
SIE
Eracent
SUMMER'S HERE &
IT'S HEATING UP
SBOM SMARTS FOR
FEDERAL &
COMMERCIAL
RESILIENCE

TODAY'S SPEAKERS

Terry Divelbliss

Eracent

Latoya Taylor

The SIE Group

Melissa Golden

The SIE Group

Stephanie Pepe

The SIE Group

HOUSEKEEPING

SIE

Eracent

BEFORE WE DIVE IN, JUST A FEW NOTES TO HELP US ALL GET THE MOST OUT OF TODAY'S SESSION:

This webinar is being recorded.

Add your Q&As into the chat.

Participants are muted by default.

Technical issues? Reach out in the chat.

AGENDA

SIE

Eracent

1. What is an SBOM?
2. Cybersecurity Implications for Federal Agencies
3. SBOMs in Commercial Industries
4. Spotlight on Eracent's SBOM Manager™ Tool
5. Real-world Case Study
6. Q&A
7. Conclusions & Next Steps

WHAT IS AN SBOM?

SIE

Eracent

1. SBOM = Software Bill of Material
2. A detailed inventory or “ingredient list” of all components in a piece of software.
3. It allows agencies to track and verify what’s inside their software applications.
4. HBOM = Hardware Bill of Material

WITHOUT AN SBOM, ORGANIZATIONS LACK VISIBILITY INTO WHAT’S RUNNING IN THEIR ENVIRONMENTS.

SBOMS SUPPORT THESE CRITICAL ISSUES

SIE

Eracent

1. Vulnerability Identification and Mitigation
2. Obsolescence and Version Management
3. License Type Risk

DON'T LET HIDDEN COMPONENTS BECOME YOUR BIGGEST SECURITY BLIND SPOT.

CYBERSECURITY IMPLICATIONS FOR FEDERAL AGENCIES

SIE

Eracent

Cyber threats are evolving, and federal agencies must stay ahead. SBOMs play a critical role in securing software supply chains.

Regulatory Compliance, **Incident Response**, and **Zero Trust Architecture** are ways in which SBOMs can help the government combat cyber threats.

Regulatory Compliance

SBOMs help agencies comply with Executive Order 14028, NIST SP 800-218, and OMB M-22-18

Incident Response

When vulnerabilities arise, agencies can quickly identify affected software and patch accordingly

Zero Trust Architecture

SBOM aligns with ZTA policies, ensuring continuous verification of software integrity

CYBERSECURITY EXECUTIVE ORDER UPDATES

SIE

Eracent

WHAT'S CHANGING UNDER NEW EO

- **ELIMINATED**: Machine-readable attestation mandates
- **ELIMINATED**: CISA's centralized attestation repository
- **ELIMINATED**: Rigid checklist-driven processes
- **SHIFT**: Move to flexible, agency-level judgments aligned with SSDF 2.0

NEW REQUIREMENTS FOR FEDERAL AGENCIES

IoT Security: "U.S. Cyber Trust Mark" required by **Jan 4, 2027**

Encryption: TLS 1.3+ required by **Jan 2, 2030**

SSDF Updates: Industry consortium by **Aug 1, 2025**

Enhanced Security: BGP routing protection & vulnerability-first AI development

CRITICAL IMPLEMENTATION DATES

Aug 1, 2025
NIST Consortium Formation

Dec 1, 2025
SSDF Update & PQC Lists

Jan 4, 2027
IoT Trust Mark Requirement

SBOMS IN COMMERCIAL INDUSTRIES

SIE
Eracent

SBOMs are becoming increasingly vital in commercial industries, including healthcare, finance, critical infrastructure, and manufacturing.

These sectors handle sensitive data, rely on complex software ecosystems, and face rising cybersecurity threats.

Critical Infrastructure Protection

Energy, transportation, and water systems rely on operational technology (OT) and industrial control systems (ICS), which are increasingly targeted by cybercriminals. SBOMs enhance visibility into supply chain dependencies.

