wiley

ALERT

What Does CISA's Secure Software Development Form Mean for Contractors?

April 1, 2024

WHAT: The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) published the final version of its Secure Software Development Attestation Common Form (Common Form) and announced availability of the Repository for submission of software producers' completed Common Form and any related artifacts. CISA has also released a User Guide for the Repository.

WHEN: CISA published the final version of the Common Form on March 11, 2024, and announced availability of the Repository on March 18, 2024.

WHAT DOES IT MEAN FOR INDUSTRY: The release of the Common Form kicks off the compliance timeline: Agencies must start collecting attestation letters for "critical software" three months after the release (June 8, 2024), and for all other covered software within six months (September 8, 2024).

CISA intends for the Repository to be the primary vehicle by which software producers may submit a completed Common Form and artifacts. The User Guide provides instructions for using the Repository. Yet some uncertainties still remain because the FAR Council has not yet revealed its proposed rule (FAR Case No. 2023-002), which would be needed to convert this effort from an internal agency compliance requirement to part of the larger acquisition process.

Purpose of CISA's Common Form

Authors

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

Cybersecurity
Government Contracts
National Security
Privacy, Cyber & Data Governance

Following the issuance of Executive Order 14028, the Office of Management and Budget (OMB) issued a guidance memorandum, OMB M-22-18, that requires agencies to obtain a self-attestation of compliance with the National Institute of Standards and Technology (NIST) SP 800-218 Secure Software Development Framework from software producers for agencies to use that producer's software. This requirement applies to new software developed after September 14, 2022, and major version changes to existing software after that date. A second memorandum, M-23-16, revised the deadline for agencies to collect software self-attestations, tying it to CISA's release of the final Common Form: Agencies must start collecting attestations for "critical software" three months after the Common Form is released and for all other software within six months.

In 2023, CISA released a draft version of the Common Form for public comment (which we previously covered here). In the final version released in March 2024, CISA made a few changes from the draft version of the Common Form:

- **Third-Party Assessments.** The final Common Form more prominently states that the software producer may choose to demonstrate conformance with the minimum requirements by submitting a third-party assessment documenting that conformance with the NIST Framework (i.e., a third-party assessment performed by a Third Party Assessor Organization (3PAO) that is either FedRAMP certified or approved in writing by an appropriate agency official). To rely on a third-party assessment, the software producer must check the appropriate box in Section III of the Common Form and attach the assessment to the form. Notably, if electing to demonstrate performance by submitting a third-party assessment, the software producer need not sign the form.
- **Signatory Authority.** The final Common Form clarifies that a form may be signed by the Chief Executive Officer (CEO) of the software producer or their designee, who must be an employee of the software producer and have the authority to bind the corporation.
- **Incorporation of Third-Party Software.** The final Common Form includes language from OMB M-23-16 explaining that third-party software incorporated into a software product does not itself require an attestation. This appears to remove a potential obligation for software producers to collect attestations from their own suppliers or subcontractors.

What is the purpose of the Repository?

CISA intends for the Repository to be the primary vehicle by which software producers may submit a completed Common Form and artifacts. Software producers that are unable to submit the form through the Repository may email a PDF version of the form to the relevant agency.

What should contractors expect next?

Agencies now face a deadline to begin collecting self-attestations. Although we expect many agencies to use the Common Form, OMB guidance leaves the door open for attestations to be supplied in other ways. Notably, OMB's initial guidance in M-22-18 "encouraged," but did not require, agencies to use a standard self-attestation form. Agencies may also develop their own forms with supplemental attestations or require additional materials as part of the attestation.

Although OMB and CISA have designed these rules to affect software that agencies purchase through procurement contracts, they have been careful to direct any requirements or guidance internally – towards agency personnel. Section 4 of Executive Order 14028 leaves it up to the FAR Council to prescribe "contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, [the SSDF]." The FAR Council has submitted a proposed rule to implement this requirement, and we expect to see that in the coming weeks. Until then, OMB's guidance will still require agencies to obtain attestations before "using" covered software, but agencies will not have a standard approach for obtaining those attestations from the entities that sell them the software.

Wiley's cross-disciplinary Government Contracts, National Security, and Privacy, Cyber & Data Governance teams are well-positioned to help large and small businesses understand their compliance and attestation requirements in the areas of Cybersecurity, National Security, and Government Contracting.