sonatype

Decoding SWFT: How DoD's Software Fast Track Redefines Secure Acquisition

Introduction: From 18 Months to 30 Days for Mission-Critical Systems

Ask any program executive about earning an Authority to Operate (ATO), and they'll likely tell you about how tedious it can be. The process, while essential, is riddled with inefficiency. Paper packages take so much time to compile, review, and approve that they're outdated as soon as they're complete. Coupled with point-in-time scans that lack context and repeated oversight through "redundant reviews," these measures often extend system deployment timelines to over 18 months. Meanwhile, threat actors evolve their tactics in a matter of hours. Every delay in deployment risks compromising mission readiness and national security, leaving the Department of Defense (DoD) at a strategic disadvantage.

This misalignment between traditional security protocols and today's operational demands is no longer tenable. Recognizing the stakes, the DoD has chosen to act. Enter the **DoD Software Fast Track Initiative (SWFT)**, an ambitious, CIO-led initiative redefining how ATOs are achieved. With SWFT, the focus shifts from static documents to dynamic data. By treating software security data as code, SWFT transforms ATO from a sluggish compliance checkpoint into an iterative, high-speed process. The goal is not incremental improvement, but a revolutionary leap—from the current 18-month timeline to as little as 30 days, making "idea to impact" a rapid and seamless reality.

In this guide, we explore how SWFT is poised to reset the standard for software security and deployment in the DoD. By leveraging cutting-edge methods and frameworks, SWFT aligns innovation with security at a speed designed for today's challenges. Stay with us as we unpack the inner workings of this paradigm shift and its implications for the future of mission-critical systems.

What is SWFT?

SWFT, announced through three RFIs in April 2025, represents an effort to revolutionize software security and deployment within the DoD. At its core, SWFT establishes a tiered pipeline aimed at accelerating trust and authorization processes without compromising security. This pipeline is composed of three critical components:

- **SWFT Tools** – Vendors are required to submit machine-readable security artifacts, including Software Bills of Materials (SBOMs), vulnerability attestations, and policy automation evidence. These ensure transparency and provide detailed insights into the security posture of software components.
- **External Assessment** – Accredited third-party evaluators independently validate the submitted artifacts. By introducing these trusted external assessments, SWFT integrates additional layers of confidence and assurance into the process.
- **Automation & AI** – Leveraging cutting-edge automation and artificial intelligence, DoD platforms process and analyze the submitted data. These advanced algorithms are instrumental in generating well-informed and efficient authorization recommendations.

Spearheaded by the DoD Chief Information Officer, SWFT demonstrates a forward-thinking approach to modernizing software security frameworks. These RFIs have set the stage for an anticipated pilot program and draft solicitation set to be released later this fiscal year. This effort signals a pivotal moment in the DoD's commitment to aligning innovation with secure, mission-critical deployment strategies.

Why SWFT Matters to System Integrators

For system integrators, adopting SWFT marks a significant shift in managing security and compliance within government contracts. By helping prime contractors reduce delivery risks, SWFT provides a clear avenue for streamlining and strengthening project execution.

By leveraging **SBOM-centric reciprocity**, integrators can eliminate the burdensome and repetitive security testing typically required across multiple contracts. This ensures compliance without redundancy, significantly reducing both time and resource expenditure. Additionally, SWFT's machine-assisted **approval processes** promise to slash wait times, enabling companies to reallocate IRAD funds toward developing innovative capabilities rather than navigating prolonged compliance obstacles. Through **standardized APIs**, integrators gain the flexibility to incorporate best-of-breed tools into their workflows without the necessity of building program-specific scanners.

This level of interoperability accelerates project timelines while maintaining robust security standards. Importantly, SWFT's forward-thinking framework encourages early adoption, empowering integrators to embed SWFT-ready pipelines into proposals today. Such proactive alignment translates into scoring technical strengths points in evaluations tomorrow, directly enhancing competitiveness in future contract awards.

Sonatype: Purpose-Built for SWFT Success

For more than 15 years, Sonatype's mission has been to secure the software supply chain from the first commit to production. As a result of this vision, the Sonatype platform aligns with SWFT's artifact-driven model, providing the tools and technologies necessary to meet the program's rigorous demands.

