**Westlaw Today**
*powered by Reuters*

# OMB announces requirements for ensuring the integrity of software used by federal agencies

**By Marcia G. Madsen, Esq., Stephen Lilley, Esq., and Cameron R. Edlefsen, Esq., Mayer Brown***

**NOVEMBER 15, 2022**

On September 14, 2022, the U.S. Office of Management and Budget (OMB) published a memorandum, M-22-18,[1] requiring federal agencies to comply with previously announced guidelines for ensuring the integrity of third-party software on an agency's information systems or that otherwise affects government information.

*Agencies must obtain a software producer's self-attestation before agencies can use the software.*

Applicable to firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software, this memorandum gives practical force to previously issued guidance for software producers[2] to the federal government.

*Agencies may request a waiver of the memorandum's requirements in "exceptional circumstances and for a limited duration."*

Under this newly issued memorandum, federal agencies must comply with the National Institute of Standards and Technology (NIST) guidance, issued pursuant to President Biden's cybersecurity executive order, which "include a set of practices that create the foundation for developing secure software."[3] (This "NIST Guidance" consists of (i) Special Publication, SP 800-218[4] (the NIST Secure Software Development Framework (SSDF)) and (ii) the NIST Software Supply Chain Security Guidance[5]).

Importantly, the memorandum requires that "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."

## Key takeaways from the OMB memorandum:

- **Affected software.** NIST Guidance requirements "apply to agencies' use of software[6] developed after [the] effective date of the memorandum or 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."
- **Key no-later-than dates.** The memorandum requires federal agencies to complete the following tasks:
  - No later than December 13, 2022, agencies must inventory software subject to the memorandum and separately inventory "critical software."[7]
  - No later than January 12, 2023, agencies shall develop a "process to communicate relevant requirements" to vendors and develop a central agency system to collect attestation letters.
  - No later than January 12, 2023, the Cybersecurity and Infrastructure Security Agency (CISA) will establish a self-attestation common form, which "incorporate[s] the minimum elements of NIST 800-218 as identified by OMB."[8]
  - No later than March 13, 2023, agencies "shall assess organizational training needs and develop training plans for review and validation of full attestation documents and artifacts."
  - No later than June 11, 2023, for "critical software" (defined above), "agencies shall collect attestation letters not posted publicly by software providers for 'critical software' subject to the requirements of this memorandum."
  - No later than September 13, 2023, for all software, "agencies shall collect attestation letters not posted publicly by software providers for all software subject to the requirements of this memorandum."
- **Self-attestation**. Agencies must obtain a software producer's self-attestation before agencies can use the software. If the



THOMSON REUTERS®

producer is unable to attest to any of the practices outlined in the NIST Guidance, "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." If the agency finds that the software producer adequately mitigates the risks, then the agency may use the software despite the lack of a complete self-attestation.

*Developers of software that is not sold to the government also will likely benefit from paying close attention to the requirements imposed through the memorandum.*

- "Self-attestation is the minimum level required." However, as needed, "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."
- Valid third-party assessments include those "provided by either a certified FedRAMP Third Party Assessor Organization (3PAO) or one approved by the agency." These assessments "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."

- **Artifacts demonstrating conformance to secure software development practices.** As needed, agencies may obtain from software producers a Software Bill of Materials (SBOM), evidence of participation in a vulnerability disclosure program, or other artifacts "that demonstrate conformance to secure software development practices."
- **Extension and waiver requests.** Agencies may request extensions for complying with the memorandum's requirements. Agencies may also request a waiver of the memorandum's requirements in "exceptional circumstances and for a limited duration."

## Practical steps for software producers

Software producers are likely already very familiar with the NIST Guidance, which was developed in coordination with industry stakeholders. The new memorandum gives new practical force to that guidance, however.

It accordingly is important for software producers to the government to identify and close any gaps in their software development processes so that they will be able to comply with and accurately self-attest that compliance with the NIST Guidance requirements.

Developers of software that is not sold to the government also will likely benefit from paying close attention to the requirements imposed through the memorandum. Such software companies may benefit from considering these requirements as guides to future expectations to which they may be subject, whether through contract, regulation, or private litigation.

## Notes

[1] http://bit.ly/3Aawj7f

[2] According to the NIST Guidance, "software producers" include commercial-off-the-shelf product vendors, government-off-the-shelf software developers, and other software developers working within or on behalf of software acquirer organizations. Special Publication, SP 800-218 at 3, http://bit.ly/3huS8Id.

[3] The NIST developed this guidance as directed by Executive Order 14028, Improving the Nation's Cybersecurity (May 12, 2021).

[4] http://bit.ly/3huS8Id

[5] http://bit.ly/3Gb8wYK

[6] Memorandum at 2. According to the NIST Software Supply Chain Security Guidance, https://bit.ly/3Gb8wYK, software that is out of scope of this guidance is "software developed by federal agencies" and "open-source software freely and directly obtained by federal agencies." However, the guidance advises that agencies "can choose to use attestations and artifacts from open-source producers who make such content available." NIST Software Supply Chain Security Guidance at 2, 6.

[7] In OMB Memorandum M-21-30, http://bit.ly/3WZMbn8, and in a NIST White Paper, http://bit.ly/3NXc7vs, NIST defined "critical software" as any software that has, or has direct software dependencies on, one or more components with at least one of these attributes: is designed to run with elevated privilege or manage privileges; has direct or privileged access to networking or computing resources; is designed to control access to data or operational technology; performs a function critical to trust; or operates outside of normal trust boundaries with privileged access. The definition applies to software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software) purchased for, or deployed in, production systems and used for operational purposes.

[8] The Federal Acquisition Regulatory Council plans to propose rulemaking requiring agencies to use this common form. *See* Memorandum at 4.

## About the authors



**Marcia G. Madsen** (L) is a partner at **Mayer Brown**, chair of the firm's government contracts practice and co-chair of its national security practice. She represents clients with regulatory, policy, transactional, litigation and investigative matters in business areas including aerospace, information technology, telecommunications and military systems. **Stephen Lilley** (C) is a partner in the firm and a member of its litigation and cybersecurity and data privacy practices. He develops strategies to manage legal risks and to shape regulatory policy and helps clients with litigation, regulatory and policy challenges. **Cameron R. Edlefsen** (R), a counsel in the firm, advises clients in the information technology, large military systems and engineering services industries regarding federal procurements and related issues. All of the authors are based in Washington, D.C. This article was originally published Oct. 5, 2022, on the firm's website. Republished with permission.

**This article was published on Westlaw Today on November 15, 2022.**