Robert J. Costello
Chief Information Officer
Cybersecurity and Infrastructure Security Agency
1110 North Glebe Road
Arlington, VA 20598

Via regulations.gov

December 18, 2023

Mr. Costello:

BSA | The Software Alliance[1] appreciates the opportunity to provide comments in response to the Cybersecurity and Infrastructure Security Agency's (CISA) Request for Comment on CISA's Secure Software Development Attestation Form.

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 driven policies and identified best practices to improve software security. One example of these efforts is the BSA Framework for Secure Software, which contains the organizational processes and product security capabilities that combine to improve software security, and which the National Institute of Standards and Technology (NIST) reflected in its Secure Software Development Framework (SSDF).

BSA supports the goal of CISA's efforts but notes three general concerns.

First, it is unclear if US Government efforts are harmonized. The National Cybersecurity Strategy states plainly, the US's "strategic environment requires . . . regulatory frameworks

[1] Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, HubSpot, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Palo Alto Networks, Prokon, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

that are harmonized to reduce duplication." US Government efforts to improve cybersecurity, software security, and supply chain security, for example, the Federal Risk and Authorization Management Program (FedRAMP), the Cybersecurity Maturity Model Certification program (CMMC), are not clearly coordinated.

Second, CISA's estimated burden is significantly lower than the true burden. Given the number, specificity, and ambiguity of the statements in the draft attestation form, as well as the potential consequences for incorrectly attesting to those statements, completing the form will take much longer than the three hours and twenty minutes CISA estimates. The draft attestation form further burdens software producers by requiring a Chief Executive Officer (CEO) or Chief Operations Officer (COO) sign the form.

Third, and illustrated in Section 9, below, CISA could improve the form by simplifying it and having each statement stand on its own. Multi-level lists with introductory phrases, some but not all of which appear to be statements to which a software producer must attest, impede the purpose of the form.

Improving software security is the top priority in BSA's 2024 Global Cyber Agenda. For this reason, BSA supports CISA's efforts to improve software security. We provide the below comments that, if addressed, will increase the likelihood that CISA's efforts deliver on our shared goal: a more secure future.

I. Update the Effective Date of the Attestation Form

The form requires attestations for software "developed after September 14, 2022." It is unrealistic to require specific attestation statements for software developed more than a year ago, when these requirements did not exist.

BSA appreciates CISA engaging with industry in developing the attestation form. One consequence of this engagement is that CISA may obtain feedback and make meaningful changes. Software producers may not be able to attest to these new and improved statements retroactively.

In consideration of the engagement and the potential improvement to the attestation form, CISA should update the effective date of the form to software developed at least 90 days after CISA publishes the final version of this document.

II. Clarify that the Form does Not Include Software Developed at the Direction of a US Government Agency

The form states that software developed by US Government agencies is not within scope of M-22-18, as amended by M-23-16, and does not require attestation.

CISA should clarify that software developed by a US Government agency includes software developed at the direction of a US Government agency. The goal of the attestation form is to obtain assurance that a software producer developed the software securely. This goal would be achieved through the software producer performing the agency's requirements under the contract, operating within an agency's development environment, or working at the direction or under the oversight of the agency.

Requiring an attestation form for software developed at the direction of an agency would be redundant, unnecessary, and burdensome for both parties.

III. Remove the Requirement that a CEO or COO Sign the Form

As drafted, the attestation form requires the signature of a CEO or COO.

The purpose of the form can be achieved without requiring a CEO or COO to sign the attestation form. CEOs and COOs are not typically present for the day-to-day implementation of secure software development practices. Consequently, a leader with the appropriate job scope, who leads these activities will be in a better position to attest to the statements in the form and accomplish CISA's stated purpose.

Moreover, and noted above, the number of hours necessary to complete the form increases dramatically when the ultimate signatory is a CEO or COO. While removing the requirement that a CEO or COO sign the attestation form does not fully address the burden of completing the form, it would at least not add to that burden.

Lastly, in the context of Title 32 § 2004.34 Foreign Ownership, Control, or Influence, this requirement may be problematic for software producers that are headquartered outside the United States.

IV. Extend the Exclusion for Open-Source Software to All Open-Source Software and Clarify that Software Producers are Attesting Only to the Software They Develop

The attestation form requires a software producer to attest to statements that become unclear in the context of open-source software. One example is that the attestation form states that "In signing this attestation, software producers are attesting to adhering to the secure software development practices outlined in Section III" a change from the original language, "In signing this attestation, software producers are attesting to the secure development of code developed by the producer." A second example is the statement that a software producer attest to "a) Separating and protecting each environment involved in developing and building software."

The Office of the National Cyber Director recognized in its Request for Information on Open-Source Software Security: Areas of Long-Term Focus and Prioritization, open-source software provides "immense benefits" and "enables software development at an incredible pace and fosters significant innovation." Given this context, it appears that the form is not intended to undermine the development and use of open-source software. However, to support efforts to improve open-source software security and the innovation that open-source software enables, CISA should revert to the original language and clarify that the attestation form only requires a software producer to attest to the secure development of code it produces.

V. Strike the phrase “The software is developed and built in secure environments”

As drafted, Section 1) requires a software producer to attest that “The software is developed and built in secure environments.”

