Government Contracts and Privacy & Cybersecurity Update

September 2022

U.S. Government Issues Software Security Procurement Guidance

On September 14, the Office of Management and Budget (OMB) issued a memorandum to all federal agencies ("OMB Memorandum") requiring them to comply with certain software security standards and guidelines published by the National Institute of Standards and Technology (NIST) when procuring third-party software solutions. The key requirement of the OMB Memorandum is to have third-party software providers attest to the security of their products and solutions, and the Federal Acquisition Regulatory (FAR) Council will undertake rulemaking on the use of a uniform standard self-attestation form.

Given the significant amount of third-party software procured by federal departments and agencies, the OMB Memorandum will impact both software developers and organizations that incorporate third-party software into the products they furnish, directly or indirectly, to the U.S. government.

Background: NIST Guidance

Pursuant to Executive Order (EO) 14028, NIST was directed to issue guidance "identifying practices that enhance the security of the software supply chain." In turn, NIST published its Secure Software Development Framework (SSDF) and Software Supply Chain Security Guidance (SSCSG) (collectively referred to as the "NIST Guidance").

The SSDF is a set of secure software development practices based on established secure software development practice documents from a broad range of organizations, such as BSA, OWASP, and SAFECode. The SSDF helps organizations meet the following secure software development recommendations:

- Organizations should ensure that their people, processes, and technology are prepared to perform secure software development.
- Organizations should protect all components of their software from tampering and unauthorized access.
- Organizations should produce well-secured software with minimal security vulnerabilities in their releases.
- Organizations should identify residual vulnerabilities in their software releases and respond appropriately to address those vulnerabilities and prevent similar ones from occurring in the future.

Separately, the SSCSG sets forth guidelines intending to assist federal employees who have software procurement-related responsibilities (e.g., acquisition and procurement officials, technology professionals) understand what information to request from software producers regarding their secure software development practices.

OMB Memorandum: Key Requirements

The OMB Memorandum requires each federal agency "to comply with the NIST Guidance when using third-party software on the agency's information systems or otherwise affecting the agency's information." Most importantly, federal agencies are now required to "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."

For purposes of the OMB Memorandum, the term "software" includes "firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software."

The OMB Memorandum applies to federal agencies' use of software developed after the OMB Memorandum's effective date and existing software that is modified by major version changes after the effective date. Although it focuses on third-party software and does not apply to agency-developed software, the OMB Memorandum notes that agencies are "expected to take appropriate steps to adopt and implement secure software development practices for agency-developed software."

Federal Agency Responsibilities

To satisfy the OMB Memorandum, federal agencies are required to undertake several measures to ensure software producers have implemented and will attest to conformity with secure software development practices, including:

- Federal agencies are required to obtain a self-attestation from the software producer before using the software, including for software renewals and major version changes.
- Agencies may obtain from software producers artifacts that demonstrate conformance to secure software development practices.
- A Software Bill of Materials (SBOM) may be required by the agency in solicitation requirements, based on the criticality of the software, or as determined by the agency. Artifacts other than the SBOM may be required if the agency determines them necessary.
- Evidence that the software producer participates in a Vulnerability Disclosure Program may be required.

The OMB Memorandum notes that compliance with EO 14028 and the NIST Guidance requires agencies to "engage in appropriate planning" and "[i]n order to ensure compliance and reduce risk, agencies must integrate the NIST Guidance into their software evaluation process." Importantly, agencies can satisfy their proof-of-software-security requirements through incorporation of the OMB Memorandum in their Request for Proposal (RFP) or other solicitation documents.

Self-Attestation Requirements and Exceptions

According to the OMB Memorandum, an acceptable self-attestation regarding software security must include, at a minimum, the following: (i) the software producer's name, (ii) a description of which product or products the self-attestation statement refers to (preferably focused at the company or product line level and inclusive of all unclassified products sold to federal agencies), and (iii) a statement attesting that the software producer follows secure development practices and tasks that are itemized in the standard self-attestation form. Self-attestation is the minimum level required, however, and federal 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.

In addition to the above-mentioned requirements, the OMB Memorandum notes that "[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."

Federal agencies are encouraged to use a standard self-attestation form when complying with the OMB Memorandum requirements, and the FAR Council plans to propose rulemaking on the use of a uniform standard self-attestation form. In addition, the U.S. Department of Homeland Security, in consultation with OMB, will produce a self-attestation "common form" for use by multiple agencies.

The OMB has created some exceptions in the event the software producer cannot attest to one or more practices from the NIST Guidance identified in the standard self-attestation form. In such circumstances, the applicable federal 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, in turn, is then required to undertake appropriate measures to ensure the confidentiality of this information and that it is not posted publicly. If the software producer supplies this documentation in lieu of the self-attestation and the agency finds it "satisfactory," the agency is permitted to "use the software despite the producer's inability to provide a complete self-attestation."

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Francis E. (Chip) Purcell, Jr.
202.263.4118
Chip.Purcell@ThompsonHine.com

Mona Adabi
202.263.4147
Mona.Adabi@ThompsonHine.com