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

THE DIRECTOR

September 14, 2022

M-22-18

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

The Federal Government relies on information and communications technology (ICT) products and services to carry out critical functions. The global supply chain for these technologies faces relentless threats from nation state and criminal actors seeking to steal sensitive information and intellectual property, compromise the integrity of Government systems, and conduct other acts that impact the United States Government's ability to safely and reliably provide services to the public.

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 the National Institute of Standards and Technology (NIST) to issue guidance "identifying practices that enhance the security of the software supply chain."[2] The NIST Secure Software Development Framework (SSDF), SP 800-218,[3] and the NIST Software Supply Chain Security Guidance[4] (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. The EO further directs the Office of Management and Budget (OMB) to require agencies to comply with such guidelines. This memorandum requires agencies to comply with the NIST Guidance and any subsequent updates.

[1] Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] Executive Order on Improving the Nation's Cybersecurity (E.O.14028), Section 4(e)
[3] Available at: https://csrc.nist.gov/Projects/ssdf
[4] Available at: https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

I. SCOPE

The Federal Information Security Modernization Act of 2014 (FISMA)[5] requires each Federal agency to provide security protections for both "information collected or maintained by or on behalf of an agency"[6] 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."[7] FISMA and other provisions of Federal law authorize the Director of OMB to promulgate information security standards for information security systems, including to ensure compliance with standards promulgated by NIST.[8]

Consistent with these authorities and the directives of EO 14028, this memorandum requires each Federal agency[9] to comply with the NIST Guidance when using third-party software on the agency's information systems or otherwise affecting the agency's information.[10] The term "software" for purposes of this memorandum includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software.[11] The following conditions apply to the requirements of this memorandum:

- These requirements apply to agencies' use of software developed after the effective date of this memorandum, as well as agencies' use of existing software that is 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 the effective date of this memorandum.

- These requirements do not apply to agency-developed software, although agencies are expected to take appropriate steps to adopt and implement secure software development practices for agency-developed software.

- An agency awarding a contract that may be used by other agencies is responsible for implementing the requirements of this memorandum.

II. ACTIONS

Ensuring software integrity is key to protecting Federal systems from threats and vulnerabilities and reducing overall risk from cyber-attacks. The NIST Guidance provides "recommendations to federal agencies on ensuring that the producers of software they procure have been following a risk-based approach for secure software development."[12] Federal agencies must 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 Guidance.

---

[5] P.L. 113-283
[6] 44 U.S.C. § 3553(a)(2)(A) (hereinafter referred to as "information")
[7] 44 U.S.C. § 3553(a)(2)(B) (hereinafter referred to as "information systems")
[8] 40 U.S.C. § 11331(b), (d); 44 U.S.C. § 3553(a)(1)-(2).
[9] The term "Federal agency" refers to an "agency" under the definition provided under 44 U.S.C. § 3502(1).
[10] Federal information systems carry the definition provided under 44 U.S.C. § 3502(8).
[11] Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e (nist.gov)
[12] *Id.*

In accordance with EO 14028 and the NIST Guidance, Agency Chief Information Officers (CIOs), in coordination with requiring offices and Chief Acquisition Officers (CAOs), must take the following steps to ensure software producers have implemented and will attest to conformity with secure software development practices.

1. **Consistent with the NIST Guidance and by the timelines identified below, agencies are required to obtain a self-attestation from the <u>software producer</u> before using the software.**

    a. A software producer's self-attestation serves as a "conformance statement" described by the NIST Guidance. The agency must obtain a self-attestation for all third-party software subject to the requirements of this memorandum used by the agency, including software renewals and major version changes.

        i. Agencies should encourage software producers to be product inclusive so that the same attestation may be readily provided to all purchasing agencies.

        ii. If the software producer cannot attest to one or more practices from the NIST Guidance identified in the standard self-attestation form, the requesting agency shall require the software producer to identify those practices to which they cannot attest, document practices they have in place to mitigate those risks, and require a Plan of Action & Milestones (POA&M) to be developed. The agency shall take appropriate steps to ensure that such documentation is not posted publicly, either by the vendor or by the agency itself. If the software producer supplies that documentation and the agency finds it satisfactory, the agency may use the software despite the producer's inability to provide a complete self-attestation.

