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

PROCUREMENT MEMORANDUM 2024-08 (REVISED)

MEMORANDUM FOR: All Department of Commerce Employees and Contractors

FROM: Brian Epley
Chief Information Officer

BRIAN EPLEY
Digitally signed by BRIAN EPLEY
Date: 2024.09.09 13:06:17 -04'00'

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

OLIVIA BRADLEY
Digitally signed by OLIVIA BRADLEY
Date: 2024.09.09 14:09:30 -04'00'

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

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 software. It has been revised to include the requirement for all software, effective September 8, 2024.

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*

[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

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 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 software of September 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 cognizant 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 cognizant 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 revised memorandum is effective as of September 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

[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.

Attachment 3-Self-Attestation Common Form