SmartSuite

Framework / Software Security / Other

CISA Secure Software Development Attestation Form (SSDAF)

CISA's Secure Software Development Attestation Form lets producers attest to four SSDF-based practices; OMB M-26-05 made agency use optional in January 2026.



What it is

The CISA Secure Software Development Attestation Form, also called the Self Attestation Common Form (version 1.0, released March 11, 2024), is the government-wide form with which a software producer tells a federal agency that it follows secure development practices drawn from NIST SP 800-218, the Secure Software Development Framework (SSDF). OMB memorandum M-26-05 of January 23, 2026 rescinded the memos that required agencies to collect it, so agencies now choose whether to ask for it.

CISA developed the form with the Office of Management and Budget (OMB) under Executive Order 14028 and OMB memorandum M-22-18 (September 14, 2022), as amended by M-23-16 (June 9, 2023). The form carries OMB control number 1670-0052, expiring March 31, 2027. Under M-26-05 each agency head is responsible for validating the security of software on the agency's network, and agencies may use the form or require a software bill of materials (SBOM) on request.

At a glance

PUBLISHER Cybersecurity and Infrastructure Security Agency (CISA)	TYPE Guidance	VERSION Common Form v1.0 (OMB 1670-0052, expires March 31, 2027); agency use optional under OMB M-26-05
EFFECTIVE March 11, 2024; optional for agencies since January 23, 2026	DOMAIN Software Security	FAMILY Other
REGION United States	ADOPTION MODEL Industry Requirement	IMPLEMENTATION COMPLEXITY Moderate

Source: cisa.gov/resources-tools/resources/secure-software-development-attestation-form

Why it matters

- **One common form** Agencies share one form rather than each writing its own, and agency-specific requirements go in an addendum (form instructions).
- **A defined scope** Software needs an attestation if it was developed after September 14, 2022, had a major version change after that date, or receives continuous changes, as software-as-a-service does.
- **Binding on future versions** An attestation covers future versions of the named product until the producer notifies agencies that its practices no longer conform.
- **A third-party route** A FedRAMP-certified or agency-approved Third Party Assessor Organization (3PAO) can assess conformance instead of a CEO signature.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CISA SSDAF

Attestation Register

Record each attestation by product, version, attestation type, signatory, date and agency, with the 3PAO option noted where used.

Practice Evidence Library

Link evidence to the four practice areas: environment controls, source code supply chain, provenance and vulnerability checks.

Vulnerability Disclosure and Remediation

Track disclosed vulnerabilities and fixes against the producer's disclosure program and pre-release policy (practice 4).

Third-Party Component Records

Keep third-party component, vendor attestation and SBOM records that support practices 2 and 3.

POA&M and Lapse Tracking

Track any practice not met, its mitigations and plan of action and milestones, and the duty to notify agencies if practices lapse.

Agency Request Reporting

Report which agency requests, products and versions have current attestations and which are due for update.

Common framework mappings

CIS Controls v8.1 | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST SP 800-161 Rev.1 | NIST 800-218 SSDF | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

CISA Secure Software Development Attestation Form

CISA's page for the Common Form: the form and instructions (English and Spanish) and the note that agencies may use it under OMB M-26-05.

cisa.gov/resources-tools/resources/secure-software-development-attestation-form

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

NIST's secure software development practices (version 1.1) on which the attestation form is based.

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

OMB M-26-05: Adopting a Risk-based Approach to Software and Hardware Security

The January 23, 2026 OMB memorandum that rescinded M-22-18 and M-23-16 and made agency use of the Common Form optional.

whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf

Frequently asked questions

What is the CISA Secure Software Development Attestation Form?

It is the Self Attestation Common Form (version 1.0, OMB control number 1670-0052) that CISA released with OMB on March 11, 2024. A software producer uses it to attest to a federal agency that its software is developed using secure practices derived from NIST SP 800-218 (SSDF). It has three sections, and Section III holds the attestation and signature.

Is the attestation form still required?

No longer by OMB. Memorandum M-26-05 of January 23, 2026 rescinded M-22-18 and M-23-16, which required agencies to collect it. Agencies may still choose to use the form and may add contract terms such as a software bill of materials on request, so producers can still be asked for it.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Which software needs a self-attestation?

Software needs the attestation if it was developed after September 14, 2022, if older software had a major version change after that date, or if the producer delivers continuous changes, as software-as-a-service does. Software developed by agencies, open source freely obtained by an agency, incorporated third-party components and freely obtained public software are out of scope.

Who signs the form and what are the alternatives?

The chief executive officer or a designee who is an employee with authority to bind the company signs Section III. The producer can instead attach an assessment by a FedRAMP-certified or agency-approved Third Party Assessor Organization (3PAO) and check the box, with no signature. Willfully false statements may violate 18 U.S.C. 1001.

How does the form relate to NIST SP 800-218?

The four practice areas are derived from the Secure Software Development Framework, version 1.1, and the form's appendix maps each statement to SSDF tasks and to Executive Order 14028 section 4(e). NIST released an initial public draft of SP 800-218 Rev. 1 (SSDF 1.2) on December 17, 2025, but the form still cites version 1.1.

License included / downloadable: Yes CISA publishes the form and its instructions as a free public PDF in English and Spanish, and they are included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/cisa-secure-software-development-attestation-form-ssdaf