wiley

ALERT

OMB Extends Timeline for Collection of Software Attestation Forms and Clarifies Scope of Requirement

June 14, 2023

On June 9, 2023, the Office of Management and Budget (OMB) issued a guidance memorandum, OMB M-23-16, that extends the timeline for agencies to begin collecting attestations for critical and non-critical software from producers of software used by government agencies. As we covered in late April, the Cybersecurity and Infrastructure Security Agency (CISA) issued a draft self-attestation form (the common form) to be completed by software producers to confirm their compliance with secure software practices in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-218, Secure Software Development Framework. Notice and comment on CISA's common form is ongoing, and comments are due by June 26, 2023.

Notably, M-23-16 provides that for critical software, agencies must collect attestations no later than three months after the common form is finalized; for other software subject to M-22-18, agencies must collect attestations no later than six months after the common form is finalized. The memorandum also includes guidance to clarify from whom agencies must collect attestations, and whether proprietary open-source software and contractor-developed software require attestation.

BACKGROUND

In September 2022, OMB issued a guidance memorandum, OMB M-22-18, that required agencies to obtain a self-attestation of compliance with NIST SP 800-218 from software producers before using their software. This requirement applies to: (1) new software

Authors

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Cybersecurity
Emerging Technologies and Nontraditional Contracting
Government Contracts
National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology

developed after September 14, 2022; (2) existing software modified by major version changes after that date; and (3) software to which the producer delivers continuous changes to the software code. The memorandum provided that agencies had 270 days after publication (June 12, 2023) to collect attestations for critical software, and 365 days (September 14, 2023) to collect attestations for all other software subject to the memorandum. Because the common form is still in draft and comments are not even due until after the deadline for self-attestations for critical software, there has been confusion among agencies and contractors about whether those dates were still applicable. OMB's most recent memorandum revises those to put events back in a more logical order, although OMB's directive may still require compliance before the FAR Council has an opportunity to issue any contracting guidance on this issue.

KEY TAKEAWAYS

Revised Timeline. Agencies must collect attestations for "critical software" no later than three months after the CISA common form is approved by OMB. Agencies must collect attestations for all other in-scope software within six months after the common form in approved. Although it is not certain when the form will be approved, the private sector should continue to take steps to identify software covered by the attestation requirement and to determine their ability to complete the current version of the form or create a plan of action and milestones (POA&M) after the common form is finalized.

Attestations Must Be Collected from the Producer of the Software "End Product." Neither M-22-18 nor the draft common form specify who is responsible for a software attestation if the software used by the agency includes other components that are not made by the producer of the software "end product." In an attempt to clarify who is responsible for the attestation, M-23-16 provides that attestations must be collected from the producer of the software end product because "the producer of that end product is best positioned to ensure its security." Agencies are not required to collect attestations from producers of third-party software components that are incorporated into the software end product ultimately used by the agency. Instead, the burden is on the end product software producer to address the security of software development practices by third-party entities.

Attestation Is Not Required for Freely Obtained and Publicly Available Proprietary Software. M-23-16 clarifies that no-cost, publicly available, proprietary software (such as web browsers) is out of scope for attestation collection, and therefore agencies are not required to collect attestations for those software products.

Federal Contractor-Developed Software May Still Require Attestation. While OMB maintains that agency-developed software is out of scope for M-22-18, M-23-16 considers whether software developed under a federal contract may constitute agency-developed software for which the agency also does not need to obtain an attestation. M-23-16 provides that whether contractor-developed software may be considered agency-developed depends on whether the contracting agency is able to ensure that secure software development practices are followed throughout the software development lifecycle. Agency Chief Information Officers (CIOs) will be responsible for those determinations. Contractors should consider seeking such determinations if the status of software developed under a contract is unclear.

Clarification Regarding POA&Ms. M-23-16 does not substantively change OMB's previous guidance on PO&AMs. If a software producer cannot attest to one or more of the practices identified on the attestation form, M-22-18 still allows an agency to use the software if the producer (1) identifies the practices to which they cannot attest, (2) documents practices they have in place to mitigate associated risk, and (3) submits a satisfactory POA&M to the agency. M-23-16 clarifies that the agency also must seek an extension of the attestation deadline from OMB and submit a copy of the producer's POA&M, or else discontinue use of that software.

Wiley's Government Contracts and Telecom, Media & Technology practices will continue to monitor developments in this area and other emerging technology issues that affect contractors.