U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

December 18, 2023

Via email: www.regulations.gov

Robert J. Costello
Chief Information Officer
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, DC 20528

Re: Agency Information Collection Activities: Request for Comment on Secure Software Development Attestation Common Form; Docket No. CISA-2023-0001 (*Federal Register*, November 16, 2023)[1]

Dear Mr. Costello:

The U.S. Chamber of Commerce welcomes the opportunity to comment on the draft Secure Software Development Attestation Common Form (the common form), administered by the Cybersecurity and Infrastructure Security Agency (CISA). The Chamber strongly supports the development of secure software products. We value having had the opportunity to comment this past June on the initial draft of the common form, which was initially released in April 2023. However, the Chamber urges CISA and the Office of Management and Budget (OMB) to delay completing the common form for several reasons:

First, our fundamental concern centers around software providers giving the federal government assurances that software used by agencies is securely developed—an effort that requires joint problem solving by CISA, OMB, and the business community. In our June letter, we offered some constructive options that could address the needs of government and industry to varying degrees. CISA, OMB, and software providers share a desire for innovative approaches to software security that can lead to sustainable policies and security practices.

Second, it is unclear to us why CISA and OMB have released the common form for another round of feedback when a number of business policy priorities and recommendations are not adequately reflected in the latest proposal. Indeed, the Chamber's central goals—mitigating liability and driving harmonization—are not embodied in the common form or related policies.

Businesses that provide software to federal agencies are, by necessity, customer oriented. One company shared, "We want to do the right thing and keep providing strong software to the government, but we need a common form that reflects more give and take between agencies and producers. This effort is a new one, and we need to build trust in the process, particularly around legal liability." The company added, "Public-private partnerships require a two-way street. Our concerns and suggestions related to the common form are not reflected in the November draft. If anything, our concerns have only increased." Nonetheless, the company said that it wants to build lasting relationships with agencies and achieve security outcomes vis-à-vis the common form that work for government and business.

Third, many individuals and organizations from both the public and private sectors believe that the current 30-day comment period is insufficient to address questions about the common form, such as its underlying details and requirements. Instead of finishing work on the common form at the end of the comment period, CISA and OMB should extend their conversations with private entities. The Chamber would like to engage CISA and OMB, as we did in May, to better understand officials' thinking on the latest draft. We want to help them develop sound and sustainable policy.

CISA and OMB should allow more time for public and private stakeholders to analyze, discuss, and provide meaningful input on the common form, which will greatly benefit the government and the business community in the long run. In the remainder of this letter, the Chamber spotlights two portions of its June comments—key points and an appendix—for further consideration by CISA and OMB. We also pose some questions, reflecting stakeholders' critique of the November draft of the common form, which we urge CISA and OMB officials to discuss with us in early 2024.

I. KEY POINTS

A safe harbor should be a leading priority for the administration, consistent with the White House's *National Cybersecurity Strategy* (NCS). CISA and OMB are urged to ensure that software producers are protected from regulatory and legal liability if they build their software in accordance with the common form.

- CISA and OMB say that they are not contemplating some form of liability protections (e.g., a legal safe harbor) for software producers, but such thinking undercuts a core element of the NCS. The strategy says that in order to "shape standards of care for secure software development," the administration will "drive the development of an adaptable safe harbor framework to shield from liability companies that securely develop and maintain their software products and services."

- The NCS adds that the safe harbor "will draw from best practices" for secure software development, such as the National Institute of Standards and Technology's (NIST's) Secure Software Development Framework (SSDF).

- The NCS calls for shifting liability onto entities that "fail to take reasonable precautions to secure their software." The strategy further calls for holding businesses liable when they fail to live up to a duty of care, which the common form promotes.

- The NCS clearly advocates for a safe harbor, but the common form effort still needs to include it. The administration should integrate a safe harbor into the common form. It is unclear how this administration and future ones will enforce or verify software producers' conformance with the common form. Software producers are concerned that they could be unfairly exposed to legal actions by an agency or a third party in the wake of a cybersecurity incident.

