sonatype

Sonatype Software Supply Chain Risk Management

Stay Compliant with NIST SP 800-218 and CISA Attestation Requirements

Software Supply Chain Risk Management is a Matter of National Security

In May 2021, the White House issued Executive Order 14028 on Improving the Nation's Cybersecurity, the first federal regulation targeting the security of software components. Designed to drive immediate improvements in the nation's IT security posture, the comprehensive measure was a direct response to several high-profile cyberattacks. In particular, the 2020 SolarWinds breach and the 2021 Log4j vulnerability underscored the susceptibility of software supply chains.

As a result, Executive Order 14028 included a directive for the National Institute for Standards and Technology (NIST) to issue guidance on enhancing the security of the software supply chain, which it did with an update to The Secure Software Development Framework (SSDF) Version 1.1, or NIST SP 800-218. EO 14028 also requires that system integrators and software vendors comply with NIST SP 800-218 by attesting to compliance using instructions outlined in the Secure Software Development Attestation Form provided by the Cybersecurity and Infrastructure Agency (CISA).

Sonatype protects and defends organizations and government agencies from the inherent risks in the open source software ecosystem. This document outlines how our capabilities align with EO 14028 Section 4 ("Enhancing Software Supply Chain Security") and CISA attestation requirements of NIST SP 800-218, including the ability to create, ingest, and continuously monitor SBOMs (Software Bill of Materials).

What is NIST SP 800-218?	What is the CISA Secure Software Development Attestation Form?
NIST SP 800-218, or SSDF, is a set of high-level software development practices recommended by NIST to be integrated into software development lifecycle (SDLC) models to reduce and mitigate vulnerabilities in published software. It was necessary because few SDLC models explicitly address security. While its focus is on suppliers to the federal government, the best practices outlined in the SSDF can benefit any organization. To implement this, CISA developed the Secure Software Development Attestation Form.	The Secure Software Development Attestation Form requires vendors supplying software to federal entities to certify through a CEO or an authorized designee's signature that their software is developed securely and adheres to the Secure Software Development Framework (SSDF) guidelines established by NIST.

The SSDF addresses four high-level practice areas, each with its own set of activities that address software security in more detail. These practice areas include:

Prepare the Organization (PO)	Protect the Software (PS)	Produce Well-Secured Software (PW)	Respond to Vulnerabilities (RV)
Ensure that the organization's people, processes, and technology are prepared to perform secure software development at the organization level and, in some cases, for individual development groups or projects.	Protect all components of the software from tampering and unauthorized access.	Produce well-secured software with minimal security vulnerabilities in its releases.	Identify residual vulnerabilities in software releases and respond appropriately to address those vulnerabilities and prevent similar vulnerabilities from occurring in the future.

Software can't be secure without fully understanding what goes into it, and untangling all these regulations can be daunting. This is where the Sonatype platform comes in. Organizations can store, manage, inspect, and track the quality and security of software components, and better-managed software supply chains result in lower risk.

Here's a summary of how the Sonatype platform can help meet these requirements:

NIST 800-218 Requirements and Sonatype

Prepare the Organization (PO)

PO 1: Define Security Requirements for Software Development

Sonatype is an industry leader in defining policies for securing third-party and source components used throughout the SDLC. The Sonatype platform makes it possible to define policies for securing open source components and enforcing them throughout development. Continuous automated monitoring lets you stay current on any new policy violations discovered, even after the software is built. Sonatype also provides constant updates for third-party policies, and an easy-to-use administrative UI simplifies policy management.

PO 2: Implement Roles and Responsibilities

This requirement ensures that everyone involved in the software development lifecycle (SDLC) is prepared to perform their function throughout the entire lifecycle. Sonatype can help define roles within this process by increasing visibility, control, and access across different stages of development.

PO 3: Implement Supporting Toolchains

The Sonatype platform features more than 30 flexible, out-of-the-box integrations and a unified CLI-based integration that can be incorporated across any suitable toolchain. Data can be passed from or to the Sonatype platform by using the API or by standard SBOMs. Sonatype delivers software with an API-first methodology, meaning other tools can readily access most information.

PO 4: Define and Use Criteria for Software Security Checks

The Sonatype platform enhances software security checks by leveraging contextual policy and precise fingerprinting. These features ensure that only high-quality, secure components are used throughout the software development lifecycle (SDLC). By defining criteria for software security checks, the platform helps identify and remediate vulnerabilities early, ensuring compliance with security standards at scale. Sonatype's comprehensive data on known vulnerabilities and its ability to enforce security policies across the development pipeline provide organizations with the tools needed to maintain a robust security posture and develop secure software efficiently.

