Cybersecurity Coalition

June 23, 2023

Robert J. Costello
Chief Information Officer
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Dear Mr. Costello,

The Cybersecurity Coalition ("Coalition") submits these comments to the Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security regarding our concerns with the implementation of the *secure software self-attestation common form* and its process. We hope that the issues detailed below will lead to further clarification and revision so that the underlying intent of the secure software self-attestation can be adequately complied with by industry. Thank you for continued willingness to collaborate on this issue.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services, who are dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace and effective policy environment that will encourage companies of all sizes to take steps to improve cybersecurity risk management.

The Coalition has suggested redline edits to the attestation form and would like to highlight the following recommendations concerning the form:

1. **Notification of Changes or Validity of Attestation**

The Coalition has concerns over the viability and appropriateness of the attestation's requirement to "attest the company will notify all impacted agencies if conformance to any element of this attestation is no longer valid." There are several practical issues with this statement. The software producer may not be reasonably aware of all agencies that could be impacted by the invalidation of an attestation. Additionally, the software producer may not be the distributor or seller of the software to the government and will have no insight into the customers of the product.

Furthermore, this aspect of the text is fundamentally a contractual commitment rather than an element of attestation. Many organizations will ultimately delegate the Chief Executive Officer's responsibility to sign these attestations to another employee. This designated employee may not be in a position to make this kind of contractual commitment on behalf of the organization. The Coalition recommends striking this section from the form.

2. **Provenance**

The Coalition would like to highlight the difficulty of complying with Section III's fourth requirement – that "the software producer maintain[] provenance data for internal and third-party code incorporated into the software." The government has acknowledged that technology is not currently available to do this in automated fashion. Complying with this requirement through manual processes is exceptionally burdensome, especially for small and medium sized organizations, and particularly as it concerns open-source code. Furthermore, the Coalition is concerned about ambiguity around what constitutes adequate 'provenance data,' within the meaning of the NIST definition of provenance from SP-800-53 r5[1], especially as it concerns elements that may be the result of third-party development, such as open-source projects that may have scores of contributors. For example, the likelihood that all personnel involved in third-party development, especially in cases of older open-source projects, could be determined is extremely unlikely in many cases The Coalition recommends that the attestation form be revised to state that the provider has made a "good-faith effort" to maintain provenance data, and that "provenance data" be clarified to mean "if the software producer uses a third-party library (proprietary or open source), they will need to keep information about attributes of the acquired library in addition to when and where it was retrieved".

3. Software Bill of Materials (SBoM) Language

The second paragraph within the section *Additional Information* contains a lengthy discussion of SBoM. This section is unnecessary as it is not a requirement for the purposes of this attestation form. The inclusion of SBoM in this section is likely to cause confusion and conflates the processes by which organizations carry out secure software development with artifacts of those processes (such as SBoMs). The Coalition recommends removing this paragraph entirely.

4. Burden Statement

The Burden Statement included in the Secure Software Development Attestation Form unduly minimizes the impact this required attestation process will have on software suppliers to the Federal Government.

In particular, the Coalition believes the government's estimate that the burden to complete necessary information collection is only 3 hours and 20 minutes substantially understates the time associated with completing the self-attestation, even by software providers who are currently adhering to secure development processes.

For example, completing the self-attestation may require the development of entirely new processes to assure the corporate signatory that the statements are true and correct. In large companies with thousands or even tens of thousands of software product development and infrastructure support staff, that may mean gathering confirmatory information from many disparate sources and implementing new workflows, training, and processes for documentation. Once the initial implementation is in place, the overall burden to the software provider may be reduced, but 3 hours and 20 minutes is far from an accurate representation of the full scope of the compliance burden.

[1] https://csrc.nist.gov/glossary/term/provenance#:~:text=2-,The%20chronology%20of%20the%20origin%2C%20development%2C%20ownership%2C%20location%2C,NIST%20SP%20800%2D53%20Rev.

5. Minimum Attestation References – Table

The Coalition believes the table under the *Minimum Attestation References* section may cause confusion. It is unclear to many organizations that this table is intended to be a helpful mapping rather than a binding checklist of items that must be complied with. We recommend that the table be moved into an annex and its purpose as a reference table be clearly articulated.

6. Sections 3 & 4

Section 3 and 4 in the table are swapped with sections 4 and 3 in the attestation form. We recommend swapping sections 3 and 4 in the table for consistency.

7. POA&M Guidance and Waivers

The current text specifies that "Further guidance on extension and waiver requests for agencies can be found on the relevant MAX page, along with agency guidance on the collection of POA&Ms." The coalition appreciates the additional guidance regarding POA&Ms in OMB memo 23-16, however the guidance will likely result in different requirements from different agencies for the same product. The Coalition recommends that POA&Ms be standardized across all agencies.

The Coalition appreciates the continued engagement on this issue and we hope that the above comments and recommendations are useful to your ongoing work. As the conversation around this topic continues to evolve, we would welcome the opportunity to further serve as a resource on both technical and policy questions to ensure that the secure software self-attestation process strikes the right balance between effectiveness and efficiency for both the public and private sector.

Respectfully Submitted.

The Cybersecurity Coalition