It is unclear what it means to attest to this statement. One potential understanding would render an attestation false if, ultimately, a malicious actor breaches the environment, even if the malicious actor uses a zero-day vulnerability to accomplish its mission, a vulnerability which the attestor could not have been aware of when attesting to the statement. Alternatively, that statement could be read as an introductory statement to which a software producer need not attest.

As BSA advocated in our June 26 response to CISA's Draft Attestation Form, and above, CISA should only include those statements to which a software producer is attesting and not include any preliminary or introductory phrases or sentences to which the software producer is not attesting. Such an approach would make the form clearer, and is illustrated in Section 9, below.

If this language remains in the form, it should be amended to read, “the software producer seeks to develop and build in secure environments through the following actions:” to reflect the reality that producers strive to develop and build software in secure environments.

VI. Align Attestation Language to Avoid Ambiguity

As drafted, Section III currently contains two general attestation statements, one of which requires a software producer to attest that it “makes consistent use of the following practices” but a second of which requires a software producer to attest that “all requirements outlined above are consistently maintained and satisfied.”

Rather than having separate statements, we suggest CISA use a single statement that provides that a software producer has, in good faith, taken reasonable, risk-based, and consistent steps to use the practices identified in the form and report to CISA if there are material changes to its attestation. Such an approach would achieve CISA’s goal by setting the expectation that security risks are managed by undertaking the practices set forth in the form.

VII. Replace the Phrase “in a manner that minimizes security risk” with “using a risk-based approach”

As drafted, Subsection 1) c) requires a software producer to attest to “enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk.”

This language may create a misunderstanding to require a software producer to relegate all other considerations, for example, functionality, to "minimize security risk." The result of this misunderstanding could be software that does not function or is not affordable but might be relatively secure. Rather, a software producer should attest to enforcing multifactor authentication and conditional access "using a risk-based approach." This change more accurately reflects CISA's goal as well as the reality of how software producers develop and deploy their products and services, and agencies' business needs.

VIII. Use a Risk-Based Approach to Address Vulnerabilities

As drafted, Subsection 4) c) requires a software producer to attest to operating a vulnerability disclosure program and addressing disclosed vulnerabilities in a timely fashion and according to any timelines specified in the vulnerability disclosure program or applicable policies.

As the National Cybersecurity Strategy states "even the most advanced software security programs cannot prevent all vulnerabilities." When determining when and how to address a vulnerability a software producer should consider numerous variables. These variables include whether the vulnerability is known to be exploited by a malicious actor as well as the severity of the vulnerability, but also the reproducibility of the exploit, dependencies, attack vector, and the expected time to produce a patch or implement a compensating control, among others. The existence of these important variables underscores why these decisions are context dependent and therefore must be risk-based.

The SSDF task Respond to Vulnerabilities (RV) 1.3 recommends software producers "have a policy that addresses vulnerability disclosure and remediation, and implement the roles, responsibilities, and processes needed to support that process" but notably and in contrast with Subsection 4) c), does not recommend action within certain timelines.

To meet the direction of Executive Order 14028, that a US Government agency may only use software if a software producer attests to using "secure software development practices drawn from the SSDF," and the attestations form's statement that the practices in the form were "derived from the secure software development framework" we recommend fidelity to the language from RV 1.3 of the SSDF.

If the Form continues to refer to timelines for accepting, reviewing, or addressing vulnerabilities, then it should explicitly support a risk-based approach. Not every vulnerability is exploitable or poses risks to product security, and software producers should take a risk-based approach to decisions about when and how to address vulnerabilities.

IX. Simplify the Attestation Form

BSA suggests CISA use a single-level list with each statement standing on its own. We suggest CISA use the following structure and statements, which track CISA's draft attestation form and include the suggested improvements noted above.

1. The software producer developed the software in environments secured by separating and protecting each environment it used in developing and building software.

2. The software producer developed the software in environments secured by regularly logging, monitoring, and auditing trust relationships used for authorization and access to any software development and build environments and among components within each environment.

3. The software producer developed the software in environments secured by enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software using a risk-based approach.

4. The software producer developed the software in environments secured by taking consistent and reasonable steps to document, as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software.

5. The software producer developed the software in environments secured by encrypting sensitive data, such as credentials, to the extent practicable and based on risk.

6. The software producer developed the software in environments secured by implementing defensive cybersecurity practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents.

7. The software producer made a good-faith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities.

8. The software producer maintains provenance for internal code and third-party components incorporated into the software.

9. The software producer employs automated tools or comparable processes that check for security vulnerabilities at a minimum, prior to product, version, or update releases.

10. The software producer has a policy or process to address discovered security vulnerabilities prior to product release.

11. The software producer has a policy that addresses vulnerability disclosure and remediation, and implements the roles, responsibilities, and processes needed to support that policy.

* * *

As we stated in BSA's 2024 Global Cyber Agenda, experience has taught us that the most effective laws and policies are built on public-private partnerships. Each of the above comments provide a path to improved software security but aim to reduce negative or unintended consequences. By updating the effective date, clarifying how this effort interacts with other similar efforts, clarifying how this effort implicates open-source software, and simplifying and streamlining some of the statements, CISA can make a significant step toward that goal. The result of addressing these comments will be more secure software, a robust digital ecosystem, and better tools for departments and agencies to leverage to serve citizens.

Thank you for your time and consideration.

Henry Young
Director, Policy