EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

June 9, 2023

M-23-16

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young

SUBJECT: Update to Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*

Introduction and Authorities

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021),[1] focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs agencies to take a variety of actions that "enhance the security of the software supply chain." In accordance with the EO, the National Institute of Standards and Technology (NIST) has released the NIST Secure Software Development Framework (SSDF), SP 800-218, and the NIST Software Supply Chain Security Guidance (hereinafter, referred to collectively as "NIST Guidance").[2] OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (M-22-18) (Sept. 14, 2022), requires agencies to comply with that NIST Guidance. Pursuant to M-22-18, agencies must only use software that is provided by software producers who can attest to complying with Government-specified minimum secure software development practices.

This memorandum reinforces the requirements established in M-22-18, reaffirms the importance of secure software development practices, and extends the timelines for agencies to collect attestations from software producers. Additionally, this memorandum provides supplemental guidance on the scope of M-22-18's requirements and on agencies' use of Plan of Actions and Milestones (POA&Ms) when a software producer cannot provide the required attestation, but plans to do so. To the extent any provision of this memorandum may be read to conflict with any provision of M-22-18, this memorandum is controlling.

[1] Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-onimproving-the-nations-cybersecurity/

[2] NIST Secure Software Development Framework (SSDF) SP 800-218; NIST Software Supply Chain Security Guidance under Executive Order (EO) 14028 Section 4e.

A. Extending Timeline for Collection of Attestations for Critical Software and Non-Critical Software

Consistent with EO 14028, M-22-18 requires each Federal agency to collect attestations from producers of software used by the agency if that software was developed after September 14, 2022, the effective date of M-22-18. Agencies are also required to collect attestations from producers of software developed prior to September 14, 2022, if that software is used by a Federal agency and either: (1) is modified by one or more major version changes after September 14, 2022, or (2) is a hosted service that deploys continuous updates. For the purposes of M-22-18 and this memorandum, "software" includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software.[3]

This memorandum modifies the deadlines by which agencies must collect attestation letters. Agencies must collect attestations for critical software subject to the requirements of M-22-18 and this memorandum no later than 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). Six months after the common form's PRA approval by OMB, agencies must collect attestations for all software subject to the requirements delineated in M-22-18, as amended by this memorandum.

B. Clarifying the Scope of M-22-18's Requirements

1. Third Party Components

Attestations must be collected from the producer of the software end product used by an agency because the producer of that end product is best positioned to ensure its security. An attestation provided by that producer to an agency serves as an affirmative statement that the producer follows the secure software development minimum requirements, as articulated in the common form. These minimum requirements include several best practices regarding how software producers should address and maintain the security of code. These naturally extend to and guide the utilization of third-party software components,[4] both open-source[5] and proprietary, and reflect best practices for minimizing risk from such components, as articulated in NIST's SSDF. Best practices include: regularly logging, monitoring, and auditing trust relationships used for authorization and access among components within the develop and build environments; taking consistent and reasonable steps to document and minimize use of software products that create undue risk; maintaining provenance data for internal and third-party code; and maintaining trusted source code supply chains.

The minimum requirements delineated in the common form address the risk of integrating components from third-parties. When software producers responsibly implement industry-leading development practices, which include minimizing risk from third-party code,[6] the burden of accounting for

---

[3] Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e (nist.gov).

[4] "Component" is defined as: A software object, meant to interact with other components, encapsulating certain functionality or a set of functionalities. A component has a clearly defined interface and conforms to a prescribed behavior common to all components within an architecture. *See* NIST SP 800-95, Guide to Secure Web Services.

[5] Open-source software is "software that can be accessed, used, modified, and shared by anyone." *See* NIST, *Open Source Code* (December 6, 2018).

[6] NIST SP 800-218: Secure Software Development Framework (SSDF) Version 1.1, February 2022. See, PO 1.3; PW 4.1; PW 4.4; PW 7.1, among others.

secure software development practices is appropriately placed on the producer of the end product rather than Federal agencies. Accordingly, agencies are not required to collect attestations from producers of third-party software components that are incorporated into the software end product used by the agency. This is true for both third-party open-source and proprietary components. A component, whether open-source or proprietary, only qualifies as a "third-party" component if it was developed by an entity other than the producer of the software end product into which it is incorporated.

2. Freely Obtained and Publicly Available Proprietary Software

Agencies are not required to collect attestations from software producers for products that are proprietary but freely obtained and publicly available. Open-source software freely and directly obtained by Federal agencies is outside the scope of NIST's guidance for agencies on software supply chain security.[7] This memorandum further clarifies that no-cost, publicly available *proprietary* software is also out of scope for M-22-18 attestation collection.

