# SOFTWARE FAST TRACK

## Request for Information Combined Summary

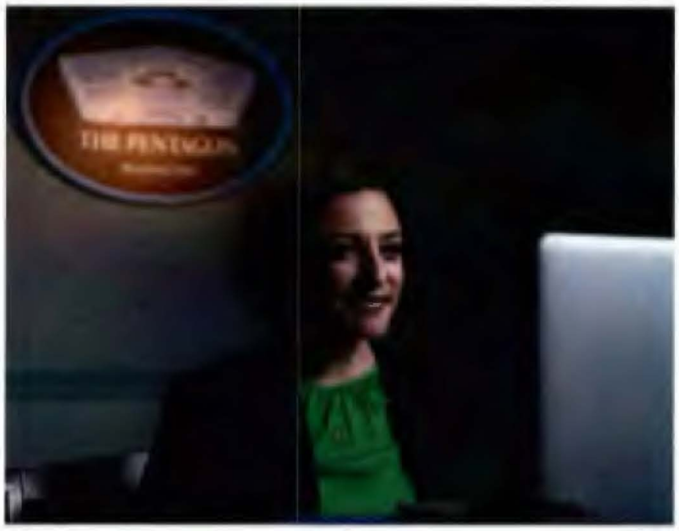
The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense (DoD) of the linked websites, or the information, products or services contained therein. The DoD does not exercise any editorial, security, or other control over the information you may find at these locations.

*Disclaimer: The SWFT RFI Combined Summary was partially assisted by generative artificial intelligence capabilities with human-in-the-loop analysis and tailoring for all inputs and output.*

# FOREWORD

On April 24, 2025, I signed a memo titled "Accelerating Secure Software," which establishes the Software Fast Track (SWFT) Initiative for the Department of War (DoW). The SWFT initiative is aligned with Secretary Hegseth's guidance (Directing Modern Software Acquisition to Maximize Lethality, March 6, 2025) and will reform the way the Department acquires, tests, and authorizes secure software.

Current systems for software procurement have not kept pace with the quickly evolving threat environment and rely on processes that are outdated and slow, with little to no supply chain visibility. The SWFT Initiative will address these challenges and improve our ability to rapidly bring cutting edge, secure software to the Warfighter, greatly increasing the lethality and resilience of the Joint Force.



***Katherine Arrington briefs the Norwegian National Defense and Security Industries Association. Washington, D.C., Jan. 13, 2021. (DoW photo by Air Force Staff Sgt. Brittany A. Chase)***

As part of the SWFT Initiative, we issued three Requests for Information (RFI) to better understand the capabilities that could accelerate secure software delivery to the federal government. We received more than 400 responses to the RFIs, and I'd like to thank you all for your thoughtful contributions. Your input is critical to understanding how the Department can transform software security through risk-based decision making when introducing new capabilities to the DoW and putting the nation on a glide path to maintaining our battlefield dominance well into the future.

Katherine Arrington
Performing the Duties of the
Chief Information Officer of the
Department of War

# EXECUTIVE SUMMARY

This document integrates analysis of 420 private sector responses to the three RFIs issued on SAM.GOV (see Appendix II) to gather market information and capabilities in accelerating secure software delivery to the federal government in three focus areas:

- What software supply chain security tools are developed and in use;
- How external assessment methodologies and organizations can support streamlining risk assessment and authorization processes for software-enabled products and services; and
- How automation and artificial intelligence (AI) can support the government's objective to accelerate secure software adoption.

The first RFI, exploring SWFT tools, highlights a strong industry consensus around established security frameworks and standards. Industry participants overwhelmingly reference National Institute of Standards and Technology (NIST) special publication (SP) 800-218[1] for secure software development, NIST SP 800-53[2] for cybersecurity controls, and NIST SP 800-161[3] for cybersecurity supply chain risk management practices. Significant reference was also given to Open Worldwide Application Security Project (OWASP) guidelines[4]. Despite this broad alignment, respondents expressed concern over the lack of consistent and standardized methods for attestation processes. Organizations noted that while many adhere to these frameworks at a technical level, the absence of precise, universally accepted guidelines for documenting compliance creates challenges when integrating these standards into existing workflows. Additional hurdles such as resource constraints, difficulties managing supply chain opacity, and cultural barriers further underscore the intricacies of enforcing a robust secure software development practice. Another notable finding was the overwhelming willingness of companies to provide Software Bills of Materials (SBOM) and artifacts, although variations in self-referential versus third-party reporting were observed. Responses for artifacts were aligned with the

[1] NIST SP 800-218: Secure Software Development Framework (SSDF) Versions 1.1: Recommendations for Mitigating the Risks of Software Vulnerabilities, February 2022 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

[2] NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, September 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[3] NIST SP 800-161r1-upd1, May 2022 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf

[4] The Open Worldwide Application Security Project (OWASP) materials, https://owasp.org/

core artifacts of the risk management framework (RMF)[5]: Security Assessment Report, System Security Plan, Risk Assessment Report, and Plan of Actions and Milestones (POA&M). However, there were additional artifacts offered to continuously monitor software suppliers or for providing attestations. Almost all artifact discussions noted the importance of automated artifacts generation and their willingness to provide these artifacts in an efficient manner through standardized formats and secure exchange processes.

