NDIA

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) Tools RFI

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 oldest and 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) Tools

1. **What specific references or industry standards does your organization leverage when considering secure software development and software supply chain threats and vulnerabilities to a company and its software products?**

To ensure the security and integrity of software development, various frameworks and tools are utilized, including NIST 800-53-based frameworks, Secure Software Development Framework (SSDF), and Security Technical Implementation Guides (STIG). Automation plays a crucial role in evaluating source code repositories against the SSDF, and templated Continuous Integration/Continuous Deployment (CI/CD) pipelines are used to automate tooling such as Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). Additionally, Software Bill of Materials (SBOMs) are established as a requirement for software produced, and open-source tooling is used to manage SBOMs and reduce supply chain risk.

Additionally, AAMI SW96, AAMI TIR57, and interaction with ISO 14971 safety risk management, SAE/ISO 21434, NIST SP 800-218 SSDF, NIST SP 800-161 (SCRM), ISO 20243 (OTTP-S), IEC 62304, IEC 81001-5-1, and UNECE Cyber Resiliency Act, UNECE WP.29 R155.

2. **SWFT may assess how a company implements secure software development as identified in the NIST Special Publication (SP) 800-218. Are there obstacles in implementing this guidance and producing an attestation to your implementation?**

Automated generation of standardized NIST 800-218 deliverables, similar to those required for NIST 800-53 compliance, could streamline the process. By using automated assembly of objective evidence for software assurance, evaluations and verification can be performed more efficiently. Approaches like

Supply-chain Levels for Software Artifacts (SLSA) compliance, which utilize metadata to attest to software artifacts, can enable automated build processes and enhance software security.

3. **For commercial software products does your company provide a Software Bill of Materials (SBOM) that includes software component (artifact) level of details? If not, what obstacles exist? If yes, what tools support this process?**

The software industry has made strides over recent years in its capability to produce SBOMs. However, it is important to note that there is no one tool to accomplish this in a company that has a broad range of offerings, development processes, and market requirements. A structured software factory CI/CD pipeline can automate the generation of Software Bill of Materials (SBOMs) for delivered software using various open-source tools, such as Syft for container images. Collaboration and open-source tools like Hoppr are essential. Hoppr provides a uniform SBOM for legacy and new software products, aggregates data from multiple suppliers, and integrates dependency trees from open-source projects. It also supports vulnerability, license, and risk assessment data augmentation, simplifying automated risk assessment. By leveraging the industry-standard CycloneDX format, Hoppr enables teams to represent the entire software supply chain as code.

4. **What artifacts does your organization produce to perform risk assessments of software? Does your organization use automated tools to produce these artifacts?**

Both automated tools and manual assessments are performed, as there are no tools in industry that can meet the needs of a broad, multi-product organization. Risk assessment is critical for operational capability, and capabilities for risk assessment require collaboration with open-source partners and leveraging industry and commercial scanning capabilities. A set of Assessment and Authorization (A&A) artifacts, including reports such as SCAP, SCTM, POA&M, SAER, SBOM, and executed STIGs, provide a detailed record of software security posture and compliance status. Tools such as vulnerability scanning, SAST, DAST, STIGs/SRG, SCAP, and Secrets scanning to ensure cyber resiliency of software deliverables are favorable. Vulnerability reports are generated using CycloneDX SBOM, and vulnerability identifications are resolved against various types, including CVE, RHSA, GHSA, OSV, and others.

The open-source MITRE SAF Heimdall2 dashboard serves as a centralized platform for analyzing and visualizing cyber risk posture, leveraging the comprehensive set of artifacts generated by the CI/CD pipeline. AI-generated vulnerability threat scores can predict the risk by providing a list of data sources reporting exploits and threat intelligence. Reporting can be automated with vendor and version details, and mitigations for every known vulnerability.

5. **Would these software risk assessment artifacts be sharable with the DoD to enable consistent and secure DoD-led risk assessments? If not, what are your recommendations for the artifacts DoD should require to equip authorization officials with adequate risk information?**

Automation facilitates inform decision-making by collecting, condensing, and organizing content into a dataset associated with specific compliance requirements. The Heimdall2 dashboard displays the measurement of risk related to test content and provides a mapping of all test content to relevant RMF controls, offering direct visibility into software compliance. Test evidence is converted into the Open Heimdall Data Format (OHDF), a JSON-based schema that enables seamless data exchange and review across different boundaries and deployments of Heimdall2.

A report showing compliance with requirements could be provided and would be dependent on what information is required and what level of detail is requested. Sensitive information should be maintained by the software provided and not shared with the DoD.

NDIA recommends that DoD provide a detailed list of metadata that should be collected and the criteria for assessment compliance. This data would be collected and maintained by the software provider. Organizations should then be offered the opportunity to be self-attested through a certification process or engage a third party. Any notification should be handled through standard SIRT activities.

6. **How could your organization support secure and automated information sharing that accelerate rigorous software security verification processes?**

Automating the sharing of critical software risk assessment artifacts through digital delivery pathways reduces manual data transfer and validation time. Exportable reports and artifacts are designed to be easily integrated and analyzed by external partners and stakeholders, enabling informed decisions about software security and risk. The use of OHDF allows assessments to be easily packaged and viewed in other disconnected Heimdall2 instances, streamlining the approach and ensuring stakeholders have access to up-to-date information.