wiley

ALERT

OMB Rescinds Secure Software Development Mandate in Favor of a Risk-Based Approach

January 29, 2026

On January 23, 2026, the Office of Management and Budget (OMB) reversed some relatively new requirements for secure software development that had been imposed on federal contractors. This move is notable because the attestation previously required had created some uncertainty. OMB issued a new memorandum adopting a risk-based approach to software and hardware security that rescinds the Biden Administration memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, and the companion memorandum M-23-16. Memorandum M-22-18 had imposed a requirement that federal agencies get a self-attestation from software producers stating that the producer complies with certain secure development practices identified in National Institute of Science and Technology (NIST) Special Publication 800-218: *Secure Software Development Framework* before the agency could use their software. M-22-18 also instructed the Cybersecurity and Infrastructure Security Agency (CISA) to create a Common Form to be used to collect those attestations.

OMB's January 23 memorandum (M-26-05) doesn't roll back all the federal software security steps taken in the prior administration. It continues to require agencies to maintain a complete inventory of software and hardware and to develop assurance policies and processes "that match their risk determinations and mission needs." In addition, agencies may still choose to use the Common Form and resources CISA developed under M-22-18, or they can develop their own risk-based approach to ensuring software and hardware security, which could include requiring producers to provide a software bill of materials (SBOM).

Authors

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Government Contracts

Privacy, Cyber & Data Governance

Background. In May 2021, the Biden Administration issued Executive Order 14028, "Improving the Nation's Cybersecurity" which, as we previously covered, instructed NIST to issue guidance identifying standards, procedures, or criteria to strengthen the security of the software supply chain. In September 2022, the OMB issued a guidance memorandum, 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. The requirement applied to new software developed after September 14, 2022, and major version changes to existing software after that date. Executive Order (EO) 14144, "Strengthening and Promoting Innovation in the Nation's Cybersecurity," issued in January 2025, provided additional direction to CISA and the FAR Council to adopt "more rigorous" third-party risk management practices. In June 2025, the Trump Administration then issued EO 14306, "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144," rescinding large portions of EO 14144 and requiring the Director of NIST to develop guidance that demonstrates the implementation of secure software development, security, and operations practices based on NIST SP 800-218.

To implement the requirements of M-22-18, CISA in 2024 developed a Common Form for self-attestation as we covered previously here. CISA's development of this Common Form was subject to public input and received 110 sets of comments. CISA finalized the form after addressing the public comments, and it was being used by agencies.

OMB's January 2026 memorandum (M-26-05) noted that M-22-18 imposed unproven and burdensome software accounting processes that prioritized compliance over genuine security investments and diverted agencies from developing tailored assurance requirements for software and hardware threats.

Agencies were instructed to maintain a complete inventory of software and hardware and develop software and hardware assurance policies and processes that match their risk determinations and mission needs. Agencies may choose to use the government-wide secure development resources developed under M-22-18, such as the Common Form, making use of the Common Form now optional.

Note for cloud service providers. M-26-05 includes a note that agencies adopting contractual terms for cloud service providers should specify that the producer must provide an SBOM of the runtime production environment upon request.

What should the private sector focus on now? Although M-26-05 seeks to alleviate potentially burdensome software accounting processes that applied broadly to all software and hardware developed for use by federal agencies, it does not eliminate agencies' obligations to ensure security of the software and hardware they purchase. To that end, agencies may continue to require SBOMs or other artifacts before adopting hardware and software for use. In terms of risk, some agencies may place a lower priority on requesting, obtaining, and verifying software security information based on the software being used or the mission being served, which in turn may lower some information gathering and reporting effort and risk for contractors and their partners.

In practice, it is unclear whether agencies will adopt more agency- or contract-specific approaches or continue to use CISA's Common Form to maintain inventory of hardware and software used. In the short term, we would expect contractors to see continued use of the Common Form or contract-specific requests unless and until agencies develop broader guidance or contract terms addressing what type of information they require and how they will collect that information. Agencies may also need to revise their policies if regulations are issued under open FAR Case 2023-002, under which the FAR Council was developing a proposed rule to standardize Supply Chain Software Security as directed in the same Biden Administration Executive Order that prompted OMB M-22-18 and M-23-16. Though several requirements promulgated in the Biden EOs have been amended, issuance of Trump EO 14306 and other activities confirm that software supply chain security remains a priority for the Trump Administration.

As we previously recommended, software producers should stand ready to determine their ability to complete attestation forms and generate SBOMs or other artifacts the government may request. Contractors that purchase software for delivery to the government should also review their current supplier arrangements and consider whether modifications are needed to be able to access sufficient information to respond to agency requests for information.