Cybersecurity Coalition

The Cybersecurity Coalition[1] represents numerous private sector organizations that include many of the leading cybersecurity and technology companies. We appreciate the Office of Management and Budget (OMB) giving industry the opportunity to provide responses to the questions posed in the document entitled *Implementation of Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4(k)*, released March 7th, 2022.

Please find our responses below. We welcome the opportunity to engage with OMB and other federal government departments and agencies to answer any further questions, and to ensure the success of this important initiative for all stakeholders.

1. **How would you describe the ideal process for Federal agencies to obtain and retain secure software development attestation documents for software being procured?**

   We recommend against being over prescriptive when defining how agencies should obtain and retain attestations until better understanding has been achieved on what approach will be most effective. As we note in several places, we believe that additional research and pilot programs are necessary before SSDF attestations can be required of software producers or used effectively by agencies. A significant part of this research and piloting must result in the identification and implementation of standards for attestation format and commonly acceptable approaches for sharing.

   Regardless of approach, key foundational elements must be:

   - Reusability. Any attestation, regardless of type, that is prepared for a software product procured by an agency should be reusable, to the maximum extent possible, by other agencies with a similar risk profile. For example, a shared service or blanket purchase agreements for a software product would include attestations that meet the agency requirements, precluding the need for additional attestations at the agency level.
   - Updateability. Software products and shared services change over time and attestations will need to be updated in a timely fashion to ensure they remain valid for the software product or shared service that are in use or being procured.
   - Accountability. Both the procuring agency and the software producer and or shared service provider should identify an accountable party as part of the

[1] https://www.cybersecuritycoalition.org/

attestation. This is necessary to ensure that as attestations are changed or expired, agency records are updated accordingly.

2. **Are there examples of successful systems, tools and procedures for assessing compliance that should be examined for applicability to the SSDF? What characteristics of other established processes are most important to emulate? Do you recommend any particular standard format(s) for attesting to compliance?**

   While this area remains immature, there is some work being done on a number of fronts. For example:

   - The Cloud Native Computing Foundation has a reference architecture currently in development that includes some guidance[2].
   - The Supply-chain Levels for Software Artifacts (SLSA)[3] has published work in this area.
   - Open Security Controls Assessment Language (OSCAL) being worked on at NIST has been highlighted as a possible mechanism for communication attestation elements[4].

   However, none of these efforts represent a widely adopted standard at this time nor does the Coalition explicitly endorse any one approach. Instead, we recommend that the federal government identify opportunities to pilot multiple approaches to determine what the most effective will be. While conducting pilots will take time and effort, the resulting lessons learned will result in a more robust and impactful adoption of SSDF requirements, tied to risk, and implemented efficiently.

3. **Are there elements of the framework for which there are alternate and potentially more effective ways (e.g., conformity assessments) of demonstrating adoption than Attestation?**

   For systems that are low risk, we recommend that self-attestation be the most acceptable and preferred method. Third-party assessments can be costly and time consuming, a problem that only gets worse as the rate of software updates increases, and in continuously updated cloud systems.

   We recognize that with higher-risk systems, third-party assessments and potentially more detailed artifacts may be necessary to ensure the appropriate level of assurance, but again point out that the more stringent the requirements, the more time and effort will be necessary to produce what is required.

[2] https://github.com/cncf/tag-security/blob/main/supply-chain-security/supply-chain-security-paper/CNCF_SSCP_v1.pdf

[3] https://slsa.dev

[4] https://pages.nist.gov/OSCAL/

4. **What risk-based factors should be considered to determine when third party attestation is most appropriate for affirming adequate SSDF practices are in place?**

   Efforts to prescribe risk factors on a broad scale routinely fail to capture risk appropriately. Instead, each agency should use the existing risk management methodology and system rating (Low, Moderate, High) as the basis for any decision regarding the appropriate level of assurance in affirming that SSDF practices are being implemented by the software producer.

   Further, each department and agency (and components within) will have varying mission processes which could mean that the level of assurance needed for a specific piece of software will be different depending on the mission. That is, the same software being deployed in a Low-risk system, will have different assurance requirements than that same software being deployed in a High risk system.

5. **How should vendors articulate the products and the boundaries of the products covered within the attestation?**

   Software producers (aka "vendors") should be given flexibility to establish the elements and boundaries of their products in whatever way is consistent with own development strategy. Allowing this flexibility enables software producers to articulate the boundaries once so that they can be reused and avoid the need for customized attestations for each consumer and purpose of the software in government systems.

   Boundaries can be demonstrated using data flow diagrams that expose where communications into and out of a product exist. Where those data flows cross a product boundary can be considered the product's authorization boundaries.

   It is important to note that any attestation will be tied to a specific version of software and/or a point in time related to the procurement date. It will be incumbent upon the procuring agency to recognize this and ensure that their records are kept up to date. In the absence of doing so, attestations that were once accurate, may not keep pace with changing software or requirements.

6. **What information do vendors need in advance in order to comply with implementation Guidance?**

   It is essential for federal departments and agencies to prioritize, based on risk, the systems and associated software where SSDF requirements should apply. Any form of attestation requires a significant level of detailed and technical effort by software producers to create and share. It also requires a sophisticated level of knowledge and operational experience on the part of agency software procurement officials to receive, process, and address to meaningfully benefit from these attestations. The aggregate level of effort across all agencies, the USG as a whole, and their collective software producers is difficult to calculate in advance but will represent significant resource allocation that will likely detract from other important security efforts. Prioritizing systems and software based on risk will help to reduce the level of effort while still ensuring that SSDF principles are applied where they are most impactful to improving security.

Further, , standards for the format and common acceptable approaches for sharing attestation information, as well as high-level and low-level (where deemed appropriate by an agency) artifacts, are necessary to ensure consistency and reduce agency and software producer confusion. Historically, other sectors (healthcare, financial services, etc.) are influenced by the requirements that the federal government requires of its suppliers. Given the significant overlap in software used across all sectors, that trend is likely to continue as it pertains to SSDF requirements. A failure to achieve broad adoption of standards and formats for artifacts will likely result in further burden for software producers, who may find themselves in a position to produce attestations and/or assessments in multiple formats.

Finally, we strongly recommend the federal government identify opportunities and mechanisms to pilot procurement requirements to ensure that all parties are able to adequately articulate what information is useful in achieving the desired goal. Too much ambiguity and unknowns will only serve to frustrate the adoption of procurement requirements, result in uneven and/or ineffectual outcomes, and put the long-term success of the effort in jeopardy.