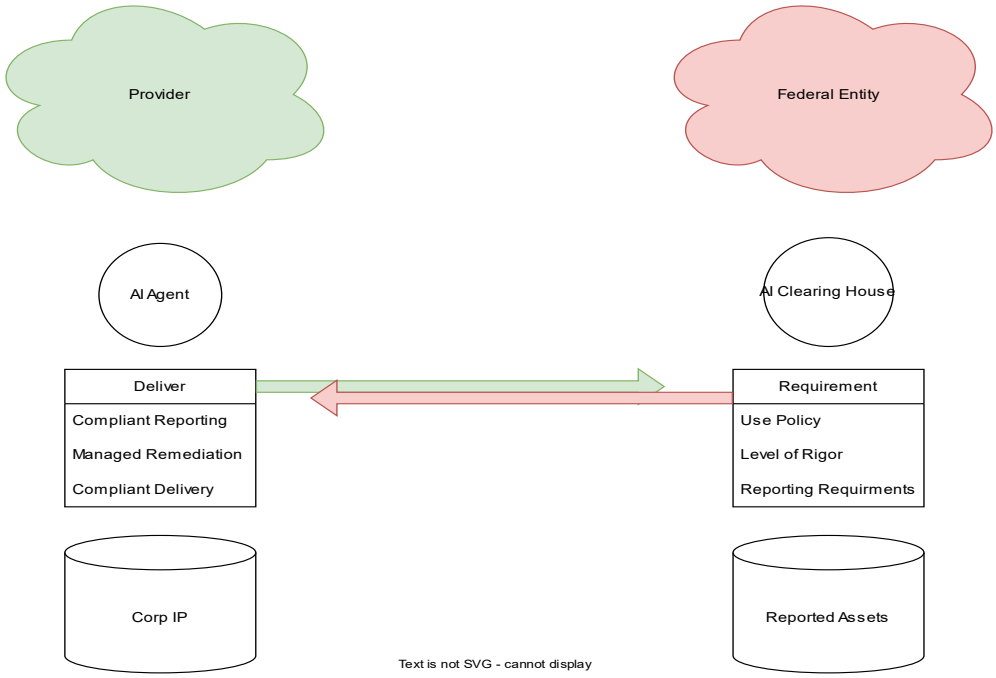
- **Name:** National Defense Industrial Association (NDIA), Michael Seeds (mseeds@NDIA.org)
- **Capability Statement:** NDIA is the nation's largest defense industry association, representing more than 1,700 corporate and over 65,000 individual members from small, medium, and large contractors, a majority of which are small businesses. Our members engage daily with the federal government's national and homeland security apparatuses. They are well-versed in the array of cybersecurity requirements and implementation challenges.

Requested Information for Software Fast Track (SWFT) Automation & Artificial Intelligence (AI)

1. **What are the possible ways that automation or AI could assist to streamline DoD-led SWFT risk assessments under the DoD defined Risk Management Framework (RMF)?**

The integration of AI-driven vulnerability analysis with system modeling enables the execution of "what if" scenarios, providing valuable insights into the potential impact of vulnerabilities on system performance and mission capabilities. By leveraging Multi-Agent Reinforcement Learning (MARL) frameworks, vulnerability scoring can be enhanced to prioritize vulnerabilities and identify potential attack vectors and sequences. By harnessing the power of AI and MARL, organizations can proactively protect their systems and assets, ensuring the success of their missions and capabilities.

NDIA recommends that the government establish a Client/Server-like model of an AI solution, which segregates actions between the provider and the consumer. In a notional implementation, the client-side AI engine is responsible for processing the analysis of data based on requirements from the consumer and delivering results in a secure manner. The server-side AI engine manages compliance of results for reporting without exposing sensitive data. Facilities exist for managing requirements, levels of compliance, and rigor that are dynamic to the provider with minimal overhead.



2. **What are potential challenges in the implementation of automation or AI for high trust situations related to cybersecurity authorization official responsibilities?**

The collection, processing, and storage of software security datasets pose significant challenges due to their complexity and sheer volume. The lack of standardization in software identifiers, such as Common Product Enumeration (CPE), PURL, and SWID, further complicates the process of entity resolution. This makes it difficult to accurately identify and manage software vulnerabilities, patches, and versions.

Several machine learning approaches are not without limitations, including high false positive rates, which can lead to significant time consumption and varied results. By continuing to advance the state-of-the-art in AI-powered software security analysis, it is possible to develop more effective and efficient solutions for managing software vulnerabilities and ensuring the security of complex systems.

3. **What are the data needs for these SWFT automation and AI capabilities, including supplier SBOM, DoD, or third-party sources?**

Key frameworks, standards, and sources include:

- **NIST 800-53**: Provides guidelines for security and privacy controls
- **CNSSI 1253**: Offers a framework for security and privacy controls in the context of national security systems
- **NIST 800-160**: Focuses on systems security engineering
- **CAPEC**: Provides a framework for understanding common attack patterns
- **NVD**: Offers vulnerability information, but has limitations in tracking threat intelligence and exploitation

- **MITRE's ATT&CK & D3FEND**: Frameworks for understanding adversary tactics, techniques, and procedures (TTPs) and defensive strategies
- **CISA**: For threat intelligence and risk assessments
- **Open and commercial sources**: To provide a comprehensive view of the threat landscape
- **OSV, Grype, GitHub, and vendors**: For datasets that add value to understanding risk and potential mitigations for software packages

4. **What are the considerations that DoD should prioritize when evaluating automation and AI solutions for DoD-led SWFT risk assessments and determinations?**

When assessing the effectiveness of a model, it is essential to consider multiple factors beyond accuracy. To ensure responsible results, define the problem or question the model may be utilized for to obtain results. Consideration should be given to the datasets and the algorithm. Develop and evaluate multiple solutions in parallel to determine the most effective approach, weighing the pros and cons of each option to inform the selection of the best solution.