

June 21, 2023

NASA SEWP Contract Holders and Customers:

This letter is to inform you of changing deadlines for implementing secure software requirements that could affect the terms of future federal orders. On June 9, 2023, the US Office of Management and Budget (OMB) issued updated guidance¹ extending deadlines for agencies to collect software attestation letters from software producers, as required under OMB Memorandum M-22-18. Under the new guidance, agencies must collect attestation letters for agency-identified “critical software” no later than three months after finalization² of the common attestation form developed by the Cybersecurity and Infrastructure Security Agency (CISA). Agencies must begin collecting attestations for *all in-scope software* six months after finalization of CISA’s common form.

NASA SEWP will keep you informed of secure software requirements as relevant information becomes available. Additional guidance from NASA is also forthcoming.

Questions about this communication may be directed to help@sewp.nasa.gov.

The remainder of this letter summarizes key requirements and policies for your awareness.

M-22-18. On September 14, 2022, OMB published Memorandum [M-22-18, Enhancing the Security of the Software Supply Chain Through Secure Software Development Practices](#). The document requires federal agencies to comply with guidelines for assuring the integrity of software used on agency information systems, pursuant to [Executive Order \(EO\) 14028, Improving the Nation’s Cybersecurity](#).

To meet federal policy, federal agencies must only use software that complies with government-specified secure software development practices. Among other requirements, M-22-18 directs agencies to obtain self-attestation letters from software producers, attesting the software producer followed secure development processes, as described by published National Institute of Standards and Technology (NIST) Guidance.³

M-23-16. OMB’s June 9, 2023 Memorandum, M-23-16, extends timelines for agencies to collect attestations from software producers and provides supplemental guidance related to scope and compliance with M-22-18 requirements.

Scope. Under M-22-18, the attestation letter requirement applies to all software (other than agency-developed software) used on an agency’s information systems, or otherwise affecting agency information. “Software” includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software. Software developed after the effective date of M-22-18, including major version changes to existing software used by agencies, is subject to the self-attestation letter requirement.

¹ [M-23-16, Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices](#)

² Finalization refers to OMB’s approval of CISA’s common form under the Paperwork Reduction Act.

³ [Special Publication \(SP\) 800-218, Secure Software Development Framework \(SSDF\)](#) and [Software Supply Chain Security Guidance](#)

Additional guidance from M-23-16 clarifies that attestations must be collected from the producer of software end-products used by an agency. When a software end-product includes third-party and/or open source components, separate attestations are not required for each component because the required secure software development requirements in the CISA's common form address the risk of integrated third-party software components.

Agency-developed software is out of scope for M-22-18. Clarifications in M-23-16 indicate attestations are not required for freely obtained and publicly available software obtained directly by agencies (e.g., open-source software and no-cost, publicly available proprietary software products).

Timing. Initial deadlines in M-22-18 are no longer applicable (M-22-18 directed agencies to start collecting attestation letters for agency-identified critical software on June 12, 2023. September 14, 2023 was the listed deadline for collecting attestation letters for *all software*). Updated guidance in M-23-16 provides new deadlines, based on the pending finalization date⁴ of CISA's self-attestation common form (discussed below).⁵

Draft Self-Attestation Common Form. On April 27, 2023, the US Cybersecurity and Infrastructure Security Agency (CISA) released a [draft secure software self-attestation common form](#) for [public comment](#), pursuant to OMB M-22-18 and EO 14028. Comments on the draft will be accepted through June 26, 2023.

SEWP's Support of Self-Attestation Letters and other M-22-18 Requirements. Similar to GSA's support of M-22-18 requirements on GSA-administered indefinite delivery vehicles (IDVs),⁶ NASA SEWP will support secure software development requirements. Upon finalization of CISA's self-attestation common form, customers may request attestation letters at the Request for Quote (RFQ)/Quote level, in accordance with deadlines outlined in OMB Memorandum M-23-16.

References to publicly posted self-attestation letters are the preferred method of meeting the requirement. Any attestation letters provided through NASA SEWP must use the forthcoming finalized version of CISA's self-attestation common form. Attestations provided through NASA SEWP must not include Plan of Action & Milestones (POA&M) or Software Bill of Material (SBOM) information.

Additional details about NASA SEWP's support of ordering agency responsibilities under M-22-18 and M-23-16 will be provided ahead of key deadlines.

⁴ Finalization refers to OMB's approval of CISA's common form under the Paperwork Reduction Act.

⁵ Agencies must collect attestation letters for agency-identified "*critical software*" no later than three months after finalization of CISA's common form. Agencies must collect attestation letters for all in scope software six months after finalization of CISA's common form.

⁶ See [Acquisition Letter \(AL\) MV-23-02, Ensuring Only Approved Software is Acquired and Used at GSA](#)