UNITED STATES DEPARTMENT OF COMMERCE
Office of the Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

PROCUREMENT MEMORANDUM 2024-08

MEMORANDUM FOR: All Department of Commerce Employees and Contractors

FROM: Ryan Higgins
Chief Information Officer (Acting)

TERRI WARE Digitally signed by TERRI WARE Date: 2024.05.31 18:29:16 -04'00'

Olivia J. Bradley
Senior Procurement Executive and
Director, Office of Acquisition Management

OLIVIA BRADLEY Digitally signed by OLIVIA BRADLEY Date: 2024.05.31 12:53:39 -04'00'

SUBJECT: Interim Procedures for the Collection of Secure Software Development Attestations

This memorandum provides interim procedures for the Department of Commerce to comply with the Collection of Secure Software Development Attestations requirements for the procurement of critical software.

Background

The security of software used by the Federal Government is vital to its ability to perform critical functions. Of particular importance is ensuring that critical software is developed securely to resist attack and prevent tampering by malicious actors. To meet these goals and improve the security of the software supply chain, section 4(e) of Executive Order (E.O.) 14028 directed the National Institute of Standards and Technology (NIST) within the Department of Commerce to develop a set of practices and guidance that create the foundation for developing secure software. Accordingly, NIST developed the Secure Software Development Framework (SSDF). This framework establishes fundamental secure software development practices using a common language to help software producers reduce the number of vulnerabilities in released software, reduce potential impact of the exploitation of undetected or unaddressed vulnerabilities and address the root causes of vulnerabilities to prevent recurrences.

Additionally, NIST developed Software Supply Chain Security Guidance[1] to help agencies get the information they need from software producers in a form they can use to make risk-based decisions about procuring software. In accordance with section 4(g) of Executive Order (E.O.) 14028, NIST also developed a definition of critical software. Pursuant to E.O. 14028, the Office of Management and Budget (OMB) issued Memorandum M-22-18, dated September 14, 2022, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*. This memorandum requires agencies to only use software provided by software producers who can attest to complying with secure software development practices as described in NIST guidance. In addition, OMB issued Memorandum M-23-16, dated June 9, 2023, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, to extend the timeline for agencies to collect attestations, clarify the scope of M-22-18's requirements, and provide supplemental guidance on the use of a plan of action and milestone (POA&M) when a software producer cannot

[1] Available at: https://csrc.nist.gov/Projects/ssdf and https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

provide the required attestation.

In accordance with E.O. 14028 and M-22-18, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed the Secure Software Development Attestation Form. This attestation 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.

The Federal Acquisition Regulation (FAR) is being amended to include the procedures for the acquisition workforce to follow to comply with the Collection of Secure Software Development Attestations requirements, however, it is not expected to be finalized prior to the required date for attestations to be received for critical software of June 8, 2024. Therefore, the following actions are required prior to the regulatory updates.

Required Actions

1. Program officials shall submit all new purchase requests[2] for information technology (IT), including requests below the micro-purchase threshold, to the Operating Unit (OU) Office of the Chief Information Officer (CIO) with a completed Office of Chief Information Officer's IT Compliance in Acquisition Checklist (IT Checklist).

2. The supplemental information provided in Attachment 1 shall be submitted with the IT Checklist to enable the OU CIO to determine whether the acquisition is subject to the Collection of Secure Software Development Attestations requirements.

3. If an acquisition is subject to the Collection of Secure Software Development Attestations requirements, program officials and contracting officers shall follow the procedures identified in Attachment 2.

Effective Date

This memorandum is effective as of June 8, 2024, for all new purchase requests for IT. This memorandum remains in effect until rescinded or incorporated into the FAR.

Questions

Please direct any questions regarding this memorandum to DOCSSSC@doc.gov.

