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

Authority: 44 U.S.C. § 3554, Executive Order (EO) 14028, Improving the Nation's Cybersecurity, and Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (M-22-18) 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.

Routine Uses: This information may be disclosed as generally permitted under Executive Order 14028, Improving the Nation's Cybersecurity (EO 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 includes using information as necessary and authorized by the routine uses published in [applicable agency SORN].

Disclosure: Providing this information is mandatory. 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* (EO 14028), emphasizes the importance of securing software used by the Federal Government to perform its critical functions. To further this objective, EO 14028 required the NIST to develop standards, tools, and best practices to enhance the security of the software supply chain; these are captured in the "Secure Software Development Framework" (SSDF) (NIST SP 800-218). [1] EO 14028 further requires that the Director of OMB take appropriate steps to ensure that Federal agencies comply with NIST guidance and standards regarding the SSDF. 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. The memorandum provides that a Federal agency may use software subject to M-22-18's requirements[2] 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 their software subject to the requirements of M-22-18 may be used by Federal agencies. This form is used by software producers to attest that the software they produce was developed in conformity with specified secure software development practices.

The following software requires self-attestation:

1. Software developed after September 14, 2022;
2. Existing software that is 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; and
3. Software to which the producer delivers continuous changes to the software code (such as 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 and do not require a self-attestation:

1. Software developed by Federal agencies; and
2. Software that is freely obtained (e.g. freeware, open source) directly by a federal agency.

Software producers who utilize freely obtained elements 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 software 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

[1] Secure Software Development Framework (SSDF) Version 1.1, https://csrc.nist.gov/publications/detail/sp/800-218/final

[2] See page 2 of M-22-18 for a description of the software subject to the memorandum's requirements.

addendum.

Software producers can submit this form by:
Online Form Instructions:

- Downloading and completing the fillable form at **<URL to be provided prior to release>**
- Clicking the submit button at the bottom of the last page

OR

Local PDF Instructions:

- Saving the completed form as a PDF using the following file format
  Software Producer: Software Producers name which manufactured/compiled the software product
  Product or Product Line name: Complete name of software product or product line
  Version: Version number of software product
  Attestation date: Date the software product was attested:
  e.g. [Software Producer]_[Product/Product Line Name]_[Version]_[Attestation Date] →Acme_SecuritySuite_4.6.2.1_20230124
- Emailing the completed PDF to **< EMAIL to be provided prior to final release >**

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 of the software producer or their designee, who must be an employee of the software producer. By signing, that individual attests that the software in question was developed in conformity with the secure software development practices delineated within the form. The software may be used by a Federal agency, consistent with the requirements of M-22-18, once the agency has received an appropriately signed copy of the form.

This form may be completed in a digital format located on the agency website or by emailing the completed PDF to the appropriate agency contact.

Additional Information:
In the event that an agency cannot obtain a completed self-attestation from the software producer(s), an agency seeking to use the producer's software must obtain documentation from the software producer identifying the practice(s) to which they cannot attest, document practices the agency has in place to mitigate resulting risks, and require a plan of actions and milestones (POA&M) to be developed from the software producer. Further guidance on extension and waiver requests for agencies can be found on the relevant MAX page, along with agency guidance on the collection of POA&Ms.

This common self-attestation form fulfills the minimum requirements set forth by the Office of Management and Budget in M-22-18. Software producers may be asked by agencies to provide additional attestation artifacts or documentation, such as a Software Bill of Materials (SBOMs) or documentation from a third-party assessor, beyond what is required by this common form. Establishing and maintaining processes for producing and maintaining a current SBOM may be utilized by the software producer as a means of documenting compliance with certain minimum requirements. Agencies that choose to require additional artifacts or documentation beyond the self-attestation form may instruct the software producer to maintain those additional elements among its own records, or to attach them to the self-attestation form, with the title and contents of the relevant addenda delineated below the signature line. The artifact may be maintained and updated by the software producer for the agency at a designated internet accessible location. Pursuant to M-22-18, any SBOMs submitted must be generated in one of the data formats defined in the National Telecommunications and Information Administration (NTIA) report "The Minimum Elements For a Software Bill of Materials (SBOM)."

