# CONFORMANCE BEYOND THE SBOM

A Practical Guide for Industry to Securely Develop Software for the U.S. Government

Brian Gallagher
President, Koniag Cyber
bgallagher@koniagcyber.com

## Executive Summary

Following Executive Order (EO) 14144 and its June 2025 amendment, federal software security requirements have evolved significantly. While EO 14028 laid the foundation for secure software supply chains, EO 14144 expanded these mandates—emphasizing practical implementation of NIST SP 800-218, memory-safe development, and resilience against AI and quantum threats. This white paper details the updated requirements and provides strategies for conformance across SSDF, NIST SP 800-171r3, and CMMC.

## The Policy Landscape Driving Secure Software Requirements

EO 14028 focused on foundational cybersecurity. EO 14144 and its June 2025 update clarified execution: removing mandates for centralized CISA attestations and enabling agencies to collect and evaluate self-attestation and documentation.

Key provisions include:

- NIST-led public-private consortiums to operationalize SSDF.
- Updated SP 800-53 controls for secure update and patching.
- Extended focus on PQC (Post-Quantum Cryptography), AI risk, and IoT assurance via Cyber Trust Mark.

## Understanding NIST SP 800-218 (SSDF)

EO 14144 reinforces SSDF's structure and mandates its operationalization. The four SSDF domains remain:

1. PO: Governance and preparedness (training, policy)
2. PS: Environment integrity (access control, build pipelines)
3. PW: Secure engineering practices (code standards, review, analysis)
4. RV: Real-time vulnerability management and disclosure

NIST is now required to publish updated SSDF implementation guidance by December 2025. Organizations must align proactively.

## FedRAMP is Not the Only Path: Alternative Compliance Routes

EO 14144 formalized the use of decentralized self-attestations rather than centralized CISA upload. Industry can show conformance by:

- Using NIST SSDF-aligned secure SDLC documentation.
- Participating in NIST consortium pilots.
- Integrating DevSecOps pipelines into DoD's cATO for Continuous Authorization.
- Mapping to maturity models like SCVS, BSIMM for deeper software assurance.

## Going Beyond the SBOM: Practical Measures for SSDF Conformance

SBOM remains a baseline expectation. EO 14144 adds urgency to the following practices:

- Patch Delivery Assurance: Build secure update mechanisms, as NIST SP 800-53 will be updated with guidance on this.
- Secure Code Engineering: Integrate memory-safe languages (e.g., Rust) and formal verification.
- Behavior Monitoring: Use anomaly detection on CI/CD pipelines to prevent pre-deployment malware.
- Quantum Readiness: Begin cryptographic agility planning.
- AI Security: Assess ML components for training data integrity and model threats.

## Alignment with NIST 800-171r3 and CMMC

EO 14144's secure development emphasis harmonizes with 800-171r3's focus on protecting CUI and aligns with CMMC Level 2 (based on 800-171) and Level 3 (based on 800-172). Vendors should build SSDF-aligned practices into their NIST 800-171/CMMC assessments to streamline compliance and demonstrate maturity.

## Continuous Monitoring and Assurance

EO 14144 shifts focus from point-in-time certifications to continuous posture management:

- Establish software telemetry and security dashboards.
- Automate vulnerability scanning and secure release validation.
- Continuously monitor AI/ML software behavior.
- Employ secure patch verification as required in upcoming NIST updates.

## Recommendations for Industry Leaders

Monitor NIST's SSDF updates and join implementation pilots.

- Prepare for patch verification mandates by modernizing delivery infrastructure.
- Develop post-quantum migration roadmaps.
- Embed AI threat modeling in your secure design reviews.
- Continue SBOM generation but support it with update assurance, source provenance, and component hardening.

EO 14144 and its June 2025 update signal a pivot to scalable, measurable, and forward-looking secure software assurance. Vendors must adapt to decentralized agency-driven attestations, evolving SSDF implementation, and continuous risk-based compliance. This paper offers a roadmap to demonstrate trustworthiness and compliance beyond mere documentation.

At Koniag Cyber, we help our clients be foundationally prepared and ahead of changing policies. Get started at koniagcyber.com/contact