THE COALITION
FOR GOVERNMENT PROCUREMENT

June 26, 2023

Robert J. Costello
Chief Information Officer
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380

Subject: Comments on Secure Software Development Attestation Common Form, Docket # CISA–2023–0001

Mr. Costello,

The Coalition for Government Procurement ("the Coalition") appreciates the opportunity to comment on the Secure Software Development Attestation Common Form released by the Cybersecurity and Infrastructure Security Agency (CISA). The proposed secure software attestation form seeks to require software producers to attest that software used by the government meets the minimum secure software development requirements identified in the form. The Coalition timely submits these comments within the 60-day comment period ending June 26, 2023.

By way of background, the Coalition is a non-profit association of firms selling commercial services and products to the Federal Government. Its members collectively account for a significant percentage of the sales generated through GSA contracts, including the Multiple Award Schedule (MAS) program. Coalition members also are responsible for many of the commercial item solutions purchased annually by the Federal Government. These members include small, medium, and large business concerns. The Coalition is proud to have collaborated with Government officials for more than 40 years in promoting the mutual goal of common-sense acquisition.

The Coalition outlines herein the following aspects of the proposed secure software attestation form that appear burdensome, ambiguous, and/or problematic for its members.

- Notification Obligation
- Third Party Assessments
- Burden of Proposed Collection of Information
- Scope of Software Impacted

Each of these topics are addressed herein, along with suggested remediation.

Notification Obligation

Currently, the CISA attestation form requires that a software producer notify "all impacted agencies if conformance to any element of the attestation is no longer valid." This requirement for software producers to notify every agency if there is a change to the attestation is cumbersome and problematic. First, a software producer may not have insight into the total number of agencies using its software, particularly if the software is being sold through a reseller or distributor. Therefore, it is unrealistic to expect the software producer to be able to notify all impacted agencies. Second, this requirement imposes a new reporting burden on the software producer on top of current notification requirements in the cybersecurity and supply chain space, and otherwise (to include DFARS 252.204-7012, FAR 52.204-25, FedRAMP, and additional cyber threat and incident information reporting FAR requirements that are forthcoming). As CISA will be maintaining the attestations on behalf of the government, the Coalition requests removing this requirement entirely or, if left in, revising it to allow for any notifications process to be centralized through CISA. Notifying one agency, CISA, of any changes to the attestation is a much more reasonable ask of software producers. There is precedent for centralized reporting for cyber-related concerns. DFARS 252.204-7012 requires reporting of any cyber incidents to the DIBNET through a secure channel.

Third Party Assessments

The Coalition notes some conflicting language in the self-attestation form relating to third party assessments. The form states software producers of software verified by a FedRAMP third party assessor organization (3PAO) and approved in writing by an agency official will not need to submit an attestation provided relevant documentation from the 3PAO is submitted, but the attestation form then includes a box for the software producer to attest that the software has been verified by a 3PAO and directs the producer to attach the documentation.

- Does the software producer need to fill out the self-attestation form if the verified 3PAO documentation is submitted?
- Is the attestation in this case limited to checking the box regarding the 3PAO assessment at the end of the form?
- How will documentation from a 3PAO be collected and maintained?

Burden of Proposed Collection of Information

The CISA proposed attestation form and the rulemaking's analysis of burden estimate that the burden of collecting the information for submission to CISA and signing the form will take roughly 3 hours and 20 minutes. This purported burden grossly underestimates the amount of time it will take for a company, particularly a company that is not FedRAMP certified, to ensure compliance with the Secure Software Development Framework, validate compliance, coordinate a response to the form, get buy-in throughout the company, and have a C-suite executive sign off on the form. Further, if a company has particular standards to which it cannot attest compliance, the company must put together a Plan of Action and Milestones (POA&M) for submission to the government which requires additional time and effort on the part of the company. The Coalition

urges CISA to update the estimated burden of collection to reflect the complexities of complying with the attestation requirement.

Scope of Software Impacted

OMB Memorandum M-22-18 and OMB Memorandum M-23-16 require software producers to attest compliance with the secure software development practices for any software that "affects" government information or will be used on government information systems. As defined by the Memoranda, the term "software" includes "firmware, operating systems, applications, and application services (*e.g.*, cloud-based software), as well as products containing software." Memorandum M-23-16 then outlines three categories of software to which these requirements will apply: (1) software developed after September 14, 2022, (2) software modified by one or more major version changes after September 14, 2022, or (3) software that is a hosted service that deploys continuous updates.

The Coalition has outstanding questions about the scope of the requirements as they apply to commercially available off-the-shelf (COTS) products, Internet of Things (IoT) products, medical devices at Federal healthcare facilities, office equipment and peripherals, and all other hardware products that contain software and connect to agency information systems. With respect to IoT, the National Institute of Standards and Technology (NIST) has developed recommended cybersecurity criteria and a voluntary labeling program in response to Executive Order 14028. Consistent with this initiative, the Coalition urges the government to consider excluding these types of products from the attestation form requirements or providing additional time for producers of these products to complete the attestation form. Similarly, for COTS products, the Coalition recommends that the government exclude such software that is not considered "critical," or allow more time for producers of non-critical COTS products to complete the form.

Other Comments

Other specific comments and questions raised by members appear in the appendix attached hereto.

The Coalition hopes you find these comments useful and thanks you for your time and consideration. If you have any questions, I may be reached at (202) 315-1053 or rwaldron@thecgp.org.

Regards,

Roger Waldron
President

Secure Software Self-Attestation Draft Form Member Questions and Comments		
#	Topic/Number of Attestation Requirement	Comment or Question
1	Applicability of Attestation	Would software currently in the sustaining phase of its development be exempt from attestation, given that only software developed after September 14, 2022, existing software modified by major version changes, and software that undergoes continuous changes such, as SaaS products, requires self-attestation?
2	Origin of Attestation	For acquired software from third parties, must the contractor providing the software provide the attestation or the OEM?
3	Open Source and Freely Obtained Software	How do the attestation requirements apply to freely obtained software (freeware, open-source software) provided to the government by a contractor?
4	Attestation Requirement 1c, pg. 4	Can network segmentation be used as a substitute for multifactor authentication?
5	Attestation Requirement 3, pg. 5	Must a separate attestation ever be provided for (i) third-party commercial code integrated into software and/or (ii) third-party open-source code? Or are provenance data sufficient?
6	Timeline for Additional SSDF Tasks	Is there a timeline in place for requiring all 42, rather than 31 of 42, tasks for self-attestation?
7	Attestation Requirement 3, pg. 5	Will software producers be required to demand SBOMs from their vendors or suppliers? If so, under what conditions?
8	Attestation Requirement 3, pg. 5	Must a separate attestation ever be obtained for tools used in the production of software, such as compilers, scanners, linters, integrated development environments *etc.*?

9	Attestation Requirement 4c, pg. 6	Vulnerability disclosure programs typically allow the public to report a vulnerability and access the status of known vulnerabilities in commercially available software. For contractor-developed software not distributed outside of the Government, a public-facing vulnerability disclosure program may not be desirable or feasible (e.g., due to classification of vulnerabilities). Vulnerability disclosure and accepting reports would be limited to secure channels and/or mediated by the government. What constitutes an acceptable definition of "operating a vulnerability disclosure program?" The NIST 800-218 RV 1.3 language, "have a policy that addresses vulnerability disclosure and remediation, and implement the roles, responsibilities, and processes needed to support that policy," requires a policy, not a vulnerability disclosure plan.