PO 5: Implement and Maintain Secure Environments for Software Development

The Sonatype platform ensures secure environments for software development by integrating with common SSO workflows and token-based authentication, providing extra security when deployed with third-party external authentication. We recommend running Sonatype in a strictly authenticated mode, requiring each user to authenticate to access any platform features. The Sonatype platform also contains a robust role-based access control (RBAC) system, which minimizes functionality and access to reporting and intelligence by role and organization. Sonatype supports deployment using multifactor authentication and can be implemented in a zero-trust model. Additionally, Sonatype can monitor, detect, and alert changes in the composition of the software built into the customer's SDLC, further enhancing the security of the development environment.

Sonatype can also be used to monitor, detect, and alert to changes in the composition of the software built into the customer's SDLC.

Protect the Software (PS)

PS 1: Protect All Forms of Code from Unauthorized Access and Tampering

Sonatype Nexus Repository is the industry standard artifact repository, offering a robust RBAC and privileges-based system for granular access control. It allows for precise versioning and control of each built artifact, ensuring that all software components are securely stored and managed. This helps limit how components can be modified, preventing unauthorized access and tampering.

In addition, Sonatype Lifecycle enhances security by detecting tampering of dependencies through precise fingerprinting. This advanced capability identifies when a dependency is not a canonical version, highlighting potential integrity issues. Sonatype Repository Firewall further strengthens protection by enforcing policies, such as ensuring that open source code in development environments has its integrity verified or that software in QA environments contains no known critical security vulnerabilities. Together, these tools ensure comprehensive protection of all forms of code from unauthorized access and tampering.

PS 2: Provide a Mechanism for Verifying Software Release Integrity

The Sonatype platform ensures the integrity of software releases through advanced fingerprinting and hash validation of all scanned components. By generating cryptographic hashes for each open source component, the platform allows users to verify the authenticity and integrity of their software. Additionally, the Sonatype platform provides a complete Software Bill of Materials (SBOM), which includes these cryptographic hashes, making the validation process transportable and ensuring that software integrity can be verified throughout the supply chain.

PS 3: Archive and Protect Each Software Release

Sonatype Nexus Repository is especially suited for storing release files, images, as well as other associated metadata such as generated SBOMs and signature files, and allows for versioning and staging as a part of a release process. It also segregates access and makes each release's artifacts completely immutable. This allows attesters to conform to this requirement. In addition to release files, release integrity information can be stored in the Sonatype Lifecycle component, allowing for segregating data and signing.

Produce Well-Secured Software (PW)

PW 1: Design Software to Meet Security Requirements and Mitigate Security Risks

Sonatype provides comprehensive intelligence for OSS components and any associated security vulnerabilities. Developers can use this information to make informed decisions about which dependencies to use, define and enforce security policies, and proactively address any known security issues.

PW 2: Review the Software Design to Verify Compliance with Security Requirements and Risk Information

The Sonatype platform can ensure that third-party components used in the project's design comply with security, licensing, and quality/architecture requirements. Policy administrators can audit and modify the standard policy set as necessary to review risk models and determine whether they adequately identify risks. Sonatype also periodically updates its built-in policy set to ensure compliance with the latest requirements.

PW 4: Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality

The Sonatype platform ensures that first-party source code is developed securely by leveraging contextual polices and high-quality dependencies

When customers encapsulate functionality into reusable modules, the Sonatype platform supports them by continuously tracking and monitoring these inner source components as if they were third-party dependencies. Sonatype's InnerSource Insight shows open source dependencies brought in by these components, helping developers and security teams quickly identify and remediate concerns. With advanced binary fingerprinting and Sonatype intelligence, the platform identifies safe upgrade paths that won't break builds. Without automation, discovering violations from inner source components is challenging and time-consuming. Sonatype Lifecycle manages component risk with continuous monitoring, quickly informing you of any issues and helping to fix them, thereby promoting the reuse of well-secured software and reducing the need to duplicate functionality.

PW 5: Create Source Code by Adhering to Secure Coding Practices

The Sonatype platform ensures that first-party source code is developed securely by leveraging contextual policies and high-quality dependencies. By integrating with Sonatype's extensive vulnerability database, the platform helps developers select secure libraries and frameworks, and automatically remediates, avoids, and mitigates vulnerabilities. This proactive approach ensures that developers build on a foundation of secure, reliable dependencies, fostering a more secure development practice.

PW 6: Configure the Compilation, Interpreter, and Build Processes to Improve Executable Security

Integrating Sonatype's software composition analysis (SCA) tools like Nexus Lifecycle into the build process, alongside policy enforcement, significantly enhances executable security as outlined in the SSDF's PW 6. Sonatype's SCA tools automatically identify and manage open-source components, flagging vulnerabilities and license compliance issues early in the development cycle. Coupled with Sonatype's policy controls, these integrations ensure that only secure, compliant components are incorporated, reducing the risk of vulnerabilities in the final executable.

