Department of Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Secure Software Development Attestation Form Instructions

Read all instructions before completing this form

Privacy Act Statement

[NOTE: *This Privacy Act Statement is unique to DHS. All agencies using this common form will need to provide an agency-unique Privacy Act Statement when they request to use this form. Each agency using this common form should provide Privacy Act Statements that conform to its applicable agency procedures and requirements.*]

Authority: 44 U.S.C. § 3554, Executive Order (E.O.) 14028, "Improving the Nation's Cybersecurity," and OMB Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices," as amended by OMB Memorandum M-23-16, "Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices," authorize the collection of this information.

Purpose: The purpose of this form is to provide the Federal Government assurances that software used by agencies is securely developed.

Background: This information may be disclosed as generally permitted under Executive Order 14028, Improving the Nation's Cybersecurity (E.O. 14028) and Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (M-22-18), as amended. This form collects contact information from vendor employees who make the attestation. For DHS, information may be disclosed as necessary and authorized by the routine uses published in DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other List System, November 25, 2008, 73 FR 71659.

Failure to provide any of the information requested may result in the agency no longer utilizing the software at issue. Willfully providing false or misleading information may constitute a violation of 18 U.S.C. § 1001, a criminal statute.

What is the Purpose of Filling out this Form?

The Federal Information Security Modernization Act of 2014 (FISMA) requires each Federal agency to provide security protections for both "information collected or maintained by or on behalf of an agency" and for "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." FISMA and other provisions of Federal law authorize the Director of the Office of Management and Budget (OMB) to promulgate information security standards for information security systems, including to ensure compliance with standards promulgated by the National Institute of Standards and Technology (NIST).

Executive Order 14028, "Improving the Nation's Cybersecurity" (E.O. 14028), emphasizes the importance of securing software used by the Federal Government to perform its critical functions. To further this objective, E.O. 14028 required NIST to issue guidance "identifying practices that enhance the security of the software supply chain."[1] The NIST Secure Software Development Framework (SSDF) (SP 800-218),[2] and the NIST Software Supply Chain Security Guidance[3] (these two documents, taken together, are hereinafter referred to as "NIST Guidance") include a set of practices that create the foundation for developing secure software.

E.O. 14028 further requires that the Director of OMB take appropriate steps to ensure that Federal agencies comply with NIST Guidance. To that end, OMB issued Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (M-22-18), on September 14, 2022. That memorandum was updated on June 9, 2023, through OMB Memorandum M-23-16, "Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (M-23-16). M-22-18, as amended by M-23-16, provides that a Federal agency may use software subject to M-22-18's requirements only if the producer of that software has first attested to compliance with Federal Government-specified secure software development practices drawn from the SSDF.

This self-attestation form identifies the minimum secure software development requirements a software producer must meet, and attest to meeting, before software subject to the requirements of M-22-18 and M-23-16 may be used by Federal agencies. This form is used by software producers to attest that the software they produce is developed in conformity with specified secure software development practices.

Software requires self-attestation if any of the conditions is met:

1. The software was developed after September 14, 2022;
2. The software was developed prior to September 14, 2022, but was modified by major version changes (e.g., using a semantic versioning schema of Major.Minor.Patch, the software version number goes from 2.5 to 3.0) after September 14, 2022; or

[1] Executive Order on Improving the Nation's Cybersecurity (E.O. 14028), Section 4(e).
[2] Available at: https://csrc.nist.gov/Projects/ssdf
[3] Available at: https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidanceunder-EO-14028-section-4e.pdf

3. The producer delivers continuous changes to the software code (as is the case for software-as-a-service products or other products using continuous delivery/continuous deployment).

Software products and components in the following categories are not in scope for M-22-18, as amended by M-23-16, and do not require a self-attestation:

1. Software developed by Federal agencies;
2. Open-source software that is freely and directly obtained by a Federal agency;
3. Third-party open source and proprietary components that are incorporated into the software end product used by the agency; or
4. Software that is freely obtained and publicly available.

