EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

January 23, 2026

M-26-05

MEMORANDUM TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Adopting a Risk-based Approach to Software and Hardware Security

Federal agencies depend heavily on commercial off-the-shelf hardware and software to support their missions. As a result, agencies must rely on hardware and software producers to ensure that their products are secure and therefore resilient against attacks by increasingly sophisticated cyber threat actors.

Each agency head is ultimately responsible for assuring the security of software and hardware that is permitted to operate on the agency's network. There is no universal, one-size-fits-all method of achieving that result. Each agency should validate provider security utilizing secure development principles and based on a comprehensive risk assessment.

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (M-22-18), imposed unproven and burdensome software accounting processes that prioritized compliance over genuine security investments. This policy diverted agencies from developing tailored assurance requirements for software and neglected to account for threats posed by insecure hardware. Accordingly, OMB Memoranda M-22-18 and M-23-16, a companion policy, are hereby rescinded.

Agencies shall continue 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 software development resources developed under M-22-18, such as the Secure Software Development Attestation Form. Agencies may also choose to adopt contractual terms that require a software producer to provide a current software bill of materials (SBOM) upon request.[1] Additionally, agencies can reference the following for additional information and options:

- NIST SP 800-218, *Secure Software Development Framework*, and associated appendices;

[1] For a cloud platform, agencies adopting such a contractual term should specify that the producer must provide an SBOM of the runtime production environment upon request.

- Cybersecurity and Infrastructure Security Agency (CISA), 2025 Minimum Elements for a Software Bill of Materials (SBOM) (published in draft form on Aug. 22, 2025); and

- CISA, A Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management (Sept. 2023).