In the second RFI, focusing on SWFT external assessment methodologies, industry respondents detailed their current audit capabilities and methodologies for evaluating software security. The responses revealed that half of the organizations maintain both internal and external audit functions. Internal audits identify common approaches such as continuous monitoring, code reviews, and regular penetration testing, or red-teaming exercises establish a proactive stance for some aspects of secure software development. External audits for impartial validation were described as typically being carried out by third-party auditors or through independent penetration testing engagements. The correlation of these audits with broader compliance regimes including frameworks such as: Federal Risk and Authorization Management Program (FedRAMP)[6], NIST standards, Service Organization Control (SOC) 2, and International Organization for Standardization (ISO) 27001[7], further evidences a mature security posture among organizations. Respondents emphasized that any external assessment functions would require not only well-defined organizational methodologies, relevant experience, and high degree of independence, but also secure data handling methodologies and established quality management. They further identified qualified personnel as a necessity to ensure assessments appropriately evaluate software operating in warfighter environments with high impact. Personnel qualifications include industry-recognized certifications and a thorough understanding of DoW security frameworks.

The third RFI centered on the role of automation and AI within the SWFT ecosystem. Here, industry insights point to a dual opportunity: the potential to streamline and enhance the efficiency of risk assessments while simultaneously addressing novel challenges to be overcome. Respondents noted that automation and AI can significantly reduce manual efforts in repetitive tasks ranging from document processing, data analysis, compliance control validation, monitoring, prediction modeling, and impact assessments, thus accelerating the overall risk evaluation process and cybersecurity authorization process. The discussion also underscored inherent challenges accompanying these technologies, such as AI explainability,

[5] DoD Cybersecurity Reciprocity Playbook, May 2024 https://dodcio.defense.gov/Portals/0/Documents/Library/(U)%202024-01-02%20DoD%20Cybersecurity%20Reciprocity%20Playbook.pdf

[6] FedRAMP, https://www.fedramp.gov/

[7] ISO 27001, October 2022 https://www.iso.org/standard/27001

data quality management, model performance and reliability, data security, automation lifecycle protection, human factors, and scalability. Automation and AI capabilities may require standardized data, defined for DoW needs, that leverages threat intelligence feeds and vulnerability databases. Additional data was suggested for monitoring configuration baselines, software development artifacts, software composition, and maintaining training data that could be informed by historical data. Specific to software products, SBOM data assists with identifying disclosed vulnerabilities. Open-Source Software (OSS) security metrics could assist tracking the cybersecurity of these components.

## CONTENTS

# INTRODUCTION

Each of the following sections address one of the three SWFT Initiative RFIs. Each section is separated into the questions asked in the respective RFI, followed by a summary of the main points from the responses. This document summarizes responses stated in the majority or through notable aspects and does not represent an endorsement of the responses provided nor dictate what a SWFT implementation plan will encompass. Nonetheless, the industry responses are informative for consensus among current opinions. Some of the consensus opinions may be incorrect for SWFT Initiative requirements, in which case the Department will need to advocate to industry for those requirements.

# SWFT TOOLS RFI

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

The following documents and sources were identified as industry standards when considering secure software development and software supply chain threat and vulnerabilities.

| | | |
|---|---|---|
| **NIST SP 800-218** | Secure Software Development Framework (SSDF): Recommendations for Mitigating the Risk of Software Vulnerabilities | 75% |
| **OWASP** | Aggregate OWASP significant references (Top 10, SAMM, ASVS, SCVS) | 66% |
| **NIST SP 800-53** | Security and Privacy Controls for Information Systems and Organizations | 60% |
| **NIST SP 800-161** | Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations | 46% |
| **ISO/IEC 27001** | Information security management systems — Requirements | 44% |
| **OpenSSF SLSA** | Supply-chain Levels for Software Artifacts (SLSA) | 30% |

The NIST SP 800-218 for the SSDF was the dominant single reference represented in over 75% of the responses. In aggregate, significant references to OWASP materials were in 66% of the responses; OWASP responses included the OWASP

Top 10, Software Assurance Maturity Model (SAMM), Application Security Verification Standard (ASVS), Software Component Verification Standard (SCVS).

There was a wide acknowledgement of NIST as a voice in establishing standards across the community. A SWFT solution that utilizes NIST SP 800-161 for cybersecurity supply chain risk management (C-SCRM), NIST SP 800-218 for secure software development, and NIST SP 800-53 for cybersecurity controls appears to align with existing industry frameworks. This correlates with existing DoW guidance pertaining to the use of NIST RMF. There were also industry and international led references to OpenSSF SLSA and ISO 27001 that could contribute to common industry standards; these require alignment with DoW policy and guidance.

## QUESTION 2: SWFT may assess how a company implements secure software development as identified in NIST 800-218. Are there obstacles in implementing this guidance and producing an attestation to your implementation?

Due to the qualitative nature of the question, data was summarized qualitatively. With respect to obstacles in implementing the SSDF, there was a mixture of responses between those that referred to specific, company experience and those that perceived obstacles for industry at large. The responses that were self-referential to their own experience were considered more significant for identifying obstacles.

- **Standardization of Attestations and Requirements:** A number of replies cited concerns with: lack of standardization for attestation to NIST SP 800-218 compliance, what qualifies as a valid attestation, what documentation and evidence is required in a body of evidence (BoE), how often or continuous an attestation is required, and that requirements may not be consistent across the government. A notable theme was that respondents were unclear on whether vendors would be able to self-attest to compliance, or if they would need to work with a third-party assessment organization. Respondents noted possible complexity in the process for collecting, consolidating, structuring, and presenting evidence for attestation. Furthermore, processes that cannot be automated could result in significant effort to support SWFT. Overall, there was a strong call for the DoW to define a legitimate attestation, identify what is required to complete an attestation, and to ensure consistency of these standards across the DoW. Many respondents indicated that the NIST SP 800-218 is only a framework, and while it maps to actionable controls in various other standards it does not prescribe an exact control set and requirements to implement. As a result, there is concern that 'compliance' with NIST SP 800-218 on a technical level is open to degrees of interpretation. Alongside needing specific requirements for compliance attestation, many would benefit from concrete control requirements aligned with the SSDF to define compliance.

