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

Background

The security of software used by the Federal Government is vital to the Government's ability to perform critical functions. Of particular importance is ensuring that 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 the potential negative impacts 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. 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] Available at: 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-REVISED

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 when 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 when 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. If no other alternate software exists, 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-REVISED

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 and all software six 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 software subject to the requirements of M-22-18:

- [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.