Software producers who utilize third party components in their software are required to attest that they have taken specific steps, detailed in "Section III – Attestation and Signature" of the common form, to minimize the risks of relying on such components in their products.

Agency-specific instructions may be provided to the software producer outside of this common form. Conformance to agency-specific requirements may be included with this form as an addendum; agencies are responsible for fulfilling any Paperwork Reduction Act requirements applicable to agency-specific additions.

If a software producer is unable to submit via the online form, they may email a pdf version of the form to the respective agency:
Online Form Instructions:

- ☐ Selecting the provided URL: https://softwaresecurity.cisa.gov

OR

Local PDF Instructions:

- ☐ Saving the completed form as a PDF using the following naming convention:
  Software Producer: Software Producers name which manufactured/compiled the software product
  Product name: Complete name of software product
  Version: Version number of software product
  Attestation date: Date the software product was attested:
  e.g. [Software Producer]_[Product]_[Version]_[Attestation Date]
  →Acme_SecuritySuite_4.6.2.1_20230124
  Individual agencies will provide their respective email addresses.

Filling Out the Form

Software Producer Information
Please provide a description of the software and information about the software producer. All fields in the attestation form are required to be appropriately completed by the software producer. Incomplete forms will not be accepted.

The form must be signed by the Chief Executive Officer (CEO) of the software producer or their designee, who must be an employee of the software producer and have the authority to bind the corporation. By signing, that individual attests that the software in question is developed in conformity with the secure software development practices delineated within this form. The software may be used by a federal agency, consistent with the requirements of M-22-18, as amended by M-23-16, once the agency has received an appropriately signed copy of the attestation form.

The software producer may choose to demonstrate conformance with the minimum requirements by submitting a third-party assessment documenting that conformance. A third-party assessment must be performed by a Third Party Assessor Organization (3PAO) that has either been FedRAMP certified or approved in writing by an appropriate agency official. The 3PAO must use relevant NIST Guidance that includes all elements outlined in this form as part of the assessment baseline. To rely upon a third-party assessment, the software producer must check the appropriate box in Section III and attach the assessment to the form. The producer need not sign the form in this instance. The agency shall take appropriate steps to ensure that the assessment is not posted publicly, either by the vendor or by the agency itself.

Additional Information:
In the event that an agency cannot obtain a completed self-attestation from the software producer, an agency may still decide to use the producer's software if the producer identifies the practices to which they cannot attest, documents practices they have in place to mitigate associated risks, and submits a plan of actions and milestones (POA&M) to the agency. When an attestation is not provided, per OMB guidance, agencies are responsible for requesting from OMB an extension or waiver for the continued use.

This common self-attestation form fulfills the minimum requirements set forth by OMB in M-22-18, as amended by M-23-16.

The attestation form, background, and instructions are subject to change and may be modified.

Secure Software Development Attestation Form
Version 1.0

Section I

☐ **New Attestation** ☐ **Attestation Following Extension or Waiver** ☐ **Revised Attestation**

Type of Attestation: ☐ Company-wide ☐ Individual Product ☐ Multiple Products or Specific Product Version(s) (please provide complete list)

If this attestation is for an individual product or multiple products, provide the software name, version number, and release/publish date to which this attestation applies. Additional pages can be attached to this attestation if more lines are needed:

Product(s) Name	Version Number[4] (if applicable)	Release/Publish Date (if applicable)
		YYYY-MM-DD

For the above specified software, this form does not cover software or any components of that software that fall into the following categories:

1. Software developed by Federal agencies;
2. Open source software that is freely and directly obtained directly by a Federal agency;
3. Third-party open source and proprietary components that are incorporated into the software end product used by the agency; or
4. Software that is freely obtained and publicly available.

Note: In signing this attestation, software producers are attesting to adhering to the secure software development practices outlined in Section III for code developed by the producer.

Section II

1. Software Producer Information
Company Name:
Address:
City:

[4] Attestations are binding for future versions of the named software product unless and until the software producer notifies the agencies to which it previously submitted the form that its development practices no longer conform to the required elements specified in the attestation.