- **Integrations:** The second most common obstacle noted was difficulties associated with integrating SSDF into existing toolchains and workflows. The amount of evidence required for NIST SP 800-218 compliance would likely require automation and integration of multiple tools within existing infrastructure. Similarly integrating manual documentation and effort into existing logical processes and workflows could be challenging. Some respondents noted that they have diverse environments which require them to identify and tune many different solutions at once. Respondents also noted they have legacy environments or other technical debt that would further challenge integration with the tooling required to implement a NIST SP 800-218 framework.

- **Resource Requirements and Constraints:** A common obstacle mentioned was the number of resources required to implement a NIST SP 200-218 framework, including:
    - Tools for automation
    - Time for documentation and attestation
    - Training for technical skill requirements
    - Potential third-party assessments for attestation

  Some respondents simply indicated this obstacle would present difficulties that would need to be overcome, while others warned the constraints might be prohibitive towards smaller businesses and drive them out of selling software to the Department.

- **Supply Chain Opacity and Complexity:** Respondents identified complexity and difficulty in addressing their third-party software component providers. Many noted that they have challenges with their own suppliers passing complete and consistent information and thus would be challenged to attest to their software supply chain. Recovering this information through software composition analysis can be inconsistent and inaccurate.

- **Unique Technology Models:** A category that emerged from seemingly disparate responses, almost exclusively self-referential in nature, was the obstacle presented to respondents who consider themselves “outliers” from standard software development. A handful of companies related to AI, firmware, Platform-as-a-Service, and Software-as-a-Service voiced concerns that NIST SP 800-218 was not designed with their models in mind; resultant SSDF requirements would not be compatible with their models or areas of focus. This assumption of the noted technologies being different from software development

and SSDF could only be a perception as there is not much detail to substantiate it.

- **Cultural Barriers and Training:** A common theme noted primarily in third-party reference was challenges with a company adopting a security-first mindset across all development teams. Whether this is only an assumed issue or because respondents were hesitant to address self-referential cultural barriers is unclear. The claimed obstacle is that staff required to comply with NIST SP 800-218 (generally development level staff or project managers) do not see the value in secure software development or view delivery timelines as more significant and may be resistant to implementing the SSDF. A handful of responses noted a need for corporate governance that would be required to galvanize such cultural changes. There was also a claimed obstacle that organizations lack sufficiently trained personnel for implementing or attesting to NIST SP 800-218 compliance.

## QUESTION 3: For commercial software products does your company provide a software bill of materials that includes software component (artifact) level of details? If not, what obstacles exist? If yes, what tools support this process?

Ninety percent of companies responded they would provide an SBOM to the Department. Within these responses were mixed answers on whether they would provide the SBOM for their own software versus they would provide an SBOM as a third-party for other software. This mixture appears to have been caused by how the RFI question was stated. Utilizing the distinction explained in Section 1.2 for “self-referential” responses about providing SBOMs for their own software, a subset analysis of the ninety percent majority for providing SBOMs showed that sixty-eight percent were self-referential about their own SBOMs, twenty-two percent were for third-party SBOMs, and ten percent were ambiguous about SBOM source. This examination indicates a sustained, significant majority response that suppliers would provide an SBOM, and it would be for their own software.

For the ten percent minority of responses that do not or would not provide an SBOM, there were multiple reasons indicated: inherent aspects of their solution, challenges they perceive cannot be overcome, or apathy about the need for an SBOM. There were some perceived inherent challenges with SBOMs related to software composition analysis, standardization across industry, operational security related to revealing software composition, and overall effort to incorporate the SBOM capability into development.

One respondent believes the important aspect of supply chain risk management is managing the supply chain risk versus passing SBOM information. A few responses indicated challenges with being able to track and manage complex and rapidly changing software composition, especially in DevSecOps or cloud environments; however, one response stated that this can be overcome with automation to generate the content. Other responses suggested that in-lieu of SBOM exchange their platform’s cloud capabilities outside of their system scope could be used to provide an SBOM.

## QUESTION 4: What artifacts do your organization produce to perform risk assessment of software? Does your organization use automated tools to produce these artifacts?

Ninety-six percent of companies responded that they perform software risk assessments and would provide risk assessment artifacts to DoW. There was ambiguity in many of the responses as to the use of automated tools to produce artifacts, either due to non-response or generic responses indicating a combination of automated and manual methods. Of responses that clearly stated the use of automated tools or manual processes, ninety-one percent of the artifacts were generated through automated means.

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

As described above, ninety-six percent of the companies responded that they would provide risk assessment artifacts to the DoW. The responses included a diverse set of nomenclature for artifact titles; direct quotes would have made summarizing the findings difficult. Risk assessment artifacts were instead categorized under the DoW CIO directed BoE artifacts defined in the Cybersecurity Reciprocity Playbook which is also defined in Annex C of Committee on National Security Systems Instruction (CNSSI) 1254. The BoE artifacts include the System Security plan (SSP), Security Assessment Report (SAR), Risk Assessment Report (RAR), and POA&Ms.

The following artifact category percentages were identified. Sub-types identified for artifacts are identified in parentheses:

- SAR – Ninety-eight percent (Vulnerability, Licensing, Quality, Incident Response, Compliance, Controls, Foreign, Configuration, SCAP, VEX)
- SSP – Forty-five percent (Training, Architecture, Assessment Plan, Threats)
- RAR – Thirty-eight percent
- POA&M – Twenty-two percent

Two additional groupings of artifacts were offered: Monitoring and Attestation. Thirty-two percent of the responses offered monitoring, which included reports and information reporting that would provide continuous monitoring of risk assessment artifact content. Twenty-one percent offered attestation, which included providing an attestation artifact for evaluated suppliers.

## QUESTION 6: How could your organization support secure and automated information sharing that accelerates rigorous software security verification processes?