            Documentation provided in lieu of a complete self-attestation, as described in the preceding paragraph, shall not be posted publicly by the vendor or the agency.

    b. The agency shall retain the self-attestation document, unless the software producer posts it publicly and provides a link to the posting as part of its proposal response.

    c. An acceptable self-attestation must include the following minimum requirements:

        i. The software producer's name;

ii. A description of which product or products the statement refers to (preferably focused at the company or product line level and inclusive of all unclassified products sold to Federal agencies);

iii. A statement attesting that the software producer follows secure development practices and tasks that are itemized in the standard self-attestation form;

iv. Self-attestation is the minimum level required; however, agencies may make risk-based determinations that a third-party assessment is required due to the criticality of the service or product that is being acquired, as defined in M-21-30.

d. A third-party assessment provided by either a certified FedRAMP Third Party Assessor Organization (3PAO) or one approved by the agency shall be acceptable in lieu of a software producer's self-attestation, including in the case of open source software or products incorporating open source software, provided the 3PAO uses the NIST Guidance as the assessment baseline.

e. Agencies are encouraged to use a standard self-attestation form, which will be made available to agencies. The Federal Acquisition Regulatory (FAR) Council plans to propose rulemaking on the use of a uniform standard self-attestation form.

2. Agencies may obtain from software producers artifacts that demonstrate conformance to secure software development practices, as needed.

a. A Software Bill of Materials (SBOMs) may be required by the agency in solicitation requirements, based on the criticality of the software as defined in M-21-30, or as determined by the agency. If required, the SBOM shall be retained by the agency, unless the software producer posts it publicly and provides a link to that posting to the agency.

b. SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information Administration (NTIA) report "The Minimum Elements for a Software Bill of Materials (SBOM),"[13] or successor guidance as published by the Cybersecurity and Infrastructure Security Agency (CISA).

c. Agencies shall consider reciprocity of SBOM and other artifacts from software producers that are maintained by other Federal agencies, based on direct applicability and currency of the artifacts.

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

d. Artifacts other than the SBOM (e.g., from the use of automated tools and processes which validate the integrity of the source code and check for known or potential vulnerabilities) may be required if the agency determines them necessary.

e. Evidence that the software producer participates in a Vulnerability Disclosure Program may be required by the agency.

f. Agencies are encouraged to notify potential vendors of requirements as early in the acquisition process as feasible, including leveraging pre-solicitation activities.

Compliance with the EO and NIST Guidance requires that agencies engage in appropriate planning. In order to ensure compliance and reduce risk, agencies must integrate the NIST Guidance into their software evaluation process as outlined in this memorandum and consistent with the timelines below. As agencies develop requirements that include the use of new software, they must request confirmation that the software producer utilizes secure software development practices. This could be accomplished through specification of these requirements in the Request for Proposal (RFP) or other solicitation documents, but regardless of how the agency ensures compliance, the agency must ensure that the company implements and attests to the use of secure software development practices consistent with NIST Guidance, throughout the software development lifecycle.

III. RESPONSIBILITIES

A. Agency Responsibility

Agencies must incorporate the requirements of this memorandum, in accordance with the following:

1. Within 90 days of the date of this memorandum, agencies shall inventory all software subject to the requirements of this memorandum, with a separate inventory for "critical software."

2. Within 120 days of the date of this memorandum, agencies shall develop a consistent process to communicate relevant requirements in this memorandum to vendors, and ensure attestation letters not posted publicly by software providers are collected in one central agency system.

3. Agencies shall collect attestation letters not posted publicly by software providers for "critical software"[14] subject to the requirements of this memorandum within 270 days after publication of this memorandum.

[14] OMB Memorandum M-21-30, available at: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf

4. Agencies shall collect attestation letters not posted publicly by software providers for all software subject to the requirements of this memorandum within 365 days after publication of this memorandum.

5. Within 180 days of the date of this memorandum, agency CIOs, in coordination with agency requiring activities and agency CAOs, shall assess organizational training needs and develop training plans for the review and validation of full attestation documents and artifacts.