State or Province:
Postal Code:
Country:
Company Website:

2. Primary Contact for this Document and Related Information (may be an individual, role, or group):
Name:
Title:
Address:
Phone Number:
Email Address (may be an alias/distribution list):

Section III

Attestation and Signature

On behalf of the above-specified company, I attest that, to the best of my knowledge, [software producer] presently makes consistent use of the following practices, derived from the secure software development framework (SSDF),[5] in developing the software identified in Section I:

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

[5] The SSDF are standards and best practices established by the National Institute of Standards and Technology (NIST) in NIST Special Publication (SP) 800-218.

build software;

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;

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;

3) The software producer maintains provenance for internal code and third-party components incorporated into the software to the greatest extent feasible;

4) The software producer employs automated tools or comparable processes that check for security vulnerabilities. In addition:
   a) The software producer operates these processes on an ongoing basis and 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; and
   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.

☐ I further attest that the software producer will notify any agency to which it has submitted this form if and when the producer ceases to make consistent use of the practices identified above in developing the software.

Signature of CEO or Designee with authority to bind the corporation

_____

Date (YYYY-MM-DD): _____
Name:
Title:

OR

☐ A certified FedRAMP Third Party Assessor Organization (3PAO) or other 3PAO approved in writing by an appropriate agency official has evaluated our conformance to all elements in this form. The 3PAO used relevant NIST Guidance that includes all elements outlined in this form as the assessment baseline. The assessment is attached.

ATTACHMENT(S):

- **[Artifact/Addendum Title]:** [Artifact/Addendum Description]

Burden Statement

The public reporting burden to complete this information collection is estimated at **3 hours and 20 minutes** per response, including time for reviewing instructions, searching data sources, gathering, and maintaining the data needed, and completing and reviewing the collection of information. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection information, including suggestions for reducing this burden, to DHS/CISA **CSCRM@cisa.dhs.gov.**

APPENDIX
REFERENCES

Minimum Attestation References:
The minimum requirements within the Secure Software Attestation Form address requirements put forth in E.O. 14028 subsection (4)(e). A mapping to specific SSDF practices and tasks is provided for reference purposes.

Attestation Requirements	**Related E.O. 14028 Subsection**		**Related SSDF Practices and Tasks**
1) The software is developed and built in secure environments. Those environments are secured by the following actions, at a minimum:	4e(i)		[See rows below]
a) Separating and protecting each environment involved in developing and building software;	4e(i)(A)		PO.5.1
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;	4e(i)(B)		PO.5.1
c) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk;	4e(i)(C)		PO.5.1, PO.5.2
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;	4e(i)(D)		PO.5.1
e) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk;	4e(i)(E)		PO.5.2
f) Implementing defensive cybersecurity practices, including continuous monitoring of operations and alerts and, as necessary,	4e(i)(F)		PO.3.2, PO.3.3, PO.5.1, PO.5.2

responding to suspected and confirmed cyber incidents;			
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;	4e(iii)		PO 1.1, PO.3.1, PO.3.2, PO.5.1, PO.5.2, PS.1.1, PS.2.1, PS.3.1, PW.4.1, PW.4.4, PW 7.1, PW 8.1, RV 1.1
3) The software producer maintains provenance for internal code and third-party components incorporated into the software to the greatest extent feasible;	4e(vi)		PO.1.3, PO.3.2, PO.5.1, PO.5.2, PS.3.1, PS.3.2, PW.4.1, PW.4.4, RV.1.1, RV.1.2
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 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; and 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.	4e(iv)		PO.4.1, PO.4.2, PS.1.1, PW.2.1, PW.4.4, PW.5.1, PW.6.1, PW.6.2, PW.7.1, PW.7.2, PW.8.2, PW.9.1, PW.9.2, RV.1.1, RV.1.2, RV.1.3, RV.2.1, RV.2.2, RV.3.3