- **Automated Artifact Generation:** Organizations could automate the generation of artifacts as part of their pipelines by using automated or AI tools for security scanning and tasks. They could continue generating artifacts after build time through continuous monitoring tools that assess software states in live scenarios or against evolving data feeds.

- **Standardized Formats:** Data exchange between the organization and the DoW would need to occur over agreed upon standardized formats. SBOMs, for example, can be described in different formats but will require specific tools to parse or generate content for the specific formats. Clear and consistent standards improve risk identification by allowing for more fine-grained validation and by allowing organizations to meet all formatting requirements.

- **Secure Exchange Processes:** There is a need for agreed upon formalized secure exchange processes which would capture:
  - **Exchange Channel Security:** Access controls such as role-based access control and multi-factor authentication requirements. Encryption requirements would also be needed for the data transfer.
  - **Data Exchange Security:** Requirements for authenticity, tracking, and non-repudiation controls such as hashing, digital signatures, and chain-of-custody records.

- **DoW System Application Programming Interfaces (API):** The best way to transfer artifacts would be over APIs connecting to DoW risk management platforms or Authority to Operate (ATO) systems (e.g., eMASS) or other DoW-controlled collection endpoints. Data in standardized formats could be submitted through these APIs consistent with an agreed-upon exchange process.

## QUESTION 1: Does your organization have an audit function that assesses software security? If yes, is this an internal or external function? Is this function performed as part of a compliance regime? Which ones?

Response categorization provided the following percentages across the internal and external audit function responses.

- Fifty-three percent organizations responded to having both internal and external audit functions
- Fourteen percent organizations have only an external audit function
- Thirty-three percent organizations have only an internal audit function

The primary methods stated for <u>internal audit</u> functions to assess software security are:

- **Continuous Monitoring:** An ongoing process of tracking and analyzing an organization's security posture in real-time, using various tools and techniques to identify potential vulnerabilities and threats. This approach helps organizations stay ahead of emerging threats and ensures that their security controls are effective.

- **Code Reviews:** A critical component of secure software development, where developers review each other's code for security vulnerabilities, bugs, and best practices. This process helps identify potential weaknesses during development to ensure that the final product is secure and reliable.

- **Regular Penetration Testing/Red-Teaming Exercises:** Penetration testing involves simulating cyber-attacks on an organization's systems to identify vulnerabilities and weaknesses. Red-teaming exercises take this a step further by mimicking advanced threat actors using tactics, techniques, and procedures (TTPs) to test an organization's defenses. These exercises help organizations improve their incident response capabilities, detect zero-day exploits, and strengthen their overall cybersecurity posture.

The primary methods stated for <u>external audit</u> functions to assess software security are:

- **Third-Party Auditors:** External experts who conduct independent assessments of an organization's software security, often to verify compliance with regulatory requirements or industry standards. They provide an objective evaluation of the organization's security controls and identify vulnerabilities or areas for improvement.

- **Independent Penetration Testing:** Involves hiring external experts to simulate cyber-attacks on an organization's software systems to test their defenses and identify vulnerabilities. This type of testing helps organizations strengthen their security posture by identifying weaknesses before they can be exploited by malicious actors.

The top compliance regimes include:

- FedRAMP – Forty-two percent
- NIST SP 800-53, NIST 800-218, NIST SP 800-171 – Thirty-one percent
- SOC 2 – Thirty-one percent
- ISO 27001 Information Security Management System (ISMS) – Twenty-nine percent
- DoW Cybersecurity Maturity Model Certification (CMMC) – Twenty-one percent
- OWASP – Seventeen percent
- DoW RMF (DoD Instruction 8510.01) Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) Compliance Requirements – Sixteen percent

## QUESTION 2: What specific organizational and personnel qualifications and requirements do you recommend for accomplishing external assessment functions within the SWFT Initiative?

The primary **organization** qualifications and requirements described in the RFI responses include:

- **Relevant Experience and Proven Track Record:** There should be relevant experience with supply chain risk management, software development, and threat areas such as Defense Counterintelligence and Security Agency (DCSA) or other Foreign Ownership, Control, or Influence (FOCI) considerations. The proven track record should include demonstrated organization experience in

conducting software security assessments for complex systems, preferably within environments with higher security and compliance demands such as defense, finance, and healthcare.

- **Secure Infrastructure and Data Handling capabilities:** Organization capability to securely handle sensitive supplier information, such as source code (if reviewed), SBOMs, vulnerability data, and intellectual property. The organization infrastructure would include secure capabilities such as FedRAMP High IL5 or IL6.

- **Established Quality Management Systems:** Quality management would include documented and repeatable organization processes that ensure consistent assessment methodologies across different systems and assessors. The establishment of a center of excellence and continuous learning programs would ensure sustainment of quality management.

- **Independence and Impartiality:** Strict organization policies and procedures should ensure assessors are free from conflicts of interest with the software suppliers they assess. There should also be organization independent verification and validation of software development through external or structural separation of assessors from solution providers.

- **Defined and Transparent Methodologies:** There should be clearly documented assessment methodologies within the organization that are based on industry best practices and may be tailored to the types of software being assessed. These methodologies should be recognized by federal and/or industry bodies (e.g., FedRAMP, CMMC Accreditation Board (CMMC-AB), American National Standards Institute (ANSI) National Accreditation Board (ANAB), Payment Card Industry Security Standards Council (PCI SSC)).

- **Accreditation/Certification:** Assessment organizations should hold relevant organizational accreditations or certifications demonstrating their competence and adherence to recognized standards.

The primary **personnel** qualifications and requirements described in the RFI responses include:

- **Accreditation/Certification:** Personnel should hold relevant accreditations or certifications demonstrating their competence and adherence to recognized standards. Noted standards were the Certified Secure Software Lifecycle

Professional (CSSLP), Certified Information Systems Security Professional (CISSP), Certified Cloud Security Professional (CCSP), Certified Information Security Manager (CISM), Security+, and Certified Ethical Hacker (CEH).