Attachments

Attachment 1-IT Checklist Supplemental Information
Attachment 2-Procedures for the Collection of Attestations
Attachment 3-Self-Attestation Common Form

[2] This includes purchase requests for new actions; not modifications for existing actions unless a checklist would otherwise be required. This also includes new orders under existing blanket purchase agreements or indefinite delivery, indefinite quantity contracts including those under existing strategic sourcing initiatives.

Supplemental Information

Secure Software Development Attestation Applicability:

1. Is this an acquisition for the use, anticipated use, development, or modification of software?[1] Yes □ No □

2. Is this an acquisition for critical software?[2] Yes □ No □

3. If the answer to 1 and 2 is Yes do any of the exceptions below apply to the entirety of the software associated with the acquisition? Yes □ No □

(i) Software with a release date or a major version change on or before September 14, 2022.
(ii) Software that is not used in a Federal information system.
(iii) Certain Government-developed software as identified in the requirements documents.
(iv) Open source software that is freely and directly obtained by a Federal agency.
(v) Software that is freely obtained and publicly available.

If the answers to 1 and 2 are Yes and 3 is No, then Secure Software Development Attestation requirements are applicable and a Secure Software Development Attestation Form, extension, or waiver is required prior to award. See Attachment 2-Procedures for the Collection of Secure Software Development Attestations for instructions.

[1] *Software* is defined by FAR 2.1 and “ (1) Means (i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and (ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled. (2) Does not include computer databases or computer software documentation.”

[2] *Critical Software* is defined by the Department of Commerce’s National Institute of Standards and Technology available at https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory.

Attachment 2-Interim Procedures for the Collection of Secure Software Development Attestations

Background

The security of software used by the Federal Government is vital to its ability to perform critical functions. Of particular importance is ensuring that critical software is developed securely to resist attack and prevent tampering by malicious actors. To meet these goals and improve the security of the software supply chain, section 4(e) of Executive Order (E.O.) 14028 directed the National Institute of Standards and Technology (NIST) within the Department of Commerce to develop a set of practices and guidance that create the foundation for developing secure software. Accordingly, NIST developed the Secure Software Development Framework (SSDF). This framework establishes fundamental secure software development practices using a common language to help software producers reduce the number of vulnerabilities in released software, reduce potential impact of the exploitation of undetected or unaddressed vulnerabilities and address the root causes of vulnerabilities to prevent recurrences.

Additionally, NIST developed Software Supply Chain Security Guidance[1] to help agencies get the information they need from software producers in a form they can use to make risk-based decisions about procuring software. In accordance with section 4(g) of E.O. 14028, NIST also developed a definition of critical software. Pursuant to E.O. 14028, the Office of Management and Budget (OMB) issued Memorandum M-22-18, dated September 14, 2022, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*. This memorandum requires agencies to only use software provided by software producers who can attest to complying with secure software development practices as described in NIST guidance. In addition, OMB issued Memorandum M-23-16, dated June 9, 2023, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, to extend the timeline for agencies collecting attestations, clarify the scope of M-22-18's requirements, and provide supplemental guidance on the use of a plan of action and milestone (POA&M) when a software producer cannot provide the required attestation.

In accordance with E.O. 14028 and M-22-18, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed the Secure Software Development Attestation Form. This attestation 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.

[1] [1] Available at: https://csrc.nist.gov/Projects/ssdf and https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

Attachment 2-Interim Procedures for the Collection of Secure Software Development Attestations

Instructions

1. **The program office shall determine if the software product(s) have an existing attestation: (If no, complete step 2)**
    a. Is an attestation available in CISA's repository here?
        i. If yes, the program official shall go to the DOC Interim Attestation Portal here and complete the questionnaire. Complete a questionnaire for each attestation and notify the contracting officer that the attestation process is complete.
    b. Has the software producer provided a publicly available attestation?
        i. If yes, the program official shall go to the DOC Interim Attestation Portal here and complete the questionnaire. Complete a questionnaire for each attestation and notify the contracting officer that the attestation process is complete.

