wiley

ALERT

CISA Seeks Comments on New Security Attestation for Software Procurements

April 28, 2023

On April 27, 2023, the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) issued a Notice of Agency Information Collection Activities to solicit public comments on a draft self-attestation form (the Common Form) to be completed by software producers (an entity that "manufactured/compiled the software product" at issue) 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. Software producers will be required to meet the SP 800-218 requirements, and attest to meeting those requirements, before their software may be used by federal agencies.

The Notice seeks input on "any aspect" of the Common Form, including the instructions. Public comments are due by June 26, 2023.

Background: In May 2021, the Biden Administration issued Executive Order (EO) 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 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 NIST SP 800-218 from software producers before using their software. This requirement applies to new software developed after September 14, 2022 and major version changes to existing software after that date.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Cybersecurity
Government Contracts
National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology

To implement this requirement, CISA developed a draft Common Form for self-attestation that, if approved by OMB, could be used by other government agencies to obtain the required self-attestations from software producers. The Notice anticipates that CISA's Common Form will provide minimum compliance requirements, but other agencies may add agency-specific requirements subject to OMB clearance.

Areas for Comment: CISA requests input on any aspect of the Common Form, including the instructions. CISA noted that it is particularly interested in comments on whether:

- The proposed information collection to implement EO 14028 and OMB guidance will have practical utility;
- CISA has accurately estimated the burden of the proposed information collection;
- There are other ways CISA can enhance the quality, utility, and clarity of the information to be collected; and
- CISA can minimize the burden of the information collection, such as through electronic submissions or automated collection.

What software is covered? The following software requires self-attestation: (1) software developed after the issuance of OMB M-22-18 (released September 14, 2022); (2) existing software that is modified by major version changes after that date; and (3) software to which the producer delivers continuous changes to the software code. "Major version changes" include using a semantic versioning schema of Major.Minor.Patch, or where the software version number goes from 2.5 to 3.0. Software developed by federal agencies or that is freely obtained (e.g., open source) do not require a self-attestation. Also, if the relevant software has been verified by a certified FedRAMP third party assessor organization (3PAO) or other 3PAO approved in writing by the appropriate agency official, based on NIST guidance, the software producer does not need to submit an attestation but must provide documentation from the 3PAO.

What information is requested from software producers? In Section I of the Common Form, software producers would indicate to which products the attestation applies by selecting whether the attestation applies company-wide, to a specific product line, to an individual product, or to multiple products or specific product versions (to be identified by name, version number, and release date). Section II requests software producer contact information. Section III provides the text of the attestation itself. In the attestation, the software producer must affirm that it makes consistent use of approximately 18 software development practices that are "derived from" NIST SP 800-218. If applicable, the software producer would also indicate any addendums or documents attached to the attestation.

Can agencies demand more than the attestation? Agencies may add agency-specific requirements to CISA's Common Form, which will set forth "minimum requirements." The Common Form notes that agencies may request additional documents, such as a Software Bill of Materials (SBOM) or documentation from a 3PAO.

What if a software producer cannot attest to meeting all of the practices identified in the form? In accordance with the guidance provided by OMB in M-22-18, CISA instructs that if a software producer cannot provide a completed self-attestation from, a federal agency must (i) obtain documentation from the software producer identifying the practice(s) to which the software producer cannot attest, (ii) document the practices the agency has in place to mitigate resulting risks, and (iii) require the software producer to provide a plan of actions and milestones (POA&M). Under OMB's guidance, if the agency finds the software developer's documentation "satisfactory," the agency may use the software despite the producer's inability to provide a complete self-attestation.

How will be form be submitted? CISA proposes that the Common Form be a fillable PDF form accessible on CISA's website. CISA also proposes that software producers would submit the form electronically either through its website or via email.

What is the estimated burden on software producers? CISA states that it estimated the number of DHS respondents, number of DHS responses, and time required to complete form submissions as follows:

- CISA assumes that each year, DHS vendors would produce 2,689 initial form submissions and half as many resubmissions due to major software changes per year, based on initial contract award data for Fiscal Years 2019-2022. CISA's estimates do not include vendors for other agencies across the government that may also use the Common Form.
- CISA estimates that a software producer would require 3 hours and 20 minutes to review the form and understand the requirements, gather information, review, and approve the release of information and submission for an initial submission, comprised of 3 hours for a software quality assurance analyst or tester and 20 minutes for the Chief Information Security Officer (CISO). These estimates are based on OMB's 2020 estimate that government contractors would require 3 hours to collect information related to compliance with the requirements of Section 889 Part A, prohibiting government procurement of certain telecommunications and video surveillance equipment.
- CISA estimates that resubmissions would require 1 hour and 30 minutes for a software quality assurance analyst or tester and 20 minutes for the CISO.
- CISA also estimates a total annual opportunity cost of $923,623.00 for the DHS information collection based on hourly compensation rates for the assumed reviewing parties: $67.90 per hour for a software quality assurance analyst or tester, and $177.66 per hour for a CISO.
- CISA also assumed that additional documents, such as SBOMs, would be readily available and would not have to be generated specifically for doing business with the government.

What will the government do with attestations and information? CISA, working with OMB and GSA, will establish a centralized repository for self-attestations and artifacts with protections to allow sharing among agencies. CISA is charged with demonstrating an initial operating capability for the repository within 18 months after OMB establishes the requirements.

What should the private sector focus on now? Software producers should identify any software that is covered by the attestation requirement and determine their ability to complete the current version of the form and generate SBOMs or other artifacts the government may request, and whether the burdens of doing so exceed CISA's estimates. Contractors that purchase software for delivery to the government should also review their current supplier arrangements and consider whether modifications are needed to comply with the attestation requirements.