- **Thorough Understanding of Security Frameworks:** Specific for SWFT DoW needs, assessors should be fluent in applying the NIST RMF, NIST SP 800-53, NIST SP 800-171, NIST SP 800-218, as well as DoW-specific guidance such as the DoW Zero Trust Reference Architecture and the DoW Cloud Computing Security Requirements Guide.

## QUESTION 3: How could SWFT external assessments demonstrate technical expertise, cybersecurity, and supply chain risk management experience that is inclusive of sensitive data protection, impartiality, and independence?

- **Technical Expertise:** Demonstrating technical expertise through verifiable qualifications of assessment personnel, industry-recognized certifications, and state-of-the-art tools for automated assessment.

- **Supply Chain Risk Management**: Ensuring that software components are secure and trustworthy by mapping and verifying supply chains, protecting sensitive information, and monitoring SBOMs

- **Impartiality and Independence:** Ensuring independence and impartiality in external assessments through conflict-free operations, third-party oversight, accreditation, and transparent evaluation criteria.

- **Data Protection:** Implementing robust data protection measures, including encryption, access controls, and secure information-sharing mechanisms, can ensure sensitive information is protected during assessments.

## QUESTION 4: What collaboration would be required among suppliers, external assessments, and DoW and what are your recommendations for secure information sharing mechanisms?

The responses identified requirements and made recommendations in the following categories:

- **Collaboration Tools & Platforms:** Secure portals for artifact exchange, risk information sharing feedback loops, continuous risk monitoring, and mitigation strategies with plans of actions and milestones.

- **Data Sharing:** Procedures to include data sharing agreements, secure data transfer, and standardized machine-readable formats.

- **Data Handling:** Documented procedures for evidence handling that preserve integrity of assessment artifacts and access controls to maintain confidentiality.

## QUESTION 5: How could an external assessment facilitate assessing the SWFT artifacts to include a supplier's software bill of materials and for DoW-led risk assessments, and automated information sharing to accelerate and maintain a rigorous software security verification process?

Recommendations to facilitate assessing the SWFT artifacts to include a supplier's SBOM include:

- **External Assessment and Validation:** External assessments can provide an independent risk evaluation in SWFT artifacts and validate SBOMs for completeness, format compliance, and alignment with standards. External assessors can also verify SBOM accuracy through cross-verification with software binaries and static analysis tools, ensure SBOM integrity via cryptographic signatures, and confirm reliability of artifacts for DoW risk decision-making. By leveraging external assessments and validation, the Department could externally scale its authorization framework for large numbers of suppliers, while maintaining limited government personnel and ensuring the accuracy and reliability of SBOMs.

- **Automated Analysis Tools for Risk Assessment and Scoring:** Automated analysis tools can ingest component inventories, software composition analysis (SCA) reports, and other data sources to enrich SBOM risk identification, while cryptographic validation and metadata enrichment ensure artifact authenticity and completeness. Risk assessments can involve identifying potential

vulnerabilities, threats, and weaknesses in SBOMs, while scoring provides another interpretation of risk likelihood.

Recommendations to facilitate **DoW-led risk assessment** include:

- **Automation and Tools**: External assessors can leverage specialized tools and methodologies to conduct thorough risk assessments and provide detailed reports that highlight security risks, suggested mitigation strategies, and compliance gaps. Automated workflows and control mappings can reduce assessment times. Secure APIs can automatically push assessment findings directly into DoW security information management systems (e.g., eMASS) to facilitate seamless integration.

- **Risk Scoring**: External assessors can generate multi-dimensional risk scores that incorporate exploitability, possible impact, propagation potential, and SCRM posture. These risk scores can highlight potential risks associated with SWFT artifacts and enable informed DoW decision-making.

Recommendations to facilitate automated information sharing to accelerate and maintain a rigorous software security verification processes include:

- **Secure and Validated Ingest:** External assessors can implement secure APIs or blockchain-based systems for traceable and tamper-proof data exchanges, ensuring that sensitive information is protected. Secure APIs can automatically push assessment findings directly into DoW security information management systems (e.g., eMASS), facilitating seamless integration into DoW's approval workflows.

- **Continuous Monitoring and Updates:** Automated information sharing and data updates are important to ensure that risk assessments remain current and accurate over time. Automated tools can generate tailored, continuous risk assessment and provide mitigation recommendations with embedded traceability to findings, vulnerabilities, and assigned remediation workflows. By leveraging continuous monitoring and updates, the DoW can maintain a higher level of confidence in the software supply chain security posture.

## QUESTION 1: What are the possible ways that automate or AI could assist to streamline DoW-led SWFT risk assessments under the DoW defined risk management framework?

This question asked about both “automation” and “AI” implementations. These are separate methods for streamlining processes, though there can be significant overlap. Automation increases workflow efficiency by executing repetitive, predefined tasks based on a set of rules. AI, alternatively, uses robust models trained on data to make decisions and learn to perform tasks with a human-like intelligence. It is important to note that while automation can incorporate AI to handle more complex tasks and decision-making, AI is not always necessary to gain the effectiveness automation has to offer. It was found that many of the responses defaulted to just stating the use of “AI” as the solution for all needs and not acknowledging automation-specific solutions. This appears to be a habit of forward-leaning nomenclature about technology expectations. Nonetheless, many of the solutions the respondents offered could be achieved with either AI or automation (or a combination of both) and the decision to use one over the other ultimately comes down to the task needs.

- **Automation of Risk Assessment:** Respondents emphasized the critical need for automation in risk assessments by developing advanced tools capable of processing and mapping diverse data types, including SBOMs, vulnerability scans, and threat intelligence feeds. Developing highly configurable pipelines to streamline risk identification is necessary to meet multiple use-case requirements. The implementation of such tools can significantly enhance efficiency in identifying security compliance gaps and producing comprehensive risk reports.

