PUBLICATION

Software Developers With Federal Government Customers Must Provide Confirmation of NIST Standards

Authors: Alisa L. Chestler, Darwin A. Hindman, III
September 26, 2022

In mid-September, the Office of Management and Budget (OMB) released a memorandum requiring federal agencies to obtain attestation from software developers before running third-party software on government networks. Under this guidance, software developers must provide confirmation to their federal customers that shows adherence to the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF), SP 800-218, and the NIST Software Supply Chain Security Guidance.

This new requirement applies to all third-party software used by federal government agencies that is developed on or after September 14, 2022, as well as existing software that is modified after that date by a major version change (e.g., version 2.5 to version 3.0). Software producers will be required to provide written self-attestation of compliance to the contracting agency.

Self-attestations will include:

- The software producer's name.
- A description of which product or products the statement refers to.
- A statement attesting that the software producer follows secure development practices and tasks that are itemized in the standard self-attestation form.

While self-attestation is the minimum level required under this memorandum, individual agencies may make risk-based determinations that a third-party assessment is required depending on the criticality of the software to that agency's function. Similarly, the contracting agency may also require the software producer to provide a Software Bill of Materials (SBOM) along with other artifacts for "critical software."

For the purposes of this memorandum, NIST has defined critical software as "any software that has, or has direct software dependencies upon, 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."

In situations where software may be used by multiple agencies under a single contract, the contracting agency is responsible for verifying attestation, and the software producer *will not* be required to self-attest to multiple agencies. However, where the same software is licensed under different contracts to different agencies, the software producer *will* be required to self-attest to each new purchasing agency.

In many situations not involving critical software, a certified FedRAMP Third Party Assessor Organization (3PAO) will be an acceptable substitution for a self-attestation.

In certain cases, complete attestation will not be required. Where a software producer cannot attest to one or more practices outlined in the NIST guidelines, the contracting agency may still elect to use the software, provided that the software producer supplies documentation of practices in place sufficient to mitigate risk as well as a plan to achieve compliance.

Federal agencies have until June 11, 2023, to collect letters of attestation from their software providers for critical software and until September 14, 2023, to collect letters for all other software in use. This means that all contractors should be developing and implementing a plan to ensure they have sufficient assurances from their software component producers to execute attestations requested from their agency partners.

If you have any questions about federal contractor requirements under this memorandum, please contact Alisa L. Chestler, Skip Hindman or a member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Group.