June 26, 2023

Docket # CISA–2023–0001

Re: Agency Information Collection Activities: Request for Comment on Secure Software Development Attestation Common Form

The Cloud Service Providers-Advisory Board appreciates the opportunity to comment on this self-attestation form to be used by software producers in accordance with the Executive Order on Improving the Nation's Cybersecurity and the Office of Management and Budget's guidance in OMB M–22–18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices. Our feedback is detailed below.

The Cloud Service Providers - Advisory Board (CSP-AB) represents the world's leading cloud companies and supports standards and policies that promote and enable secure cloud adoption in the public and private sectors. Our member companies are global leaders in the drive to provide safe, scalable, and accredited digital government services, with a focus on both the civil servants delivering those services and the end-users receiving them.

FedRAMP Reciprocity

Cloud service providers (CSPs) who provide services to the Federal Government (IaaS, PaaS, SaaS) have invested heavily in developing expertise, internal processes, and security measures to become FedRAMP authorized. FedRAMP is already considered a high bar of compliance and along with the latest Rev. 5 Baselines which emphasize supply chain rather than creating a parallel and burdensome process for FedRAMP authorized providers to sell software to the Federal Government, we strongly encourage CISA and OMB to leverage the existing FedRAMP controls and processes to streamline CSP's ability to provide assurances towards the software attestation requirements.

The CSP-AB has provided a control mapping from the currently released self-attestation form to the latest Rev. 5 FedRAMP baselines (which has been shared with both FedRAMP and OMB). Based on this mapping exercise, the FedRAMP high baselines cover a majority of the relevant requirements of the common form. This parity should be leveraged either via direct reciprocity or via an official control level mapping (provided by CISA/OMB), prior to the date of first attestation submissions so that repeating the same processes would not be necessary (controls that the Federal government already has assurances for) and only the delta controls would need to be asserted in CSP attestations.

Harmonization Between Agencies

In addition to leveraging the FedRAMP authorization process, which includes attestation by an authorized 3PAO, to meet the common form's requirements the CSP-AB recommends that CISA and OMB provide specific guidance to Departments and Agencies that those organizations who are FedRAMP authorized meet the minimum security requirement set forth in the attestation form, and as such do not have to provide separate secure software attestation as well as subsequent artifacts. Further, we recommend the following be removed for the attestation form

"However, relevant documentation from the 3PAO is required" and the following added in its place "follow the standard FedRAMP process for additional documentation". This work would be inline with the Federal government's National Cyber Strategy (published in March 2023) that emphasizes harmonization between frameworks to get the best value out of each.

The CSP-AB also recommends removing the check box section that says "I attest that the referenced software has been verified by a certified FedRAMP Third Party Assessor Organization (3PAO) or other 3PAO approved by an appropriate agency official, and the Assessor used relevant NIST Guidance, which includes all elements outlined in this form, as the assessment baseline. Relevant documentation is attached". The statement above clarifies that CSPs do not need to attest if their software is verified by 3PAO, meaning they wouldn't be required to complete the form.

Reduce Burden of Artifacts

Even in cases where an agency accepts the attestation provided by a 3PAO, the current process allows agencies to require additional artifacts to support the attestation. A third party attestation by definition provides a higher level of assurance to agencies than a self-attestation would (as it is being adjudicated by an impartial third party), therefore the CSP-AB strongly recommends that 3PAOs who are already adjudicating high baseline authorization decisions, be directly leveraged to provide the highest level of assurance to federal agencies via incentivizing the 3PAO process over self-attestation. The CSP-AB strongly recommends that OMB/CISA put out additional guidance stating that follow up artifact requests be limited only to self-attesting software providers and for specific controls found to be in non-compliance by a 3PAO.

Time Burden

The CSP-AB believes that the common form's estimate of 3 hours and 20 min per response is an unrealistic time expectation, especially without regard for attestation level. There are member organizations who estimate 40 hours per "product" (Service) at minimum, and many of our member agencies provide hundreds of services to the federal government. Additionally, if a software producer uses a 3PAO, the time burden (and cost) significantly increases to include the time spent with the assessor to gather evidence and conduct the assessment. Finally, each attestation will have to go through thorough legal and technical review by each software provider, which adds to the time burden of the attestation. Based on all of the above the CSP-AB recommends the removal of the "3 hours and 20 minutes" time listed in the common form as well as a 180 day timeline for turnaround of the common form for critical services. To highlight the point, the original due date for CISA to establish a standard self-attestation common form was due on January 12, 2023 and even in June we are now wrapping up the comments period. There was a 6 month delay in creating the form; the same grace should be provided for software producers to be compliant with its requirements.

Software Bill Of Materials (SBOM)

While the current form does not mandate SBOMs as part of the minimum software security requirements, it does specifically call out SBOMs as an additional artifact that an agency may require. The software producer may be required to maintain an SBOM or potentially to attach an SBOM as an artifact supporting the attestation. We believe that SBOMs can serve as a tool in a software producer's overall vulnerability management approach, but providing the SBOM to federal government customers adds minimum security value, and may in fact lead to more opportunities for vulnerability exploitation, especially without an established secure repository. Departments and agencies have varying capabilities to safeguard the artifacts submitted by software producers, and therefore maintaining a software producer SBOM could be a liability for the federal government. Therefore, the CSP-AB encourages CISA to remove references to the collection of SBOMs from the common form as well as highlight alternative artifacts of provenance data outside of delivered SBOMs to agencies. For example, focusing on a software producer's ability to maintain provenance data versus sending SBOMs.

POA&M Process

The CSP-AB supports the ability for software producers to work with agencies to provide POA&Ms in lieu of self-attestation forms. This will allow agencies to continue using software while working with software providers to meet the requirements outlined in the form. CSP-AB encourages CISA and OMB to either allow direct POA&M mappings to be tracked via FedRAMP (so that it is a single carried issue that has proper visibility) or allow agencies to make risk based decisions based on the visibility of POA&Ms and not require additional waivers for continued use of any specific software. A blanket policy such as this for a new process goes against the best interest of federal agencies to accomplish their missions and does not allow proper iteration of the process.

Sincerely,

Laura Navaratnam

Executive Director

The Cloud Service Provider - Advisory Board

csp-ab.com