6. *Extensions*. Agencies may request an extension for complying with the requirements of this memorandum. The extension request shall be submitted to the Director of OMB and must be transmitted 30 days before any relevant deadline in this memorandum and accompanied by a plan for meeting the underlying requirements.

   Specific instructions for submitting requests for extensions will be posted in MAX.gov at this URL: https://community.max.gov/x/LhtGJw.

7. *Waivers.* Agencies may request a waiver—only in the case of exceptional circumstances and for a limited duration—for any specific requirement(s) of this memorandum. The waiver request must be submitted to the Director of OMB and must be transmitted 30 days before any relevant deadline in this memorandum and accompanied by a plan for mitigating any potential risks. 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.

   Specific instructions for submitting requests for waivers will be posted in MAX at this URL: https://community.max.gov/x/LhtGJw.

8. Compliance with Other Authorities. In executing the activities required by this memorandum, agencies shall comply with laws governing the collection, use, and dissemination of information.

B. OMB Responsibility

1. Within 90 days from the date of this memorandum, OMB will post specific instructions for submitting requests for waivers or extensions to the MAX.gov links identified above.

2. Within 180 days from the date of this memorandum, OMB, in consultation with CISA and the General Services Administration (GSA), will establish requirements for a centralized repository for software attestations and artifacts, with appropriate mechanisms for protection and sharing among Federal agencies.

C. CISA Responsibility

1. Within 120 days from the date of this memorandum, CISA, in consultation with OMB, will establish a standard self-attestation "common form" for Paperwork Reduction Act (PRA) clearance that is suitable for use by multiple agencies.

2. Within 1 year from OMB's establishment of requirements, CISA, in consultation with GSA and OMB, will establish a program plan for a government-wide repository for software attestations and artifacts with appropriate mechanisms for information protection and sharing among Federal agencies.

3. Within 18 months from OMB's establishment of requirements, CISA will demonstrate an Initial Operating Capability (IOC) of the repository.

4. Within 24 months from OMB's establishment of requirements, CISA will evaluate requirements for the Full Operating Capability (FOC) of a Federal interagency software artifact repository through traditional OMB processes.

5. CISA will publish updated guidance on Software Bill of Materials (SBOM) for Federal agencies, as appropriate.

D. NIST Responsibility

Update SSDF guidance as appropriate.

IV. POLICY ASSISTANCE

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

APPENDIX A

This table summarizes all actions in the memorandum above:

Requirement	Actions following publication	Responsible Body
Agencies shall inventory all software subject to the requirements of this memorandum.	Within 90 days	Agencies
Agency CIOs shall develop a consistent process to communicate relevant requirements in this memorandum to vendors, and ensure attestation letters are collected in one central agency system	Within 120 days	Agencies
Agencies shall collect attestation letters for "critical software" subject to the requirements of this memorandum	Within 270 days	Agencies
Agencies shall collect attestation letters for all software subject to the requirements of this memorandum	Within 365 days	Agencies
Agency CIOs shall assess training needs and develop training plans for the review and validation of software attestations and artifacts	Within 180 days	Agencies
OMB will post specific instructions for requesting waivers and extensions to identified MAX.gov sites.	Within 90 days	OMB
OMB will establish the requirements for a centralized repository for agency secure software attestations and artifacts	Within 180 Days	OMB
In consultation with GSA and OMB, CISA will establish a program plan for a Government-wide repository for software attestations and artifacts with appropriate mechanisms for information protection and sharing among Federal agencies	One year from the establishment of requirements	CISA
CISA will demonstrate IOC of the attestation and artifact repository	18 months after establishment of requirements	CISA
CISA will evaluate requirements for the Full Operating Capability (FOC) of a Federal interagency software acquisition artifact repository through traditional OMB processes	24 months after establishment of requirements	CISA
CISA will publish updated SBOM guidance	As appropriate	CISA
CISA will establish a self-attestation common form for PRA clearance, incorporating the minimum elements of NIST 800-218 as identified by OMB.	Within 120 days	CISA
NIST will update SSDF guidance.	As appropriate	NIST