- **Vulnerability Identification:** Developing both automated and AI-driven methods of vulnerability identification plays a significant role in risk assessment. The main goals are to detect potential security risk and prioritize remediation efforts which can be achieved through development of a model with the ability to prioritize identified vulnerabilities based on a risk level within the context of a DoW-defined task. By taking the results generated by the vulnerability assessment and automatically feeding them to a model that ranks the risk, stakeholders could quickly take meaningful action to mitigate the most severe vulnerabilities.

- **Document Processing:** Document-related tasks should be streamlined. Automatic document generation of resources like security assessment reports

and code documentation can reduce the burden of tedious, time consuming tasks on humans while also producing documents that are consistently formatted and machine-readable for use in other tools. AI methods like natural language processing and large language models can extract information from documents to more efficiently track and manage requirements, identify risk areas, and perform information retrieval.

- **Automated Data Ingestion and Analysis:** There is a need to develop methods for seamless integration of data from diverse sources, such as software development pipelines, vulnerability scans, SBOMs, and telemetry data. Configurable processing pipelines create an agile environment, limiting the need to continuously develop new solutions. Automation of evidence collection and ingestion into workflows can reduce the burden of human labor by minimizing tedious tasks. Automated data analysis facilitates tracking of evidence and maintaining a documented chain-of-custody.

- **Compliance and Controls Validation:** Coordination across SBOMs, RMF, and NIST SP 800-53 can become complicated and disrupted when large amounts of documentation are received in non-standard formats. AI solutions can enhance this process by extracting and mapping artifacts outlined in a BoE. Correlating information across various data sources (e.g., STIG requirements, common vulnerabilities and exposures (CVEs)) will create a comprehensive compliance assessment. This kind of automation will be facilitated by BoE artifacts that follow machine-readable, standardized formats for ingestion and analysis.

- **Monitoring**: There is a need for automation and AI real-time monitoring to continuously track and analyze various aspects of software security, supply chain, and system configurations. Establishing monitoring systems to continuously perform anomaly detection can help identify potential risks and vulnerabilities before they can cause harm. The data from these systems can be used to generate real-time security alerts or dashboards that automatically update information that assessors, vendors, Authorizing Officials (AOs), and stakeholders can utilize for decision-making.

- **Prediction Modeling:** AI can be utilized to forecast potential threats and vulnerabilities by analyzing historical data, threat intelligence, and real-time security events. This would generate insights that can be used to predict the risk of certain vulnerabilities to a given objective as well as help outline the impact, should they be exploited. Through scenario modeling and impact simulation, the DoW can better prepare for and mitigate future risk. Prediction models can aid in remediation planning by identifying the most effective strategies to address the potential threats, thereby enhancing overall security posture.

- **Mission Impact Assessment:** There are benefits of generating impact analysis. Understanding how software security risks can affect the accomplishment of DoW objectives provides context for AOs to make informed decisions. Automating risk assessments and generating impact reports specific to DoW missions will provide AOs and stakeholders an enterprise view of impact.

- **Authorization Processes:** Automation and AI-driven risk assessments confer secondary benefits These tools can facilitate knowledge transfer by providing AOs with concise security posture summaries and real-time risk scoring and prioritization which enables AOs to make better-informed decisions than with traditional methods. To further improve the process, the creation of configurable approval chains and event-driven notification workflows can automate the dissemination of AO decisions.

## QUESTION 2: What are potential challenges in the implementation of automation of AI or high trust situations related to cybersecurity authorization official responsibilities?

- **AI Explainability:** AI explainability is an important challenge when incorporating AI algorithms into larger systems. There is an essential need for understanding AI in high-stakes environments, emphasizing the importance of transparency in AI logic and decision-making processes to make them comprehensible to the human analyst. Using inherently interpretable models, tooling, and/or algorithms to provide explanations for AI outputs is paramount to building trust and diagnosing undesirable behavior. Transparency promotes understanding among AOs and other stakeholders, enabling them to grasp why specific outcomes were reached. There is a concurrent need to incorporate a human-in-the-loop to maintain accountability and adherence to standards.

- **Data Quality:** Data quality is a challenge when employing AI methods. High-quality data that is accurate and reliable is essential for AI systems to generate trustworthy and effective results. Low-quality data can lead to problems such as inaccurate model outputs, biased decision-making, and reduced trust in the tools. To ensure reliable AI outputs, data must be evaluated for cleanliness, completeness, and biases, with validation and verification processes in place to detect potential errors. Continuous tracking and aggregation of DoW, commercial, and third-party published datasets is essential for maintaining AI model relevance in a constantly evolving environment such as cybersecurity. Failing to incorporate new data in a timely manner can result in model drift that causes degrading model performance over time. There is a lack of standardized,

open source labeled datasets for training models. Dataset curation is a significant start-up cost when training AI models, and this highlights a need for the broader coordination to build and maintain cybersecurity-specific datasets.

- **AI Model Performance and Reliability:** AI models must be accurate and reliable, and perform as expected across various situations. Key aspects include model generalization and robustness to handle out-of-distribution inputs, adversarial testing to uncover vulnerabilities, monitoring model accuracy, and updating to maintain optimal performance. Model monitoring involves validating and verifying model outputs, along with post-training to detect false positives or negatives. Given the rapid evolution of cybersecurity threats, AI models will need to adapt to these threats to avoid inaccurate assessments and produce consistent outputs when processing evolving inputs.

- **Data Security:** Sensitive data must be protected from unauthorized access, use, or disclosure. This requires robust handling and storage practices, along with access control and authentication mechanisms to ensure only authorized personnel can access the data. Encrypting data and using secure communication protocols is important for safeguarding data both within and outside of network boundaries.

