THE COALITION
FOR GOVERNMENT PROCUREMENT

December 15, 2023

Subject: Secure Software Self-Attestation Common Form
ICR Reference No. 202311-1670-001

To Whom It May Concern:

On November 16, 2023, the Cybersecurity and Infrastructure Security Agency (CISA) released a Request for Comment soliciting feedback on a draft Secure Software Development Attestation Common Form, which the agency developed based on the National Institute of Standards and Technology's Secure Software Development Framework (SSDF) and in consultation with the Office of Management and Budget. By this letter, The Coalition for Government Procurement (Coalition) timely submits its comments on this draft Secure Software Development Attestation Common Form.

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 General Services Administration (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 asserts the following recommendations:

- **Recommend re-assessing or clarifying the triggers for requiring a new attestation**. Currently, the Common Form requires attestation for "existing software that is modified by major version changes (*e.g.*, using a semantic versioning schema of Major.Minor.Patch, the software version number goes from 2.5 to 3.0) after September 14, 2022"; and for "software to whose code the producer delivers continuous changes (such as software-as-a-service products or other products using continuous delivery/continuous deployment)." We recommend that CISA consider whether a periodic attestation requirement (*e.g.*, annually or every 3 years) may offer a more streamlined requirement for software producers.

- **Recommend clarifying the scope of notification requirements**. The current draft requires the software producer to attest "the company will notify all impacted agencies if conformance to any element of this attestation is no longer valid." Frankly, this notification obligation is unrealistic, as it is very difficult for companies that sell to multiple agencies or through a reseller. There should be one point of contact for reporting (*i.e.*, CISA). Additionally, we request that CISA clarify the following for the final version of the attestation form:
    - What is the threshold for notification where there may be small or temporary changes that impact the attestation?
    - Are there any timelines associated with this required notification?
    - Is the software producer required to notify the agency prior to every update to the attestation?
    - How does this reporting requirement harmonize with existing reporting requirements (*i.e.*, DFARS 252.204-7012 reporting requirements)?

- **Recommend clarifying the scope of "software" impacted.** The Coalition recommends clarifying whether the attestation form is applicable 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.

- **Recommend revising the Burden Statement to reflect accurately the burden associated with completing this attestation.** The attestation form states the following about the information collection burden:

    > information collection is estimated at 3 hours and 20 minutes per response, including time for reviewing instructions, searching data sources, gathering, and maintaining the data needed, and the completing and reviewing the collected information.

    The form requires ***the CEO*** of a company to "attest that all requirements … outlined are consistently maintained and satisfied[,]…" and that the company involved "will notify all impacted agencies if conformance to ***any element*** of [the] attestation is no longer valid." [Emphasis added.]

    The Coalition believes that requiring an attestation by the CEO of an organization (which might operate globally) is quite challenging in and of itself, but requiring it to be made based on only 3 hours and 20 minutes of data collection is wholly unrealistic.

To understand the administrative (and legal) burden here, CISA might imagine the effort involved with securing such information and assuring its sufficiency so that the Secretary of Homeland Security could commit personally to its veracity in court or before Congress under oath. The Department would have to cascade the information review through all of its constituent agencies, secure the required information, and validate its veracity at multiple levels up the chain. Now, from the corporate standpoint, add to that due diligence activity the associated personal risk to the CEO and the corporation of falsely certifying, even inadvertently, the submission under the attestation. That risk would drive an extra layer of review.

The sum total of activities involved in completing the attestation simply could not be accomplished in the time identified. For this reason, the Coalition believes the burden associated with this software attestation should be revisited and reassessed with empirical data that accounts for the risk that is associated with the head of a private sector organization making such attestations.

The Coalition greatly appreciates the opportunity to submit these comments on the draft Secure Software Development Attestation Common Form and hopes you find them useful. If you have any questions, I may be reached at (202) 315-1053 or rwaldron@thecgp.org.

Thank you for your time and consideration of the Coalition's comments.

Sincerely,

Roger Waldron
President