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

Via www.regulations.gov

June 26, 2023

Dear Mr. Costello:

BSA | The Software Alliance appreciates the opportunity to provide comments in response to the Department of Homeland Security's Request for Comment on Secure Software Development Attestation Common Form (Docket No. CISA-2023-0001).

BSA is the leading advocate for the enterprise technology sector. Our members are among the world's most innovative companies and help to drive digital transformation by providing the solutions that make businesses and government agencies more competitive and effective, including cybersecurity; identity, credentialing, and access management; human resources management; customer relationship management; design and modeling; collaboration and communication; data analytics, visualization, and backup; and ticketing and workflow solutions.

BSA has consistently and energetically supported efforts to improve software security including those called for in the Administration's May 2021 Executive Order on Improving the Nation's Cybersecurity (EO 14028), and March 2023 National Cybersecurity Strategy. Indeed, improving software security is the first priority in BSA' s 2023 Global Cyber Agenda and our commitment to software security led us to develop the BSA Framework for Secure Software, which is cited heavily in the National Institute of Standards and Technology's Secure Software Development Framework (SSDF).

With regards to the attestation form specifically, software producers should make good-faith, reasonable, and risked-based decisions. BSA recommends DHS edit the opening sentence to include that the attestation is made in good faith, and the attestor will make reasonable, and risk-based use of the practices in the attestation form.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

BSA offers the following additional comments and recommendations aimed at achieving the general goal of improving software security and the specific goal of improving the software and cybersecurity of US Government agencies.

I. DHS Should Ensure the Attestation Advance Broader Security Goals

A. Improve Software Security by Developing a Safe Harbor

The attestation form identifies multiple Administration priorities aimed at improving software security, including EO 14028 and the National Cybersecurity Strategy. These documents suggest shifting responsibility to software producers while simultaneously providing software producers that leverage best practices a safe harbor from liability. As the National Cybersecurity Strategy, Strategic Objective 3.3 states, "the Administration will drive the development of an adaptable safe harbor framework to shield from liability companies that securely develop and maintain their software."

BSA recommends DHS design the attestation form for the purpose of satisfying the requirements of a safe harbor identified in Strategic Objective 3.3 and support the use of the form for that purpose.

B. Support Reciprocity with FedRAMP

The draft attestation form provides that if a third-party assessor organization (3PAO) certifies the software using NIST guidance, then the software producer does not need to submit the attestation form.

It makes sense that a software producer that is certified under FedRAMP would be exempt from submitting an attestation form, as the SSDF practices and tasks reflected in the attestation form reference the security controls in NIST SP 800-53, a central element of FedRAMP. However, the attestation requirements do not necessarily always perfectly align with FedRAMP requirements.

BSA recommends DHS clarify that, even when a FedRAMP certification does not perfectly align with the requirements of the attestation, certification from a 3PAO meets the requirement for the attestation form.

BSA further recommends that if a 3PAO has provided relevant documentation to the Federal Government as part of the FedRAMP process, then it need not provide the same relevant documentation as part of the attestation form process. This change would ensure the new common form process is integrated into existing FedRAMP processes as seamlessly as possible.

II. DHS Should Clarify to What Statements a Software Producer Must Attest

The attestation form has 5 numbers, 11 letters, and 2 small roman numerals, as well as 52 related SSDF practices and tasks. OMB and CISA have stated in recent meetings that software producers will be required to attest to the statements contained in the numbers and the letters but not to the SSDF practices or tasks.

In the context of DHS's explanation, the form is less clear. For example, it does not make sense for a software producer to attest to the statement in Section 2, i.e., "The software producer has made a good-faith effort to maintain trusted source code supply chains by:" A plain reading of Section 2, suggests that a software producer would not be required to attest to the number, as OMB and CISA explained, but only to the letters in Section 2.

BSA recommends, to simplify and clarify the attestation form, DHS make the attestation form a one-level list of statements to which DHS will require a software producer to attest. BSA further recommends that DHS eliminate the SSDF practices or tasks from the attestation form, for reasons further explained in Section V below.

III. DHS Should Remove Extraneous Material from the Document

The material provided currently includes extraneous information that produces more questions, opportunities for misinterpretation, and opportunities to undermine the purpose of the attestation form.

BSA appreciates DHS's effort to "show its work," provide software producers with a helpful map to SSDF practices and tasks and clarify that agencies may request additional information from a vendor. However, including such information undermines the goal of the *common* attestation form, which is supposed to streamline the process and not create just another form for software producers to complete before they complete separate forms for every US Government agency.