Harmonization and reciprocity need policymakers' attention. The administration is urged to create a workable reciprocity regime involving the common form, FedRAMP, and multiple agencies.

- CISA and OMB have said that reciprocity between common form attestations and FedRAMP is a work in progress. The Chamber urges CISA and OMB to explain their efforts in this area before the common form is finalized. Harmonization and reciprocity is a leading Chamber goal.

- Agency officials say that an important goal of the common form is to enable software producers to attest to their specific products once and have several agencies leverage the form—sign once, use many times. A business told the Chamber that OMB needs to clarify the applicability of existing FedRAMP authorizations for cloud service providers so that FedRAMP-authorized providers don't have to provide separate software attestations.

- To further illustrate, a number of software producers have expressed uncertainty about reciprocity between their attestations to the common form vis-à-vis (1) their existing FedRAMP certifications and (2) multiple federal agencies that may use the common form.

- The business told the Chamber, "The paragraph about FedRAMP assessments [on p. 4 of the April common form/p. 7 of the November common form], which refers to relevant NIST guidance, stands out. We predict that there will be significant confusion over how to apply these provisions, given that M-22-18 [amended by OMB memorandum M-23-16] is based on the SSDF, while FedRAMP is usually tied to other NIST publications. The two are similar, but not the same."

- A firm added, "Getting reciprocity between the common form and FedRAMP locked down is all the more crucial given the modernization of the FedRAMP program."

Government officials are underestimating the burdens and costs associated with the common form. The comment periods have not given industry enough time to undertake a fair accounting of the qualitative and quantitative aspects of common form compliance and a software producer's related obligations.

- The burdens and costs tied to the common form attestations are probably not realistic when factoring in the following activities: (1) identifying the multitude of components used in developing software, (2) documenting the environments where they are acquired and placed in software end product(s), (3) collecting code provenance data, and (4) providing common forms and other information to agencies.

- It remains unclear to many in industry when and how often a common form must be submitted to an agency. What officials consider a major version change could vary within an agency as well as among them. Greater clarity on these issues could considerably change the cost calculations connected to the attestations.

- To help ameliorate costs, the administration should not prescribe granular mandates on how software is produced—but, in the spirit of the SSDF, focus on the practices or the processes used within a software producer's environment. CISA and OMB should focus on "the importance of processes," a company told the Chamber. Delivered artifacts for any individual product should not be overly emphasized as a means of demonstrating compliance. Rather, the focus of policy should be on the best practices that a software producer runs its products through to deliver software more securely.

- One firm said to the Chamber, "Looking at the language of the attestation text, there are parts that still use ambiguous language. [Our firm] has questions about subsections 1(a)–(c) [on p. 8 of the April common form/p. 6 of the November common form]." Among other things, the firm indicated, it will be important to know whether—

    - One "environment" has to be both separated and protected from another environment or environments.

    - "Components" need separate logging, monitoring, and auditing for authorization and access.

    - An "environment" requires both multifactor authentication and conditional access.

- The firm added, "The common form isn't self-explanatory. If [CISA and OMB] leave these ambiguous concepts in the common form [which the November draft does], it will be helpful if they permit software producers to attach explanatory materials to ensure that an agency and the software provider are not miscommunicating about the meaning or scope of the attestation."

- What's more, the government is downplaying the cost of providing agencies with additional attestation artifacts or documentation, especially a software bill of materials (SBOM). A business told the Chamber that SBOMs are not always going to be readily available and may have to be generated specifically for doing business with the government. “This is because an SBOM is not the only way to manage a vulnerability, nor has it been the primary way for private entities to assess third-party software.”

- The business noted, “Many companies have other tools available to track third parties’ software vulnerabilities. The breadth and complexity, among other issues, pertaining to SBOMs does not render them a silver bullet.”