- **Automation Lifecycle Protection:** Automation tools and AI systems themselves must be secure and trustworthy from development through deployment. If not protected, then automated tools are targets for tampering (e.g., model poisoning) or other exploitation (e.g., software vulnerability). This requires that extra steps be taken to ensure security during all stages of development and operations.

- **Integration Challenges:** There are multifaceted challenges to incorporate more advanced capabilities, like AI-driven and automated tools, into existing infrastructures. These challenges include the difficulty of ingesting and transforming data due to varying data standards and formats. Legacy systems often feature outdated or poorly supported software and hardware components, lack modular design, and present software incompatibilities, all of which complicate integration and require time-consuming development of adapters. Limited resources, such as computing power and memory, also constrain the types of AI technologies that can be used. This parallels the fact that integrating diverse technologies, especially in air-gapped environments, poses both technical and procedural challenges. These integration concerns will be a challenge for developing and maintaining up-to-date AI capabilities.

- **Human Factors:** Human factors can pose an impediment to automation and AI adoption; human behavior and culture must be considered when interacting with

such capabilities. These factors include: biases in decision making, cultural changes in how an organization's processes currently operate, communication barriers between technical and non-technical teams, as well as providing interfaces that are easy and intuitive to use. User complacency or misplaced trust in automation can also lead to errors or a reduction in situational awareness. Educating users becomes an important part of any automated or semi-automated process integration.

- **Scalability** There are scalability and performance challenges with automation and AI. As AI system adoption grows, it is crucial to design these systems to handle varying data volumes, training requirements, and user population effectively. Inadequate resource allocation, such as insufficient computational power, can restrict the performance of AI functionality, leading to performance bottlenecks. It is also essential to prevent delays in automation integration through managing costs such as initial hardware investments and ongoing resource needs. Designing systems with an evolution plan that accommodates new hardware and software advancements presents an additional challenge.

## QUESTION 3: What are the data needs for these SWFT automation and AI capabilities, including supplier SBOM, DoW, or third-party sources?

- **Standardization:** It is important to establish standardized formatting for common data sources, like SBOMs, as well to ensure that all data is machine-readable. To be effective, automation and AI tools need to understand the schema or structure of the data to be able to process data correctly. If the data ingestion stage bottlenecks, then creating and maintaining custom-created rules across non-standard data will be necessary.

- **Necessary DoW Data Types:** To ensure that all stakeholders understand what is expected to perform DoW RMF risk assessments it is necessary for DoW to identify and classify the various data types that support the development, deployment, and maintenance of a secure software supply chain.

- **Threat Intelligence Feeds:** Threat Intelligence feeds offer both real-time updates and context on active exploits, attacker TTPs, and insights into supply chain risks. By incorporating these feeds into the SWFT risk assessments, organizations can improve their ability to detect and respond to threats in real-time. The types of Threat Intelligence Feeds that should be considered include:

- Commercial threat intelligence and open-source intelligence feeds from reputable providers
- Government agency threat intelligence for information on national security threats
- Threat actor profiles in the form of foreign adversary lists

- **Vulnerability Databases:** Understanding the vulnerabilities that threats exploit relies on up-to-date threat knowledge. New and emerging vulnerabilities develop quickly, and these conditions require the continuous monitoring of vulnerability data. A variety of vulnerability data sources such as CVEs and Common Weakness Enumerations (CWEs) in the National Vulnerability Database and the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) Catalog are available to meet this need.

- **Configuration Baselines:** By establishing a clear understanding of system configurations, organizations can identify potential security risks, prioritize remediation efforts, and maintain an accurate picture of their overall cybersecurity posture. The types of data used to build out a configuration baseline include:
  - Hardware and software baselines
  - Network baselines (e.g., design artifacts, traffic data, trust boundaries, service interaction patterns)
  - Configuration management databases to track changes to the systems over time, which can include Infrastructure-as-Code templates
  - Runtime environment metadata to understand how systems are configured and deployed in production
  - Security control details, like firewall policies and access control lists
  - System contingency plans in the event of a disruptions or failure

- **AI Training Data:** High-quality data is required for effective AI model training. Diverse and representative datasets ensure accurate and reliable AI outputs. This applies to all incoming data, including supplier-provided data, DoW-specific datasets, and third-party sources. AI-specific data needs, in addition to the data discussed in the other sections, are:
  - Verified and validated datasets labeled and vetted to ensure there are no gaps, biases, or artifacts that can negatively influence training or model development

  - Model cards listing the metrics of the AI models assist understanding the capabilities and software/hardware needs, in addition to the data used in training of the chosen models
  - Training data requirements – clear and concise needs so that new data can be seamlessly added
  - Model benchmarks allow for organizations to effectively gauge model performance against their broader community. Standardized benchmarks provide insight into their own utility, indicating when new benchmarks need to be developed over time.