Additionally and importantly, with regards to the SSDF practices and tasks, and the references to SBOMs, even if the attestation form itself states "this form does not require software vendors to use each of the practices and tasks identified or produce an SBOM," experience teaches us that the inclusion of such information creates the possibility that agencies will either misinterpret the attestation form to require a software producer attest to each practice or task or provide an SBOM or to believe that requiring a software producer to undertake each practice or task or provide an SBOM is worthwhile and thus require it.

BSA recommends DHS remove any material from the document except those statements to which a software producer must attest. As noted above, the attestation should be limited to the requirements, nothing else.

BSA further recommends that, to support the Administration's goals of harmonization, DHS and OMB actively encourage agencies to require *only* the common attestation form, after they have published the final version of the common form through compliance with the Paperwork Reduction Act.

IV. DHS Should Clarify the Substance of Portions of the Attestation Form

DHS can address much of the ambiguity of the attestation form by changing the structure, but some language in the attestation form needs further clarification to help software producers understand their obligations and ultimately help DHS achieve its goals.

A. Section 1: Eliminate or Clarify the Meaning of "developed and built in secure environments"

As currently drafted, and pursuant to DHS's explanation that a software producer must attest to the numbers and letters, the attestation form requires a software producer to attest that "The software was developed and built in secure environments." It is not reasonable for a software producer to attest to an environment being "secure." If a software producer is the victim of a cyber incident, then that attestation will, by definition, be false. In reality, risks, for example zero-day vulnerabilities, will always exist.

Software producers should manage risks to their development environments in good-faith, making reasonable, and risk-based decisions.

BSA recommends DHS eliminate Section 1 and make a) through f) standalone statements to which a software producer would attest. If, however, DHS intends a software producer to attest to developing and building in secure environments, then DHS should publish a definition of what that means and provide stakeholders an opportunity to comment on that definition.

B. Section 3: Eliminate Substantially Similar Requirements

As drafted, Sections 3 and 2 a) are substantially similar. Section 3 requires a software producer to attest that it "employs automated tools or comparable processes in a good faith effort to maintain trusted source code supply chains" while Section 2 a) requires a software producer to make a "good-faith effort to maintain trusted source code supply chains by a) employing automated tools or comparable processes."

BSA recommends DHS eliminate Section 3.

C. Section 5 a): Align the Subsection with Other Statements

Section 5 a) requires a software producer to "ensure" its processes operate on an ongoing basis, which sets an unreasonable standard to satisfy.

BSA recommends DHS edit Section 5 a) to read "The software producer operates these processes on an ongoing basis and, at a minimum, prior to product, version, or update releases."

D. Section 5 b): Align Expectations for Vulnerability Response with Best Practices for Risk Management

Section 5 b) requires a software producer to have a policy or process to address discovered security vulnerabilities prior to product release and operate a vulnerability disclosure program.

As the US National Cybersecurity Strategy notes, "the most advanced software security programs cannot prevent all vulnerabilities" and the multi-lateral document "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default" acknowledges that even software that is secure-by-design "will continue to suffer vulnerabilities." Importantly, not all vulnerabilities are exploitable, and vulnerabilities that are exploitable do not all present the same risk.

BSA recommends DHS improve Section 5 b) by editing it to read: The software producer has a policy or process to make risk-based determinations to respond to known, exploitable vulnerabilities.

E. Section 5 c): Use Internationally Recognized Standards for Coordinated Vulnerability Disclosure

Section 5 c) requires a software producer to attest that it operates a vulnerability disclosure program.

The cybersecurity community has developed internationally recognized standards in ISO/IEC 30111 and 29147. These internationally recognized standards were endorsed by Congress in the Cyber Incident Reporting for Critical Infrastructure Act, Division Y, H.R. 2471 (P.L. 117-103), which directs the Director of CISA to "develop principles that govern the time and manner in which information relating to a security vulnerability may be shared

consistent with common industry best practices and United States and international standards."

Further, pursuant to the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), subsection (d)(1), agencies are required to use internationally recognized standards to carry out their policy objectives.

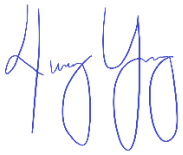
Software producers should manage vulnerabilities good-faith, reasonable, and risk-based decisions.

BSA recommends DHS edit Section 5 c) to read: c) The software producer follows internationally recognized standards to operates a vulnerability disclosure program.

V. Conclusion

BSA appreciates the opportunity to provides comments on the draft attestation form. We hope DHS will strengthen the attestation form by ensuring that the attestation form is aligned with and supports the Administration's broad software security goals; removing material that could be misinterpreted; and clarifying the substance of the statements to which a software produce must attest.

We look forward to continuing to work with DHS on this important issue.



Henry Young
Director, Policy