- Furthermore, the business said, “We are concerned about disclosing SBOMs to agencies due to the subjectivity of the attestation form and SBOMs being dynamic and untested. Our concern is heightened in light of the False Claims Act (FCA), which presents an ambiguous risk to us and many other entities depending on how the common form and the FCA are enforced.”

- The business continued, “There is also a misleading assumption seemingly held by some federal officials that SBOMs should already exist and, therefore, should not be included in a software producer’s responses and cost calculations. This misunderstanding about future costs is particularly concerning to industry.”

Guardrails need to accompany government requests for attestations and artifacts. The common form and harmonization will only work if agencies are dissuaded from making data requests beyond a software producer’s attestation.

- The Chamber believes it is helpful that the approximately 60 minimum attestation references on the common form were placed in an appendix [pp. 8–9 of the November proposal] to reinforce statements made by CISA and OMB that they are guidance and not a checklist.

- Still, multiple businesses interpret the provisions cited in Executive Order (EO) 14028 and the practices and tasks in the common form as strict requirements for producing software—not as guidance, despite assurances from agency officials. After all, such thinking is particularly reasonable given the administration’s push for cybersecurity regulation.

- Similarly, industry parties are concerned that substantial confusion surrounds the common form, likely leading to suboptimal security outcomes for both software producers and their agency customers. Businesses contend that reasonable guardrails should accompany both the common form’s attestation requirements and any additional artifacts or documentation that the common form refers to.

- CISA and OMB officials say that agencies are not expected to issue their own common form, which is positive. These officials are commended for getting several agencies to collaborate. However, the Chamber thinks that the common form and harmonization efforts will only work if agencies are dissuaded from asking for information requests beyond a software producer's attestation. This point cannot be emphasized enough.

- A company told the Chamber, "The common form needs guardrails to have meaning—or scope creep will set in." It said that the government needs to issue guidance saying that if a business' software is verified by a third party assessment organization, or 3PAO, then it should not need to submit ad hoc artifact requests to agencies.

References to an SBOM should be removed from the common form. Among other reasons, policymakers have no apparent plan for streamlining agency SBOM requests.

- It seems that no change was made to the common form concerning an SBOM. The Chamber isn't opposed to SBOMs, particularly for groups that choose to use them and when an entity receiving the SBOM has the agency to make required security updates. But we strongly believe that federal policymaking on an SBOM is far too immature, including lacking in interagency streamlining, for agencies to request SBOMs without creating considerable burdens and confusion, particularly for small and midsize businesses.

- It is the Chamber's view that references to an SBOM should be removed from the common form. (The November draft common form mentions SBOMs.) Among other reasons, policymakers, including the administration and Congress, have no apparent plan for how they will harmonize agency requests for SBOMs.

- The Chamber's June letter suggests a middle-ground approach, which could be for the common form to make explicit that maintaining an SBOM—that is, to demonstrate provenance—is wholly *optional* for software producers. The common form calls on a software producer to maintain provenance data for internal and third-party code incorporated into the software end product. Federal officials have suggested that by having an SBOM, an entity has "provenance covered."

- A business told the Chamber that provenance is a gray area. "Software producers need flexibility in demonstrating compliance with this requirement without SBOMs becoming mandatory."

- The Chamber urges policymakers to exclude software-as-a-service (SaaS) products from any SBOM requirement due to the conceptual challenges of generating timely and useful SaaSBOMs.

- A firm said, "First, SaaS applications are inherently dynamic, with code and configurations frequently updated more than once a day. Any supplied SaaSBOM would be out of date shortly after it was generated. Requiring SaaS providers to produce and constantly update SBOMs could pose an undue burden and impede innovation, which should be weighed carefully against the security benefits gained by such rapid processes."