Software Supply Chain Resiliance

Organizations across industries rely on open-source and third-party software. By adopting SBOMs, companies can identify untrusted or vulnerable components.

Zero Trust & Security Compliance

Private organizations are shifting to Zero Trust security models. SBOMs align with Zero Trust principles by ensuring continuous software integrity monitoring and real-time vulnerability detection.

COMMERCIAL SECTOR IMPACTS

SIE
Eracent

Software Vendors: Shift to secure-by-design tooling based on SSDF 2.0

IoT Manufacturers: Prepare for federal cybertrust label compliance

Cloud Services: Support PQC-ready encryption and TLS 1.3+

AI/ML Vendors: Adopt vulnerability management and rapid patching processes

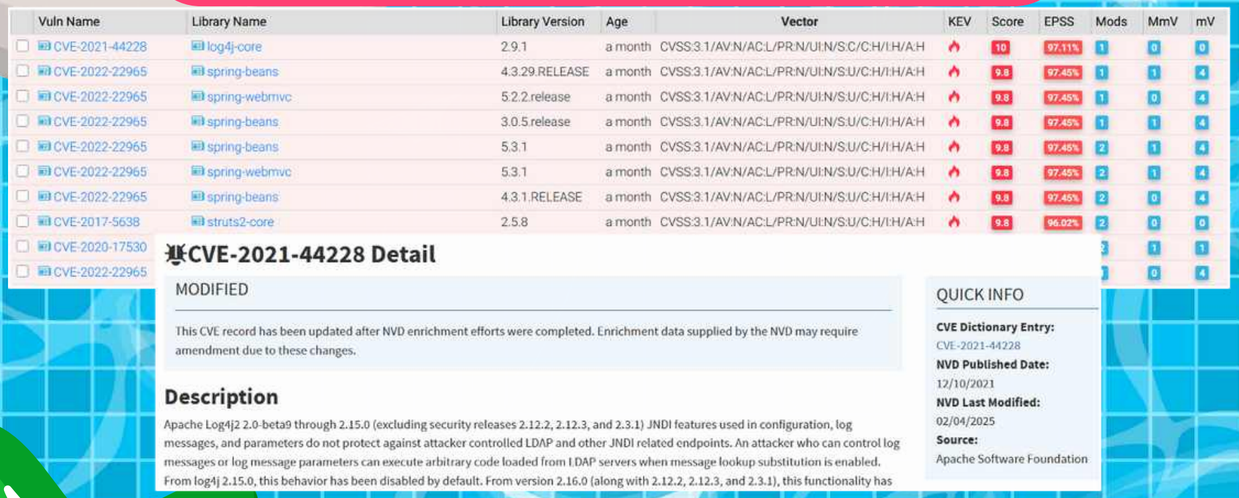
KEY TAKEAWAY

SBOMs remain essential for cybersecurity compliance and operations. The new EO streamlines implementation by removing bureaucratic attestation requirements while adding stronger security mandates for IoT, encryption, and AI systems.

