Cybersecurity Coalition

December 15, 2023

Robert J. Costello
Chief Information Officer, Department of Homeland Security,
Cybersecurity and Infrastructure Security Agency

VIA ELECTRONIC SUBMISSION

Re: Request for Comment on Secure Software Development Attestation Common Form

Dear Mr. Costello:

The Cybersecurity Coalition ("Coalition") appreciates the opportunity to submit comments to the Cybersecurity and Infrastructure Security Agency (CISA) regarding our concerns with its draft Secure Software Development Attestation Common Form ("Form"), released on November 16, 2023. We hope that the issues detailed below will lead to further clarification and revision so that the underlying intent of the secure software self-attestation can be adequately complied with by industry. Thank you for continued willingness to collaborate on this issue.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services, who are dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace and effective policy environment that will encourage companies of all sizes to take steps to improve cybersecurity risk management.

We would like to highlight the following recommendations concerning the form:

1. Clarify Provenance Definition

The Form includes an attestation that "the software producer maintains provenance for internal code and third-party components incorporated into the software." There is no definition of the term "provenance" in the Form.

The Form references the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF),[1] which in turn references NIST SP 800-53 Revision 5.[2] Therefore, software producers may interpret "provenance" in the Form as having the NIST SP 800-53 definition: "The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include the personnel and

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

processes used to interact with or make modifications to the system, component, or associated data." The Coalition believes that, using this definition of provenance, software producers would be unable to attest for any product that includes open-source components.

Therefore, the Coalition recommends that CISA revise the Form to state that the software producer has made a "good-faith effort" to maintain provenance data. The Coalition also recommends CISA clarify that maintaining "provenance" means, "if the software producer uses a third-party library (proprietary or open-source components), they will need to keep information about attributes of the acquired library in addition to when and where it was retrieved."

As a longer-term solution, the Coalition also recommends NIST revise the definition for provenance included in SP 800-53 to state: "The chronology, *if available,* of the origin, development, ownership, ~~location,~~ and changes to a system or system component and associated data. It may also include *location, as well as* the personnel and processes used to interact with or make modifications to the system component, or associated data*. Provenance must be captured as events occur, and thus some or all of the elements may not exist for a system, component, or associated data.*"

2. Provide CEO Authority to Delegate Signature of the Form

The Coalition believes that requiring either a Chief Executive Officer (CEO) or Chief Operating Officer (COO) to sign the Form will pose an undue burden to software producers.

The Coalition appreciates the intent to build executive buy-in and accountability on implementing secure-by-design principles in software development. However, large companies have varied product lines and will likely need numerous Forms to cover all the products sold to the government. The requirement to have each Form signed by the CEO will create an additional and unnecessary burden for companies.

Therefore, the Coalition recommends CISA allow CEOs to identify appropriate designees to sign the form on behalf of their organization. This would ensure that the software producer can deliver the Form in a timely and accurate manner. CISA could impose a requirement that such delegations are made in writing by the CEO in order to ensure accountability.

3. Requirement to Notify Impacted Agencies of Changes to the Form

The Coalition believes that the Form's requirement to notify "all impacted" agencies of changes to their attestation is not feasible. Software producers should only be required to inform agencies with whom they have a contractual relationship for the software of any changes to the attestation form. Government agencies may use the software producer's products to provide information or shared services to other agencies without the software producer's knowledge. It is unreasonable to expect the software producer to be aware of such agreements and know every agency which may be using or impacted by their software.

Therefore, the Coalition recommends that CISA change the second sentence in the statement to read as follows: "I further attest the company will notify agencies with whom they have a contract, if conformance to any element of this attestation is no longer valid."

4. Consistency of Attestation Requirements

The Coalition believes there are inconsistencies with each of the attestation form requirements. In one instance the attestation is that the "software producer has made a good-faith effort," while in other instances it is that the "software producer maintains." The Coalition recommends that CISA add consistency to the requirements for each attestation requirement.

The Coalition suggests adding the phrase "takes reasonable steps to consistently maintain and satisfy the following" to the statement preceding the attestation requirements.

5. Establish More Realistic Burden Estimates

The Coalition believes that the Burden Statement included in the Form unduly minimizes the impact this attestation process will have on software suppliers to federal agencies.

The Coalition argues that CISA's estimate that the burden to complete necessary information collection is only 3 hours and 20 minutes substantially understates the time associated with completing the self-attestation, even by software producers who are currently adhering to secure development processes. Before signing the Form or creating a POA&M, software producers will need to collect data, conduct manual code reviews, review logs, work with suppliers to collect provenance information, and review the data with leadership. Moreover, the fact this form could be used as evidence in a False Claims Act case from the Department of Justice, corporate legal counsels, Chief Legal Officers, and Corporate Risk Officers will require significant levels of review before the Form can be signed. Accordingly, the Coalition believes that the time for legal review will increase the overall burden on software producers.