- The firm continued, "As the National Telecommunications and Information Administration notes in its report on SBOMs, SaaSBOMs are of minimal use to customers or end users for the purposes of vulnerability management, because they are neither responsible for nor capable of remediating any issues in question.[2] Given these challenges, we recommend instead measures to provide transparency into SaaS tools (e.g., through submissions of FedRAMP authorizations and sharing of continuous monitoring data, including response times to emergency directives)."

Industry needs greater clarity on rulemakings that govern the common form. At the time of this writing, a Federal Acquisition Regulation (FAR) case has been initiated to implement section 4(n) of EO 14028, requiring software providers to attest to the common form, but substantive details and next steps are unclear.

- The Chamber asked federal officials whether all agencies, including the Department of Defense, will be implementing the requirements in M-22-18, amended by OMB memorandum M-23-16, or just a subset via a rule(s).

- An open FAR case is expected to implement section 4(n) of EO 14028, requiring "suppliers of software available for purchase by agencies to comply with, and attest to complying with, applicable secure software development requirements in accordance" with the common form, apparently.

- It is the Chamber's understanding that government officials may not speak to the details of the FAR in advance of the publication of the rule. Thus, it remains unclear whether policymakers intend to issue separate regulations to implement (1) M-22-18 and M-23-16 (making its provisions contractual requirements) and (2) the common form. It is also unclear whether the regulations flow down to the suppliers of prime contractors.

II. QUESTIONS FOR CONSIDERATION BY CISA AND OMB (SELECTED EXAMPLES)

Appendix B of this letter—which is basically a redline of section III of the April version of the common form—was included in the Chamber's June letter to CISA and OMB. Few of our changes were incorporated in the November version of the common form. The common form is largely unchanged from April despite much constructive input from business organizations.

- **Will CISA and OMB explain their views on the Chamber's recommendations?** Underpinning the Chamber's thinking is that software security will be better enhanced if federal policymakers and software producers apply some guiding practices and principles—particularly ones involving a good-faith effort, risk-based decision making, and reasonableness—to the entire common form. Such guiding practices and principles are not reflected in the latest draft of the common form.

- **Why does the common form require the signature of a software producer's chief executive officer (CEO) or—newly added to the November proposed common form—a chief operating officer (COO)?** A firm told the Chamber, "This mandate is inconsistent with the spirit of the EO and OMB memorandums M-22-18 and M-23-16. In particular, a CEO or COO is not directly involved in the security operations at the ground level; this role is better fulfilled by a more appropriate designee."

  The objectives of the common form can be achieved without requiring a CEO or COO to sign the attestation form. The firm added, "CEOs and COOs are not typically present for the day-to-day implementation of secure software. A person who leads these activities will be in a better position to accomplish CISA's stated purpose."

  One organization added, "The work hours needed to complete the form will increase dramatically when the signer 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 exacerbate that burden."

- **What more can CISA and OMB do to clarify that software and components developed for or at the direction of federal agencies are not within the scope of M-22-18/M-23-16 and, hence, do not require attestation?** Policymakers should clarify that software and components developed for or at the direction of a federal agency are, by definition, "software developed by agencies"—and thus out of scope for compliance with the common form. "Some private entities," a business told the Chamber, "are already operating within federal development environments, including under the direction and oversight of federal agencies. We are already accountable to these agencies and their leadership."

- **How can officials extend the exclusion for open-source software beyond what is directly procured by the federal government?** Put another way, how can officials clarify that software producers are only attesting to the secure development of the code that they develop and not third-party components? An organization told the Chamber, "In meetings with industry earlier this year, CISA and OMB said that software producers are not required to attest to the compliance of third-party components with the common form. However, the revised form amends language in section I that should have confirmed this position." (See the excerpted text below.)

  The organization added, "We request that CISA and OMB honor their statements, confirming that software producers are only required to attest to the secure development of code they produce and that a software producer's attestation does not extend to third-party components.

  - April common form (p. 7)
    "Note: In signing this attestation, software producers are attesting to the secure development of code **developed by the producer**." This attestation is targeted in scope.