A significant number of core software applications, such as web browsers, to which Federal agencies must have access are offered for use to members of the public at no cost. Users of this software have no opportunity to negotiate with the producer, and therefore it will not be feasible for agencies to obtain attestations from the producers of such software. Agencies are, nevertheless, required to assess the risk in utilizing such software and take appropriate steps to minimize or eliminate identified risks.

Though freely obtained, demonstrations or pilots of software products that are otherwise unavailable on a no-cost basis remain subject to M-22-18 attestation requirements, as amended.

3. Federal Contractor Developed Software

Agency-developed software remains out of scope for M-22-18 and any attestation collection requirements. Whether software developed under a Federal contract may constitute "[a]gency-developed software" for the purposes of M-22-18, as amended, depends on whether the contracting agency is able to ensure that secure software development practices are followed throughout the entire software development lifecycle (i.e., requirements, design, development, testing, deployment, and maintenance). Agencies, in their development of software, are expected to appropriately leverage the NIST SSDF (SP 800-218).

If there are questions regarding whether software developed by Federal contractors should be considered agency-developed, agency CIOs are required to make that determination on behalf of the agency. Agency CIOs are in the best position to determine in a given case whether the agency's specification and supervision of contract performance meet the standard articulated above.

If an agency must, under M-22-18 and this memorandum, obtain an attestation before using a given software application, then that application will remain subject to the attestation requirement even if it is deployed, configured, or modified by a Federal contractor on behalf of an agency.

C. Guidance on the Use of Plans of Action and Milestones Submitted to Federal Agencies by Software Producers

[7] Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e (nist.gov), page 2.

M-22-18 provides that, if a software producer cannot attest to one or more practices identified in the attestation form, an agency may still use the 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 satisfactory Plan of Action and Milestones (POA&M).[8] That alternative to attestation creates a means for agencies to work with software producers[9] who do not yet meet the minimum requirements identified in the common form, but plan to do so.

This memorandum makes an adjustment to M-22-18's alternative to attestation. First, the producer of a given software application must identify the practices to which they cannot attest, document practices they have in place to mitigate associated risks, and submit a POA&M to an agency. If the agency finds the documentation satisfactory, it may continue using the software, but must concurrently seek an extension of the deadline for attestation from OMB. Extension requests submitted to OMB must include a copy of the software producer's POA&M.

The agency must discontinue use of the software if the agency finds the software producer's documentation unsatisfactory or if the agency is unable to confirm that the producer has identified the practices to which it cannot attest; documented practices they have in place to mitigate associated risk; and submitted a POA&M to the agency. Additionally, if the agency fails to submit an extension request, the POA&M is not considered valid, and the agency must discontinue use of the software.

In instances where multiple agencies are affected by a software producer's inability to attest to minimum requirements for one or more software products, OMB will prioritize consideration of agencies' extension requests for software product(s) that share a common POA&M. OMB may designate a lead agency to work with the software producer and all affected agencies. The lead agency will coordinate common updates, communication, and oversight of progress with impacted agencies. Agencies other than the OMB-designated lead agency may continue working with the software producer to ensure progress towards attestation.

Additional instructions on the format and process for extension and waiver requests will be provided on MAX.gov. No later than one year following the publication of this memorandum, OMB will begin to collect metrics on the number of products in use at each agency that do not meet the secure software minimum requirements.

D. Future Updates to Guidance

Additional clarifications and general updates on implementation of M-22-18 and this memorandum will be posted on the appropriate MAX.gov or successor site.

All questions or inquiries concerning this memorandum should be addressed to the OMB Office of the Federal Chief Information Officer (OFCIO) via email: ofcio@omb.eop.gov.

[8] M-22-18 at 3.
[9] OMB Memorandum M-22-18, Section II. Actions and Section III. Responsibilities, available at: https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

Appendix A

This table summarizes the updates to key dates in M-22-18 and outlines new dates as modified by this Memorandum.

Requirement	**Actions following publication**	**Responsible Body**
Agencies shall collect attestation letters for "critical software" subject to the requirements of M-22-18, as amended by this memorandum.	3 months after OMB PRA approval of common form	Agencies
Agencies shall collect attestation letters for all software subject to the requirements of M-22-18, as amended by this memorandum.	6 months after OMB PRA approval of common form	Agencies
OMB will begin to collect metrics on agency approval of POA&Ms, as well as the number of extensions and waivers in place at each agency.	Within 1 year of issuance of this memorandum	OMB