While the Coalition acknowledges that the overall cost of compliance will decrease as software producers continue to implement best practices over time, we believe the Form will still take far more than 3 hours and 20 minutes to complete. Coalition members have indicated the burden of completing these tasks could range from 200 to 1,000 hours per product. Large companies will likely need to complete multiple forms, further increasing the total burden of completing self-attestations. Therefore, the Coalition recommends revising the amount of time it estimates software producers will need to complete the Form.

6. Address PDF Naming Conventions

The Coalition believes that the "Local PDF Instructions" on Page 3 of the Form may not function well depending on how the software producer fills out Section I of the Form on Page 5.

The Coalition would highlight that, if the software producer selects a "Company-wide" attestation, there would be no "product name" or "version number" to include. Similarly, if the software producer selects a "Multiple Products or Specific Product Version(s)" attestation, there would be multiple entries for "product name" and "version number."

Therefore, the Coalition recommends clarifying the PDF naming conventions to account for these situations.

In addition to the comments above, we have enclosed a redline version of the Secure Software Development Self-Attestation Form that implements these suggestions.

The Cybersecurity Coalition appreciates the ability to submit these comments for CISA's consideration. As the conversation around this topic continues to evolve, we would welcome the opportunity to further serve as a resource on both technical and policy questions to ensure that the secure software self-attestation process strikes the right balance between effectiveness and efficiency for both the public and private sector.

Respectfully submitted,

The Cybersecurity Coalition

Enclosure: Redline Secure Software Development Self-Attestation Form

Department of Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Secure Software Development Attestation Form

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" (E.O. 14028), 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 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-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.

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 whose code the producer delivers continuous changes (such as software-asa-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; and

[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-securityguidanceunder-EO-14028-section-4e.pdf

3. 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 addressed using an addendum to the form.

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 name(s): Complete name of software product(s) or product line. If the software producer is attesting for multiple products or product lines, it should separate the product or product line names with an ampersand (&). If the software producer is attesting for the entire company, it should write "Company Wide" in this field.
~~**Version: Version number of software product**~~
Attestation date: Date the software product was attested:
e.g. [Software Producer]_[Product(s)]_~~[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 (CEO)~~ or Chief Operating Officer (COO)~~ of the software producer, or their designee. If the form is signed by a designee, such designation must be made in writing by the CEO. The signatory must be an employee of the software producer. By signing, that individual attests that the software in question is 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, as amended by M-23-16, once the agency has received an appropriately signed copy of the form.

The software producer may choose to demonstrate conformance with the minimum requirements by submitting a third-party assessment documenting that conformance. The 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.

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, 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 M22-18, as amended by M-23-16. 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 certified FedRAMP third party assessor organization (3PAO) or other 3PAO approved in writing by an appropriate agency official, 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. 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)."

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, multiple products, or product line, 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 (if applicable)	Release/Publish Date (if applicable)
		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;
2. Open source software that is freely and directly obtained directly by a Federal agency; or
3. 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.

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):

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 takes reasonable steps to consistently maintain and satisfy~~makes consistent use of~~ the following practices, derived from the secure software development framework (SSDF),[4] 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 build software;

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

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

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 has made 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 has made a good faith effort to maintain~~s~~ provenance[5] for internal code and third-party components incorporated into the software;

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, 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; 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.

To the best of my knowledge, I attest that the software producer has taken reasonable steps to consistently maintain and satisfy ~~all~~ requirements outlined above ~~are consistently maintained and satisfied~~. I further attest the company will notify ~~all impacted~~ agencies whom they have a contract with, if conformance to any element of this attestation is no longer valid.

Signature of CEO or ~~COO~~ designee and Date (YYYY-MM-DD):
_____ **<note this form will be digitally signed>**

OR

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

ATTACHMENT(S):

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

[5] Meaning that if the software producer uses a third-party library (proprietary or open source), they will need to keep information about attributes of the acquired library in addition to when and where it was retrieved.

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.**

APPENDIX
REFERENCES

Minimum Attestation References:

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

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:	4(e)(i)	[See rows below]
a) Separating and protecting each environment involved in developing and building software;	4(e)(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;	4(e)(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;	4(e)(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;	4(e)(i)(D)	PO.5.1
e) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk;	4(e)(i)(E)	PO.5.2
f) Implementing defensive cybersecurity practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents;	4(e)(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 employing automated tools or comparable processes to address the security of internal code	4(e)(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
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;	4(e)(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, 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; 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 appliable policies.	4(e)(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