- **Historical Data:** Historical cybersecurity data can provide significant benefits when training AI models: knowledge of past threats, attack patterns, and defense mechanisms help to orient around cybersecurity needs, even if data is dated. This data helps in identifying trends and anomalies that may indicate potential security breaches. By learning from previous incidents, AI models can improve their predictive accuracy, enhance threat detection, and develop more robust strategies to possibly mitigate future risks. Types of historical data include:
  - Historical RMF/ATO data such as SSPs, POAMs, and other eMASS information
  - Cybersecurity incident reports
  - Incident response metrics/plans such as logs and remediation outcomes

- **SBOM Data Requirements:** SBOMs can enhance transparency and security by providing detailed SCA information about the software's constituent elements. These allow stakeholders to enhance the SBOM data by mapping the elements to known vulnerabilities, cyber threats, associated systems, and other resources to facilitate risk management. The contents of these documents can determine the ease of performing risk assessment thus SBOMs are important as they contain a comprehensive inventory of all software components. There must be a clear understanding of the software's composition, including version numbers, suppliers, licenses, and vulnerabilities. Specific SBOM needs include:
  - Standardized, machine-readable formats (e.g., CycloneDX, SPDX)
  - Component identification (e.g., software versioning, package URL (PURL))
  - License information
  - Component provenance
  - Component dependency relationships
  - Component metadata (e.g., function, purpose, processing characteristics)

- **OSS Security Metrics:** OSS could provide robust and innovative software solutions for DoW-defined needs. However, due to unrestricted access to its source code allowing anyone to view, modify, or distribute code, additional effort is needed to identify, track, and mitigate OSS component risk. The following additional OSS data were recommended:
    - OSS project health data through metrics like commit frequency, issue tracking and community engagement
    - Maintenance data (e.g., patching, commits)
    - Code quality metrics to measure useability and potential for vulnerabilities
    - Community trust analysis (e.g., code reliability, foreign contributor analysis)
    - OSS component IDs to track software in DoW systems

- **Software Development Artifacts:** There is a challenge with integration of new capabilities into older systems. Development documentation and data may mitigate the issue. Software development documentation such as practices, testing information, pipeline architecture and deployment needs can help with understanding components and their interdependencies.

# CONCLUSION

Overall, the findings across the three RFIs paint a picture of an industry actively working to align with established security standards while grappling with the practical challenges of standardization, integration, and automation. This aligns directly with the DoW's SWFT Initiative, launched to reform and accelerate the Department's acquisition, testing, and authorization of secure software by defining clearer cybersecurity requirements and promoting rapid software adoption. The responses indicate a broad readiness among Defense Industrial Base (DIB) companies to embrace advanced methodologies and tools that can enhance risk assessments and streamline the Department’s software authorization processes, especially through approaches like Continuous ATO which can significantly reduce delays and improve security posture. The responses endorse the NIST controls, including NIST 800-53 and the emphasis of the current RMF on protecting information, and ensure proper information and records management, accessibility, and privacy.

The insights emphasize the need for clear, consistent guidelines and robust collaboration among suppliers, external assessors, and DoW stakeholders to fully realize the potential of SWFT initiatives in a secure and efficient manner. By implementing SWFT's modular, reusable authorization framework and leveraging technologies like SBOMs for transparency and automated analysis, the DoW and DIB can foster a more secure software supply chain, proactively identify vulnerabilities, and accelerate the delivery of robust, mission-ready software to the warfighter.

# APPENDIX I – ACRONYMS AND ABBREVIATIONS

| Acronym | Meaning |
|---|---|
| SWFT | Software Fast Track |
| RFI | Requests for Information |
| DoW | Department of War |
| NIST | National Institute of Standards and Technology |
| SP | Special Publication |
| OWASP | Open Worldwide Application Security Project |
| SBOM | Software Bill of Materials |
| RMF | Risk Management Framework |
| FedRAMP | Federal Risk and Authorization Management Program |
| SOC | Service Organization Control |
| ISO | International Organization for Standardization |
| OSS | Open-Source Software |
| SAMM | Software Assurance Maturity Model |
| ASVS | Application Security Verification Standard |
| SCVS | Software Component Verification Standard |
| C-SCRM | Cybersecurity Supply Chain Risk Management |
| SSDF | Secure Software Development Framework |
| IEC | International Electrotechnical Commission |
| SLSA | Supply-chain Levels for Software Artifacts |
| BoE | Body of Evidence |
| CNSSI | Committee on National Security Systems Instruction |
| SSP | System Security Plan |
| SAR | Security Assessment Report |
| RAR | Risk Assessment Report |
| POA&M | Plan of Actions and Milestones |
| APIs | Application Programming Interfaces |
| ATO | Authority to Operate |
| eMASS | Enterprise Mission Assurance Support Service |
| TTPs | Tactics, Techniques, and Procedures |
| ISMS | Information Security Management System |
| CMMC | Cybersecurity Maturity Model Certification |
| DISA | Defense Information Systems Agency |
| STIGs | Security Technical Implementation Guides |
| DCSA | Defense Counterintelligence and Security Agency |
| FOCI | Foreign Ownership, Control, or Influence |
| CMMC-AB | Cybersecurity Maturity Model Certification Accreditation Body |
| ANAB | ANSI National Accreditation Board |
| PCI SSC | Payment Card Industry Security Standards Council |
| CSSLP | Certified Secure Software Lifecycle Professional |
| CISSP | Certified Information Systems Security Professional |
| CCSP | Certified Cloud Security Professional |

| | |
|---|---|
| **CISM** | Certified Information Security Manager |
| **CEH** | Certified Ethical Hacker |
| **SCA** | Software Composition Analysis |
| **AI** | Artificial Intelligence |
| **CVEs** | Common Vulnerabilities and Exposures |
| **AOs** | Authorizing Officials |
| **CWEs** | Common Weakness Enumerations |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **KEV** | Known Exploited Vulnerabilities |
| **PURL** | Package URL |
| **SPDX** | Software Package Data Exchange |
| **DIB** | Defense Industrial Base |

# APPENDIX II – SAM.GOV RFIS

To read the Request for Information (RFI) – Software Fast Track (SWFT) Tools please visit: https://sam.gov/opp/753c9598b7904657b528e9de39efdee8/view

To read the RFI – Software Fast Track (SWFT) External Assessment Methodologies please visit: https://sam.gov/opp/4a79c3e777c24d14a69d6c090950a755/view

To read the RFI – Software Fast Track (SWFT) Automation & Artificial Intelligence (AI) please visit: https://sam.gov/opp/7ca9ff30bad5407db7de079f7bf397c0/view