  - November common form (p. 5)
    "Note: In signing this attestation, software producers are attesting to **adhering to the secure software development practices outlined in Section III**." This attestation is overly expansive in scope and unworkable.

- **Has CISA and OMB established a repository to securely store common form and/or a plan of action and milestones (aka a POA&M)?** A firm told the Chamber that "the collection of common forms and/or PO&AM should not start until a repository is completed. If a detailed POA&M is expected from software producers, the resulting document will contain highly sensitive information. The government needs to ensure that common form and/or POA&M-related documentation is secured by appropriate controls and not posted publicly."

  The firm added, "Having collection requirements but no centralized and safe way to protect sensitive and proprietary materials will elevate security risks. These forms will contain information about what software is deployed and where throughout the federal government. In the event that there is a discovered and exploitable software vulnerability in a particular software product, these forms could serve to facilitate a potentially devastating cyberattack against agencies that have deployed this software product."

  Further, the firm noted, "Having a secure and centralized repository in place will facilitate software producers' reporting of major version changes to their software, while also dramatically reducing the likelihood of agency confusion."

- Also, the firm said, "The language in the draft common form stating that a software producer must 'notify all impacted agencies if conformance to any element of this attestation form is no longer valid' should be deleted. Rather, for clarity and effectiveness, a producer's obligation should only be to report material changes to attested software—and then only report to CISA, not to all federal agencies. CISA should have the responsibility to identify and notify agencies that are impacted by such material changes, whether through the use of a central repository or some other secure means."

***

Thank you for the opportunity to provide CISA and OMB with comments on the November 2023 version of the proposed common form. If you have any questions or need more information, please do not hesitate to contact me (meggers@uschamber.com).

Sincerely,

Matthew J Eggers

Matthew J. Eggers
Vice President
Cyber, Space, and National Security
Policy Division
U.S. Chamber of Commerce

Appendix B

Preliminary Recommended Edits to Section III of the Draft Common Form

There is basic agreement between government and industry in support of developing secure software products. The Chamber wants to engage CISA and OMB, among other agencies, on our preliminary revisions to the common form. Our approach focuses on using sound software risk management practices and principles to strengthen cybersecurity. The Chamber believes that software security will be better enhanced if federal policymakers and software producers apply some guiding practices and principles—particularly ones involving a good-faith effort, risk-based decision making and reasonableness—to the entire common form.

The common form's attestation requirements reflect this important thinking, including by referring to "minimized security risk" in part 1 and "good-faith effort" in part 2. The Chamber's targeted changes will further assist agencies and software producers in applying these actions and concepts more fully to better mitigate risks and threats. In sum, government and industry have a mutual interest in fostering optimal cybersecurity outcomes by driving closer relationships between efficient risk management and software security.

Please note that the Chamber's preliminary recommended edits to the common form should not be construed as an endorsement of it.

***

Section III

Attestation and Signature

Part 1. The Chamber believes that the first sentence could be interpreted as requiring perfect software security by conclusively saying that software is "developed and built in secure environments." However, the practical reality is that software producers seek to develop and build in secure environments by following the requirements in part 1 [p. 7 of the common form]:

The Chamber recommends modifying the opening paragraph of the Attestation and Signature section (proposed additions in bold text).

On behalf of the above-specified company, I attest that [software producer] presently **and in good-faith** makes consistent**, reasonable, and risk-based** use of the following practices, drawn from the secure software development framework (SSDF), in developing the software identified in Section I [p. 5 of the common form]:[1]

[1] References to the common form pertain to the proposal released on April 27, 2023, unless otherwise stated.