If the relevant software has been verified by a certified FedRAMP third party assessor organization (3PAO) or other 3PAO approved in writing by an appropriate agency official, and the assessor used relevant NIST guidance, the software producer does not need to submit an attestation. However, relevant documentation from the 3PAO is required.

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

Minimum Attestation References:
The minimum requirements within the Secure Software Attestation Form address requirements put forth in EO 14028 subsection (4)(e) and specific SSDF practices and tasks. For reference, please review the chart below.

Attestation Requirements	**Related EO 14028 Subsection**	**Related SSDF Practices and Tasks**

1) The software was developed and built in secure environments. Those environments were 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 cyber security practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents;	4e(i)(F)	PO.3.2, PO.3.3, PO.5.1, PO.5.2
2) The software producer has made a good-faith effort to maintain trusted source code supply chains by: a) Employing automated tools or comparable processes; and b) Establishing a process that includes reasonable steps to address the security of 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 data for internal and third-party code incorporated into the software;	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:	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,

a) The software producer ensured these processes operate on an ongoing basis and, at a minimum, prior to product, version, or update releases and 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.		RV.1.1, RV.1.2, RV.1.3, RV.2.1, RV.2.2, RV.3.3

Secure Software Development Attestation Form

Section I

[ ] New Attestation [ ] Attestation Following Extension or Waiver

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

If this attestation is for an individual product, multiple products, or product line, provide the software name, version number, and release/publish date to which this attestation applies:

Product(s) or Product Line Name	Version Number (if applicable)	Release/Publish Date
		YYYY-MM-DD

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

1. Software developed by federal agencies; or
2. Software that is freely obtained (e.g., freeware, open source) directly by a federal agency

Note: In signing this attestation, software producers are attesting to the secure development of code developed by the producer.

Section II

1. Software Producer Information
Company Name:
Address:
City:
State or Province:
Postal Code:
Country:
Company Website:

2. Primary Contact for this Document and Related Information (may be an individual, role, or group):
First Name:
Last 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 [software producer] presently makes consistent use of the following practices, drawn from the secure software development framework (SSDF),[3] 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 minimized 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;

    e) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk;

    f) Implementing defensive cyber security practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents;

2) The software producer has made a good-faith effort to maintain trusted source code supply chains by:
    a) Employing automated tools or comparable processes; and

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

b) Establishing a process that includes reasonable steps to address the security of third-party components and manage related vulnerabilities;

3) The software producer employs automated tools or comparable processes in a good-faith effort to maintain trusted source code supply chains;

4) The software producer maintains provenance data for internal and third-party code incorporated into the software;

5) The software producer employs automated tools or comparable processes that check for security vulnerabilities. In addition:
   a) The software producer ensures these processes operate on an ongoing basis and, at a minimum, prior to product, version, or update releases; and
   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.

I attest that all requirements outlined above are consistently maintained and satisfied. I further attest the company will notify all impacted agencies if conformance to any element of this attestation is no longer valid.

Please check the appropriate boxes below, if applicable:

- ☐ There are addendums and/or artifacts attached to this self-attestation form, the title and contents of which are delineated below the signature line.
- ☐ I attest that the referenced software has been verified by a certified FedRAMP Third Party Assessor Organization (3PAO) or other 3PAO approved by an appropriate agency official, and the Assessor used relevant NIST Guidance, which includes all elements outlined in this form, as the assessment baseline. Relevant documentation is attached.

Signature and Date (YYYY-MM-DD): _____ **<note this form will be digitally signed>**

Title of Individual signing on behalf of the organization _____

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 the completing and reviewing the collected 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/Cybersecurity and Infrastructure Security Agency (CISA) **CSCRM_PMO@cisa.dhs.gov**

ATTACHMENTS:

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