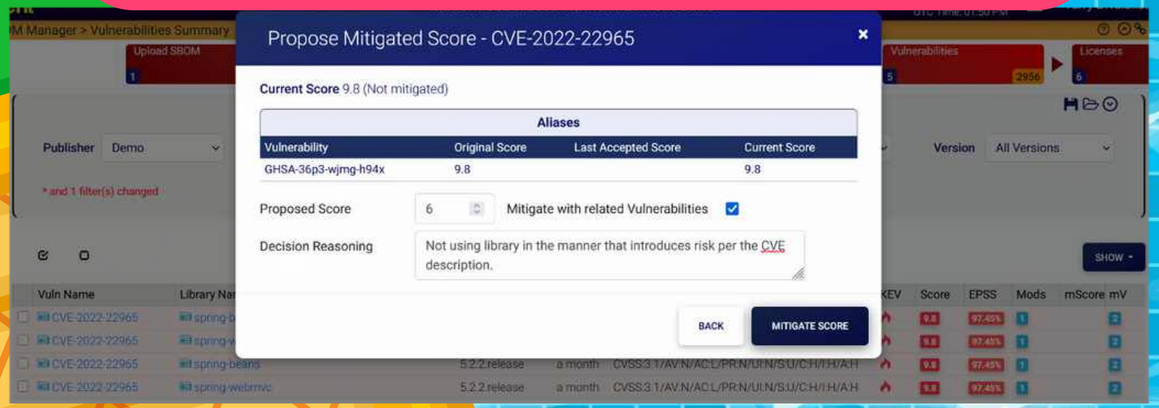
ERACENT'S SBOM TOOL

SIE Eracent

VULNERABILITY DETAILS & CVES



VULNERABILITY SCORE MITIGATION



Eracent's SBOM Manager™ is a consolidated repository of content for multiple SBOMs. The tool's functionality meets requirements for software consumers and developers.

SBOM Manager™ offers:

- Risk scores, levels of criticality, dependencies and more
- Vulnerability data from NIST NVD, GitHub Advisory, OSV and other trusted sources
- Visibility when new vulnerabilities are reported
- Version tracking and obsolescence management are built in

COMMON QUESTION:
DOES SBOM MANAGER CREATE SBOMS?

No - SBOM Manager™ ingests and refines SBOMs provided by vendors or your dev teams

HERE'S HOW IT WORKS:

1. SBOMs come from vendors/OEMs (CycloneDX, SPDX, SWID formats)
2. SBOM Manager deconstructs and organizes components
3. Platform performs error checking and creates corrected versions
4. Fast indexing maps components to associated products

SIE

Eracent

CASE STUDY: DOD SOFTWARE FAST TRACK (SWFT) INITIATIVE

SIE Eracent

KEY MANDATE DETAILS

- **Effective Date**: June 1, 2025 *(ACTIVE NOW)*
- **Scope**: All software vendors selling to Department of Defense
- **Goal**: Replace slow Risk Management Framework (RMF) with AI-powered system
- **Processing**: Automated evaluation against 12 distinct risk characteristics

TRIPLE SBOM REQUIREMENT

- **Production Environment SBOM** - Live system documentation
- **Sandbox Environment SBOM** - Testing environment transparency
- **Third-Party Verified SBOM** - Independent validation required
- **AI Analysis**: Automated backend evaluation for digital ATO approval

TRANSFORMATIONAL IMPACT

- **Eliminated**: Mountains of paperwork and human review delays
- **Accelerated**: Software approval from months to potentially days/hours
- **Enhanced**: Supply chain transparency for military applications
- **Standardized**: SBOM formats (SPDX, CycloneDX) across DoD procurement

DESCRIPTION OF IMPACT - PENTAGON'S MOST AMBITIOUS SOFTWARE MODERNIZATION EFFORT

- **FIRST MAJOR AI-POWERED** government software approval system
- **AFFECTS ALL** defense contractors and software vendors
- **CREATES COMPETITIVE ADVANTAGE** for vendors with mature DevSecOps practices
- **SETS NEW STANDARD** for automated security assessment in government procurement
- **TRANSFORMS COMPLIANCE** from burden into business differentiator

SIE

Eracent

QUESTIONS & ANSWERS

CONCLUSIONS & NEXT STEPS

- SBOMs enhance supply chain security, compliance, and risk mitigation
- Agencies must adopt SBOMs to meet federal cybersecurity mandates
- Eracent's SBOM Manager™ simplifies SBOM integration, making compliance easier

SIE

Eracent

CONTACT US

SIE

LTAYLOR@SIECONSULTINGGROUP.COM
WWW.THESIEGROUP.COM

Eracent

TERRYD@ERACENT.COM
WWW.ERACENT.COM