1) The **software producer seeks to**~~ is~~ develop~~ed~~ and buil**d**~~t~~ in secure environments~~. Those environments are secured by~~ through the following actions, at a minimum:

a) Separating and protecting each environment involved in developing and building software;

b) Regularly logging, monitoring, and auditing trust relationships used for authorization and access:

i) to any software development and build environments; and

ii) among components within each environment;

c) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimized security risk;

d) 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;

e) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk;

f) Implementing defensive cyber security practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents;

2) The software producer has made a good-faith effort to maintain trusted source code supply chains by:

a) Employing automated tools or comparable processes; and

[Page break in original]

b) Establishing a process that includes reasonable steps to address the security of third-party components and manage related vulnerabilities;

Part 3. The Chamber recommends deleting part 3. It is essentially identical to part 2a). Note that subsection 2a) states, “The software producer has made a good-faith effort to maintain trusted source code supply chains by: a) Employing automated tools or comparable processes.” Part 3 states, “The software producer employs automated tools or comparable processes in a good-faith effort to maintain trusted source code supply chains.”

~~3) The software producer employs automated tools or comparable processes in a good-faith effort to maintain trusted source code supply chains;~~

4) The software producer maintains provenance data for internal and third-party code incorporated into the software;

Part 5. The Chamber also recommends making edits to part 5a) to reasonably alter an extremely difficult standard to satisfy. We suggest edits to parts 5b) and 5c) to align the requirements with consensus security vulnerability program practices. The Chamber's edits in parts 5b) and 5c) take into account the following—

- All software has vulnerabilities.

- Not every vulnerability is equally exploitable or poses identical risks to product security. Component integration and compensating controls could make it extremely unlikely that malicious actors will exploit a vulnerability.

- Software producers frequently manage software vulnerability risks by considering specific vulnerability risk levels and the criticality of data and systems that could be affected by a particular vulnerability.

Here are the Chamber's suggested edits to part 5 (proposed additions in bold text and deletions in strikethrough text):

5) The software producer employs automated tools or comparable processes that check for security vulnerabilities. In addition:

> a) The software producer ~~ensures~~ **operates** [Note: CISA and OMB agreed to incorporating "operates" in the November proposed common form. But this revision is modest compared to the Chamber's overall recommendations.] these processes ~~operate~~ on an ongoing basis and, at a minimum, prior to product, version, or update releases; and
>
> b) The software producer has a policy or process to **make risk-based determinations to remediate or otherwise appropriately address discovered security vulnerabilities that a software producer identifies as critical or high severity** prior to product release; and
>
> c) The software producer operates a vulnerability disclosure program and accepts, reviews, and **makes risk-based determinations to remediate or otherwise appropriately address** disclosed software vulnerabilities **that a software producer identifies as critical or high severity** in a timely fashion.
>
> **The software producer takes the following into consideration in making the risk-based determinations referenced in b) and c) above: the severity of a vulnerability, the likelihood that the vulnerability can be exploited, how product configuration or use may affect the vulnerability, potential mitigations against harm, and other relevant factors. The software producer takes the same**

considerations into account in determining target time frames for timely resolution of a vulnerability.

The Chamber believes that the two sentences struck through below should be deleted. Among other challenges, they are repetitive of the opening language beginning with “On behalf of the above-specified company. …” Also, they rely on impractical absolutes, such as the double use of “all” and “consistently maintained and satisfied.” This language does not track with software producers’ good-faith pursuit of building products securely and managing vulnerabilities based on risk.

In addition, the common form and the broader policy in which it resides do not feature a safe harbor for industry, which both the Chamber and the NCS support. In addition, software producers may be unaware of all 434 agencies[3] that use a software producer’s software.

[To the best of my knowledge [added to the November version of the common form,] ~~I attest that all requirements outlined above are consistently maintained and satisfied. I further attest the company will notify all impacted agencies if conformance to any element of this attestation is no longer valid.~~

[1] https://www.federalregister.gov/documents/2023/11/16/2023-25251/agency-information-collection-activities-request-for-comment-on-secure-software-development

[2] https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

[3] https://www.federalregister.gov/agencies
https://www.usa.gov/agency-index