2. **If the software product(s) do not have an existing attestation, the contracting officer shall request that the vendor submit an attestation form from the software provider(s).**
    a. The language in Appendix A may be used by the contracting officer to request the attestation form. The Secure Software Development Attestation Form is provided as Attachment 3.
    b. Once an attestation form has been received, the program official shall go to the DOC Interim Attestation Portal here and complete the questionnaire. Complete a questionnaire for each attestation received and notify the contracting officer that the attestation process is complete.

3. **If the software producer(s) provide documentation other than an attestation form, the program office is required to submit an extension.**
    a. The program official shall go to the DOC Interim Attestation Portal here and complete the questionnaire then contact DOCSSSC@doc.gov for extension procedures. Complete a questionnaire for each extension required and notify the contracting officer that the extension request is submitted.

4. **If the software producer(s) cannot attest to the product or provide other documentation, the program official shall identify alternate software product(s) that can or have completed the attestation form. If no other alternate software exists and justification for use can be fully documented, follow step b. below.**
    a. If an alternate software that meets the requirements for Secure Software Development Attestations is identified, the program official shall follow step 1 outlined above.
    b. The program official shall go to the Interim Attestation Portal here and complete the questionnaire then contact DOCSSSC@doc.gov for waiver procedures. Complete a questionnaire for each waiver needed.
        i. The procurement will be on hold until the waiver request is reviewed by the DOC Chief Information Officer and the OMB response is received. The Director of OMB, in consultation with the Assistant to the President

and National Security Advisor (APNSA), will consider granting the request on a case-by-case basis.

1. If the request is approved by OMB, complete the acquisition process as planned.
2. If the request is denied by OMB, then the procurement is canceled.

Attachment 2-Interim Procedures for the Collection of Secure Software Development Attestations

Appendix A

Subject: Department of Commerce Software Attestation

Dear [Insert name of Software Producer POC],

On September 14, 2022, the Office of Management and Budget (OMB) issued the *Memorandum for the Heads of Executive Departments and Agencies (M-22-18)* requiring each Federal agency to comply with the NIST Secure Software Development Framework when using third-party software on the agency's information systems or otherwise affecting the agency's information.

On June 9, 2023, OMB issued *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M-23-16)* which extended the timeline for collecting attestations and clarified the scope of M-22-18's Requirements.

What does the memorandum say?

The M-22-18 requires that federal agencies only use software provided by software producers who can attest to complying with the Government-specified secure software development practices, as described in the NIST Secure Software Development Framework.

The term "software" as identified in the M-22-18 includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software.

The M-23-16 specifies that agencies should begin collecting attestation letters for "critical software" subject to the requirements of M-22-18 three months after the M-22-18 attestation common form released by the Cybersecurity and Infrastructure Security Agency (CISA) (hereinafter "common form") is approved by OMB under the Paperwork Reduction Act (PRA).

What does this mean for you?

The Department of Commerce has identified the following proposed products that [SOFTWARE PRODUCER] provides as "critical software":

- [INSERT PRODUCT NAME]
- [INSERT PRODUCT NAME]
- [INSERT PRODUCT NAME]

Software producers should complete the Secure Development Software Attestation form, attached, in accordance with the Secure Development Software Attestation Instructions.

Attestations, other documentation, or waiver requests should be submitted to [Insert Email] no later than [Insert Date]. Please contact [Insert Email] with any questions regarding the form or the process.

OMB Control Number: 1670-0052
Expiration Date: 3/31/2027

Department of Commerce

Secure Software Development Attestation Form Instructions

Read all instructions before completing this form

Privacy Act Statement

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. The U.S. Department of Commerce "Department," does not collect personally identifiable information (name, address, e-mail address, social security number, or other personal unique identifiers) or business identifiable information on our websites unless we specifically advise you that we are doing so.

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
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;

[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

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
Send the completed PDF form via email to [insert email address here].

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.

OMB Control Number: 1670-0052
Expiration Date: 3/31/2027

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]

OMB Control Number: 1670-0052
Expiration Date: 3/31/2027

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