Sonatype SBOM Manager

Sonatype SBOM Manager is purpose-built to generate, ingest, enrich, and securely share SBOMs with VEX (Vulnerability Exploitability eXchange) data. It supports exporting SBOMs in industry-standard CycloneDX and SPDX formats. SBOM Manager provides fully documented REST APIs for programmatic interaction, available through help.sonatype.com, and supports high-availability (HA) deployments in Kubernetes environments using Helm charts. These capabilities ensure teams can manage complex SBOM requirements with precision and interoperability.

Sonatype Lifecycle

Sonatype Lifecycle enforces NIST 800-218 **Secure Software Development Framework (SSDF) policies directly in CI pipelines**, creating an essential safeguard for secure builds. It generates detailed reports and artifacts, such as CycloneDX and SPDX SBOMs, that serve as evidence for attestation and can be reviewed by external assessors. Lifecycle provides extensive REST APIs for integration and makes detailed event data available in the policy-violation.log for monitoring. It supports high-availability deployments and allows teams to implement policy gates that can warn or fail a build based on criteria such as a dependency's CVSS score (e.g., >= 7.0) or its integrity rating. Lifecycle, in conjunction with SBOM Manager, facilitates provenance attestation by enabling automated exports of SBOMs and allowing VEX data to be programmatically added to reflect a component's vulnerability status.

Lifecycle also allows teams to implement SSDF policy gates, blocking builds when a dependency exceeds a CVSS score of 7.0 or lacks a verified hash, critical to ensuring application integrity. Additionally, it facilitates provenance attestation by enabling automated exports of CycloneDX or SPDX SBOMs for external assessor signatures, as well as automated VEX merge functionality to integrate vendor VEX statements into every SBOM snapshot during pipeline runs.

Sonatype Nexus Repository

Sonatype Nexus Repository is the foundation for hosting trusted, tamper-evident binaries that align with SWFT's mission. It supports HA clustering via Helm and provides comprehensive REST endpoint exposure for artifact introspection. By offering high-availability solutions and tamper-proof technologies, Repository Manager ensures the integrity and security of the software supply chain while reducing operational risks.

Sonatype Repository Firewall

Sonatype Repository Firewall acts as the first line of defense, quarantining suspicious artifacts at the point of entry and analyzing them with unrivaled speed. It proactively blocks malware before it enters the pipeline, emits real-time webhook events for rapid incident response, and logs artifact decisions comprehensively for audit purposes. With these tools, Sonatype Firewall ensures absolute control over the flow of artifacts, enabling teams to respond swiftly to potential threats without disrupting productivity.

These capabilities are not abstract theorizing—they are proven solutions deployed today. Across six IL6-plus programs within the Air Force, Army, and Intelligence Community environments, the Sonatype air-gapped environment (SAGE) is a trusted backbone for SWFT readiness. Just in FY 2024, Sonatype's platform successfully blocked over 3 million malicious download attempts and now catalogs 270 million component hashes. This unmatched intelligence empowers Department of Defense assessors with the tools they need to maintain comprehensive software supply chain security.

Seamless Integration with Your AI Risk Engine

Integrators frequently ask, "How can we integrate Sonatype data into our analytics or machine learning pipelines?" Sonatype provides multiple mechanisms for integration, including comprehensive REST APIs and webhooks, that deliver vulnerability alerts and policy decisions into your SIEM, data lake, or AI-based risk scoring systems.

Data Type	Integration Method	API Endpoint / Mechanism
P Policy Violations	Log File Monitoring	The policy-violation.log file contains a real-time, line-delimited JSON record of all policy events (create, fix, waive).
M Policy Violations	REST API (Pull)	The Report REST API can be polled to retrieve detailed policy violation data for a specific application report.
SBOM Management	REST API (Push/Pull)	The SBOM Manager API allows for importing, exporting, and retrieving SBOMs and their associated VEX data.
Quarantine/ Audit Events	Webhooks (Push)	Nexus Repository can be configured with global or repository-specific webhooks to send HTTP POST requests for audit and repository events, such as a component being quarantined.

