SmartSuite

Framework / Software Security / NIST Special Publications

NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities

NIST SP 800-218, the SSDF v1.1 (February 3, 2022), sets 19 secure software development practices and 42 tasks in four groups; attestation to it is optional for agencies since OMB M-26-05.



What it is

NIST SP 800-218, the Secure Software Development Framework (SSDF) Version 1.1, is NIST's set of 19 high-level secure software development practices, broken into 42 tasks, that software producers add to whatever software development life cycle (SDLC) model they use. The National Institute of Standards and Technology (NIST) published it on February 3, 2022, superseding the SSDF v1.0 white paper (CSWP 13 of April 23, 2020), in response to Section 4 of Executive Order 14028 of May 12, 2021. It is voluntary: the federal attestation requirement that OMB M-22-18 built on it was rescinded by OMB M-26-05 on January 23, 2026, which keeps the SSDF and CISA's attestation form available as resources agencies may choose to use.

Section 2 arranges the practices in four groups: Prepare the Organization (PO.1 to PO.5), Protect the Software (PS.1 to PS.3), Produce Well-Secured Software (PW.1, PW.2 and PW.4 to PW.9, PW.3 having been folded into PW.4 and PO.1 in this version) and Respond to Vulnerabilities (RV.1 to RV.3). Table 1 gives each practice its tasks, notional implementation examples and informative references to sources such as BSA, OWASP, SAFECode, SP 800-161 Rev. 1 and IEC 62443-4-1. Appendix A maps the subsections of Section 4e of the Executive Order to the practices and tasks that address them (Table 2), and Appendix C is the change log.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION Version 1.1 (SP 800-218, February 2022); Rev. 1 (v1.2) in draft
EFFECTIVE February 3, 2022	DOMAIN Software Security	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY High

Source: csrc.nist.gov/pubs/sp/800/218/final

Why it matters

- **A shared vocabulary** Practice identifiers such as PO.1, PS.3 or RV.2 and task identifiers such as PW.7.1 let a producer, an acquirer and an assessor refer to the same expectation (Table 1).
- **Outcomes, not methods** Section 1 says the SSDF identifies practices but does not prescribe how to implement them, so it fits any SDLC model and toolchain.
- **Shift left by design** Section 1 explains that the earlier security is addressed in the SDLC, the less effort and cost the same level of security requires, and the practices start with the organization before any code is written.
- **Traceable to the Executive Order** Appendix A Table 2 shows which practices and tasks address each subsection of Section 4e of EO 14028, the basis of the government's secure software work.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-218 SSDF

Practice and Task Register

Load PO.1 to RV.3 and their 42 tasks from Table 1 as linked records, each with its purpose, the organization's implementation statement and the environment names the organization has defined.

Security Requirements Record

Keep the security requirements for organization-developed software (PO.1.2) and the design decisions, risks and requirements tracked for each product (PW.1.2) as records tied to the software they govern.

Release Archive and Provenance

Record each release, its integrity verification mechanism (PS.2) and the provenance data collected for its components (PS.3.2), with the archive location required by PS.3.

Vulnerability Response Workflow

Use Cyber & IT Risk to run RV.1 identification, RV.2 assessment, prioritization and remediation and RV.3 root-cause analysis, with owners, dates and the practice each fix feeds back into.

Supplier Attestations

Use Third Party Risk Management to hold suppliers' SSDF statements and any attestation form or SBOM an agreement requires, mapped to the practices they cover.

Reporting by Practice Group

Dashboards summarize implementation status and open vulnerabilities by PO, PS, PW and RV, and show which EO 14028 Section 4e subsections (Appendix A) are covered.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | MITRE ATT&CK | NIST CSF 2.0 | NIST SP 800-160 Vol. 1 Rev. 1 | NIST 800-53 Rev.5 | OWASP ASVS 4.0

Official resources

NIST SP 800-218, Secure Software Development Framework (SSDF)

Provides practices for integrating security into the software development lifecycle.

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

NIST SP 800-53, Security and Privacy Controls for Information Systems

Outlines security controls that align with secure software development processes.

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST Cybersecurity Framework

Describes common policies to improve cybersecurity risk management.

nist.gov/cyberframework

Frequently asked questions

What are the four practice groups in NIST SP 800-218, and how many practices and tasks are there?

Prepare the Organization (PO.1 to PO.5), Protect the Software (PS.1 to PS.3), Produce Well-Secured Software (PW.1, PW.2 and PW.4 to PW.9) and Respond to Vulnerabilities (RV.1 to RV.3), which is 19 practices (Section 2 and Table 1). Table 1 lists 42 active tasks; five task identifiers from version 1.0 (PW.3.1, PW.3.2, PW.4.3, PW.4.5 and PW.5.2) are shown as moved into other tasks.

Do federal software suppliers still have to attest to the SSDF?

Not by government-wide mandate. OMB M-22-18 and its companion M-23-16 required agencies to obtain attestations against SP 800-218, and OMB M-26-05 rescinded both on January 23, 2026. M-26-05 tells agencies to maintain a complete inventory of software and hardware and to set assurance policies that match their risk determinations, and says they may still use the Secure Software Development Attestation Form and may require a software bill of materials by contract. Individual agencies can therefore still ask for one.

 © 2026 SmartSuite Inc. All rights reserved.

What changed from SSDF version 1.0 to version 1.1?

Version 1.1 added practice PO.5 on implementing and maintaining secure environments for software development, and tasks PO.1.2 on documenting security requirements for organization-developed software, PS.3.2 on collecting and sharing provenance data for release components, and PW.1.2 on tracking security requirements, risks and design decisions. Practice PW.3 was removed, its tasks moving to PO.1.3 and PW.4.4, and Appendix C holds the full change log. Version 1.0 was published as white paper CSWP 13 on April 23, 2020.

Is there a newer version of the SSDF than 1.1?

Not a final one. NIST published the initial public draft of SP 800-218 Rev. 1, Secure Software Development Framework Version 1.2, on December 17, 2025, and the comment period closed on January 30, 2026; the SSDF project page still lists version 1.1 as the final publication. Separately, SP 800-218A of July 26, 2024 is a final community profile that augments the SSDF for generative AI and dual-use foundation model development.

How does NIST SP 800-218 relate to Executive Order 14028?

Section 4 of Executive Order 14028 of May 12, 2021 directed NIST to identify or develop standards and practices for software supply chain security, and NIST updated the SSDF to version 1.1 after a June 2021 workshop and more than 150 position papers. Appendix A Table 2 maps each subsection of Section 4e of the Order to the SSDF practices and tasks that address it, which is how the later attestation program and CISA's attestation form were built on the publication.

License included / downloadable: Yes NIST SP 800-218 is free of charge from NIST, with Table 1 also published as a spreadsheet on the CSRC record.

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-218-secure-software-development-framework-ssdf

© 2026 SmartSuite Inc. All rights reserved.