Our platform is designed to maximize the security and integrity of the software supply chain throughout the SDLC.

PW 7: Review and/or Analyze Human-Readable Code to Identify Vulnerabilities and Verify Compliance with Security Requirements

Sonatype allows for policy to trigger automatic code review requests via pull or merge request functionalities, as well as self-service code change suggestions for developers in their IDEs. The policy can be modeled after the organization's code review policies and can be automated. Sonatype's policy set can provide points of interaction throughout the stages of the SDLC, enforcing some actions or gating depending on the associated stage and policy. The Sonatype platform also enables complete automated code review and analysis for all third-party dependencies and the entire software supply chain.

PW 8: Test Executable Code to Identify Vulnerabilities and Verify Compliance with Security Requirements

Our unique firewalling capability allows for sandboxing dependencies for malicious code testing, enabling organizations to implement policies for potentially harmful code embedded in binary dependencies. The Sonatype platform is designed to maximize the security and integrity of the software supply chain throughout the SDLC. It is fully compatible with various software testing methodologies, ensuring seamless integration into any stage. Moreover, it supports multiple analysis methods, allowing for the comprehensive identification and resolution of code and dependency issues. This ensures that software remains secure and reliable, regardless of the development methodologies used.

Respond to Vulnerabilities (RV)

RV 1: Identify and Confirm Vulnerabilities on an Ongoing Basis

The Sonatype platform is especially suited for this task. By using Sonatype Lifecycle and Sonatype Repository Firewall, users can automate the review and evaluation process based on policies. This can include architectural considerations and can be repeated on a per-application build basis. Sonatype Nexus Repository Manager, combined with Sonatype Repository Firewall, allows for automatic vetting of newly acquired open source components, including integrity, known vulnerability, licensing, and architectural considerations.

RV 2: Assess, Prioritize, and Remediate Vulnerabilities

The Sonatype platform records known security vulnerabilities and can consume any additional information provided in SBOMs into the system. They can also be exported to

any issue management system for further tracking. Sonatype also integrates with ServiceNow, Splunk, and Jira to ensure easy workflow integration.

RV 3: Analyze Vulnerabilities to Identify Their Root Causes

The Sonatype platform records and provides the root causes of all security vulnerabilities discovered in third-party components.

Secure Software Development Attestation Form and Sonatype

The Secure Software Development Attestation Form requires vendors supplying software to federal entities to certify through a CEO or an authorized designee's signature that their software is developed securely, adhering to the Secure Software Development Framework (SSDF) guidelines established by NIST. The Secure Software Development Attestation form outlines the minimum requirements a software developer must meet – and attest to meeting – before the federal government can use it.

The Sonatype platform simplifies compliance with SSDF requirements and allows complete adherence to these new standards.

Attestation Requirement	Sonatype Capabilities
1) The software is developed and built in secure environments. Those environments are secured by the following actions, at a minimum: a) Separating and protecting each environment involved in developing and building software; b) Regularly logging, monitoring, and auditing trust relationships used for authorization and access: i) to any software development and build environments and ii) among components within each environment; c) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk; d) Taking consistent and reasonable steps to document, as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;	Sonatype can integrate with the most common SSO workflows, as well as token-based authentication for extra security. This allows users to conform to all requirements as they pertain to tooling provided by Sonatype. **Our licensing model does not restrict the Sonatype platform from being deployed as many times as possible in as many networks as needed.** All Sonatype tools are recommended to run in a strictly authenticated mode, which requires each user to authenticate in order to access any features. We recommend deploying the platform using external authentication systems that allow conforming to this requirement. Regarding minimizing access to the internet, Sonatype tools can be used to achieve this in two ways: by allowing developers to access trusted software artifacts from an internal repository and auditing any new incoming components using Sonatype Repository Firewall or by allowing developers to access Sonatype verified and enriched component intelligence. **Each Sonatype policy enforcement activity does not require internet access from the tooling or developer at all—just network access to where the platform is deployed.** Sonatype policy actions can be deployed and enforced in such a way that humans outside of a select group of administrators do not need access. We recommend

e) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk; f) Implementing defensive cybersecurity practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents;	utilizing Sonatype's out-of-the-box build steps provided for most CI and build tools to help design this. **The Sonatype platform can also be used to monitor, detect, and alert to changes in the composition of the software built into the customer's SDLC.** For example, should a piece of software contain a tampered open source library, the Sonatype platform will trigger an alert of this change if continuous scanning is in effect.
2) The software producer makes a good faith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;	**Sonatype Nexus Repository is the industry standard for artifact repositories and has a robust RBAC and privileges-based system that allows for granular access. Additionally, Sonatype Lifecycle and Sonatype Repository Firewall allow for defining the referenced policy, e.g., open source code in development environments must have their integrity verified, or software in QA environments must contain no known security vulnerabilities ranked critical.** Sonatype Nexus Repository Manager allows for versioning and controlling each built artifact and piece of software, as well as storing them for posterity. This allows for conforming to this requirement for binary artifacts. Using continuous monitoring, it's possible to alert software developers or application owners of any new additions to their SBOM, allowing for a review process to take place. **The Sonatype platform is a robust tool designed to enhance the security and integrity of software executables.** The platform ensures authenticity and integrity through a comprehensive system that includes a vast database for verifying open-source signatures, detailed analysis to identify any modifications, inner source elements, known or unknown components within open-source artifacts, and ongoing integrity monitoring. This monitoring is facilitated by an integrity rating feature, alerting users to any changes in the integrity of the open-source components they use. This multifaceted approach allows organizations to confidently utilize open source and inner source components while maintaining their software's security, compliance, and operational reliability.
3) The software producer maintains provenance for internal code and third-party components incorporated into the software to the greatest extent feasible;	This is a core functionality that the policy set shipping with the Sonatype platform provides. **The out-of-the-box policies are compatible with SSDF, PCI, IEC, and other standards and provide a core set of security requirements** that are simple to implement and enforce. These requirements can then be applied to software or SBOMs provided by third-party providers, open source projects, or even internal software projects. The policy set can be exported and communicated with the desired third parties.

	Using the Sonatype platform, software vendors can automatically create SBOMs that provide provenance 5 data and integrity verification mechanisms for all components. Additionally, upon accepting an SBOM from a vendor, it's possible to confirm the provenance and integrity of each component using the Sonatype Intelligence set. The Sonatype platform provides automatic enforcement actions in case of non-compliance of components to the established policy. This can include automatic remediation actions, notifications, and alerting, as well as recommended rectification and remediation actions depending on the type of policy violated. The reporting features of the platform provide a comprehensive view of what is available.
4) The Software producer employed automated tools or comparable processes that check for security vulnerabilities. In Addition: a) The software producer operates these processes on an ongoing basis and, at a minimum, prior to product, version, or update releases b) The software producer has a policy or process to address discovered security vulnerabilities prior to product release; c) The software producer operates a vulnerability disclosure program and accepts, reviews, and addresses disclosed software vulnerabilities in a timely fashion and according to any timelines specified in the vulnerability disclosure program or applicable policies	The Sonatype platform is built on automated scanning and detection of third-party components, including open source, inner source, commercial components, and completely automatic components. Sonatype's wide suite of integrations enables this automatic information gathering to be built across the SDLC. **No additional tools are required for SBOM management and SCA or software supply chain management using Sonatype. Nonetheless, the platform coexists with any other tooling used and can exchange information via SBOMs to APIs, webhooks, or even directly via import/export of SBOMs.** The built-in policy set in the Sonatype platform can automate a bulk of the decision-making on new and historic security vulnerabilities, malicious components, and a host of other issues with the supply chain. Automation in such a way is built on enforcing the automated policy via the user's DevSecOps pipeline. The Sonatype platform ships with a role-based access control system, allowing appropriate privileges to be granted and enforced.

Sonatype's mission is to bring security and speed to open source development and provide organizations with total control of their SDLC. Sonatype supports this by making it easier to enforce security policies automatically, verify third-party compliance, and manage SBOMs that remove the uncertainty of complex and evolving compliance requirements.

To learn more about how the Sonatype platform can help manage software supply chain risk management, contact us today.

sonatype

Sonatype is the leader in software supply chain optimization. Sonatype's platform empowers enterprises to create safer software faster and to protect against the inherent risk from free open source components used to develop modern software applications. As founders of Nexus Repository and stewards of Maven Central, the largest public repository of Java, Sonatype pioneered software supply management and maintains the world's leading knowledge base of open source intelligence for software composition analysis and dependency management.

Sonatype's platform integrates this intelligence with customers' Software Development Lifecycle and delivers reliable automated identification and remediation of vulnerable and malicious open source code while also enabling customers to generate and continuously monitor SBOMs (Software Bill of Materials) to increase their security posture and be prepared for the next zero-day threat or software supply chain attack.

Sonatype is an enabling technology for compliance with NIST SP 800-218, "Secure Software Development Framework (SSDF)" in response to Presidential Executive Order 14028, Section 4, "Enhancing Software Supply Chain Security." More than 2,000 organizations, including 70% of the Fortune 100, fifteen million software developers and hundreds of government customers rely on Sonatype to set and enforce policies for open source governance, and "shift left" to deliver software applications that are secure by design and secure by default. For more information, please visit **Sonatype.com**, or connect with us on **Facebook**, **Twitter/X**, or **LinkedIn**.

Headquarters
8161 Maple Lawn Blvd,
Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High
St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place,
Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com