Your analytics engine can poll the REST APIs or subscribe to webhook events to receive security data. This data can then be enriched with mission context to calculate a risk score within your own platform. This plug-and-play model aligns with the SWFT Automation & AI RFI directive to "utilize supplier SBOM, SWFT artifacts and attestations, and DoD-specific knowledge" for accelerated authorization decisions.

Certify Once, Use Many

Imagine an Air Force squadron tasked with deploying the latest drone telemetry service into the Advanced Battle Management System (ABMS). Under the legacy system, each squadron must independently collect SBOM data and undergo a repetitive risk management framework (RMF) review for approval. This fragmented approach not only delays critical deployments but also expends significant resources and creates redundancies, preventing the armed forces from achieving operational agility.

With SWFT and the Sonatype platform, this process could be radically streamlined. Here's how it would work:

1

Vendor Submits an SBOM

Using Sonatype's SBOM Manager or Lifecycle, the vendor generates and submits a complete, machine-readable SBOM that includes a detailed view of all software components, dependencies, and metadata. This submission complies with the latest cybersecurity mandates and ensures high-quality, transparent documentation.

2

Certified Assessor Validates Policies

Leveraging Sonatype's Lifecycle evidence, a certified assessor validates the SBOM against established security and compliance benchmarks. The process incorporates automated policy enforcement powered by Sonatype's unmatched data intelligence—cataloging over 270 million component hashes—to detect risks or anomalies in seconds.

3

DoD AI Cross-Checks Risk Data

The Department of Defense integrates advanced AI algorithms to cross-reference the submitted SBOM with dynamic threat intelligence. This step provides a thorough risk evaluation and ensures that all known vulnerabilities, malicious code, and compliance gaps are flagged before approval.

4

Reusable Approval Issued

Once cleared, the AI issues a reusable authorization for the software. This approval, securely logged and maintained within SWFT, can now be applied across squadrons and use cases, eliminating the need for duplicate reviews. The result? A standardized, trusted certification that works seamlessly across deployments.

With SWFT and Sonatype driving modernization, the "Certify Once, Use Many" model reduces deployment timelines from years to mere weeks. Drone telemetry services and other mission-critical applications can achieve operational readiness on time without compromising on security or quality. Centralizing these processes not only saves resources but also strengthens the Department of Defense's ability to innovate and respond to emerging threats faster than ever before.

Partner With Sonatype

Whether you're crafting a SWFT RFP response or aiming to modernize your existing CI/CD pipeline, Sonatype can help by offering:

API Integration Briefing	Helm-Chart Deployment Demo	Secure Artifact Pipeline Showcase
Discover how our REST and event-driven APIs, embedded in SBOM Manager and Lifecycle, feed into powerful AI-driven analytics.	See hands-on demonstrations of high-availability Kubernetes deployments (Big Bang-compatible) designed for both classified and unclassified environments.	Explore a seamless artifact pipeline using Sonatype Lifecycle and SBOM Manager to generate, manage, and enrich industry-standard SBOMs (CycloneDX/SPDX) in a fully interactive sandbox environment.

Contact our **Federal Solutions team today** to schedule a session tailored to your needs. Together, we'll accelerate secure software delivery to the mission, driving innovation and enabling the operational excellence that SWFT demands.

sonatype

Sonatype is the leader in secure software development built on open source and AI. As the maintainers of Maven Central and creators of Nexus Repository, Sonatype has spent two decades pioneering how the world manages and secures open source software — making Sonatype the trusted authority for modern software supply chains. With unmatched open source visibility and a unified product suite built for modern software development, Sonatype gives enterprises the intelligence and automated governance they need to harness the full potential of open source and AI. Sonatype handles the complexity behind the scenes: guiding component and model selection, blocking harmful malicious code, automating dependency and vulnerability management, and ensuring faster, more reliable builds — so developers spend more time on innovation and less time on remediation and rework. Trusted by more than 15 million developers, Sonatype helps power secure, modern software development at nearly 2,000 global organizations including 70% of the Fortune 100. To learn more about Sonatype, please visit **www.sonatype.com**.