Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

Microsoft Response to Office of Management and Budget Implementation Questions – *Implementation of Software Supply Chain Security Guidance Under Executive Order 14028 Section 4(k)*
March 18, 2022
Submitted via email to OFCIO@omb.eop.gov

Microsoft appreciates the opportunity to provide feedback to the Office of Management and Budget (OMB) on its approach to partnering with the National Institute for Standards and Technology (NIST) to implement Executive Order (EO) 14028 Sections 4(e) and 4(k). We recognize the complexity of OMB's and NIST's taskings, the pace of timelines outlined by the EO, and the importance of an implementation approach that achieves the EO's full potential to enhance software supply chain security. Based on learnings from preparing to demonstrate conformance and partnering with agency customers, Microsoft is keen to contribute to an effective, consistent approach to cross-agency implementation.

We encourage OMB, NIST, and other U.S. government partners to manage an iterative process focused on realizing the EO's intended security and assurance outcomes. As our below responses to OMB's questions elaborate, we believe that near-term guidance can help agencies get started with a process for which there's readiness today while a phased approach can achieve significant additional benefits as agency and vendor understanding, tools, and partnerships mature. Throughout that process, we also propose that OMB and NIST continue to engage with industry, allowing opportunities for further exchange on known, anticipated, and to-be discovered challenges as well as input on regularly updated guidance.

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

An ideal process for Federal agencies to enhance supply chain security assurance would foster collaboration and partnership between and among agencies and vendors by increasing transparency and as-needed information exchange, facilitating shared security expectations, and building trust needed to make informed risk decisions. It would recognize and embrace the diverse software ecosystem (from single person open-source projects to multinational enterprises), the breadth of technologies, and the pace of innovation. Threat actors have learned that they are more powerful when they collaborate and continuously evolve, and in an ideal process, supply chain participants would similarly scale knowledge, efficiencies, and improvements.

We believe the foundation of this ideal process is the automated secure exchange of verifiable supply chain artifacts between all participants in a supply chain. This exchange would allow upstream suppliers to share artifacts with each other, facilitating downstream attestations and allowing policies to be applied to artifacts as they move through the supply chain. This is a vision that we outlined in a June 2021[1] submission to NIST and have continued to pursue both internally and with industry and open source partners.[2] It requires supply chain data stores that meet requirements for decentralized identity and trust as well as transparent and immutable logging of evidence and enforcement of controls; a data model and exchange format for providing all types of artifacts and evidence that products or components conform to requirements; and

[1] https://www.nist.gov/system/files/documents/noindex/2021/06/08/Microsoft%20-%20Executive%20Order%20-%20NIST%20workshop%20position%20paper%205-%20Software%20integrity%20chains%20Microsoft%20Corporation.pdf
[2] https://github.com/ietf-scitt

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

APIs to read, write, and query data stores. We discuss iterative steps that can be taken towards this vision in our subsequent answers.

In the immediate term, agencies can work toward an interim process consistent with NIST's Feb. 4 *Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e*, which recommended agencies require first-party attestation and request high-level artifacts of conformance. A centralized process for obtaining, validating, tracking, and retaining high-level artifacts and first-party attestation information for conformant software would enable efficiencies and consistency across agencies. Allowing for automation wherever feasible would further enhance efficiencies. Retaining artifacts or requested supply chain information, such as Software Bills of Materials, in a centralized manner (with appropriate data protection and access controls applied) would also help address agency infrastructure and security resourcing challenges and vendor security concerns. As processes and artifacts mature and automated secure exchange is enabled, retention can be facilitated by data stores with the characteristics described above.

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?

Systems, tools, and procedures with the following characteristics would maximize the benefits of greater transparency and support collaboration among all supply chain participants:

- They can be used throughout the supply chain – rather than just at the final step of end supplier to end consumer. Participants in supply chains are often both producers and consumers, and they may create new, transform existing, assemble, and re-package artifacts.
- They reduce redundancy across resource-intensive assessments and authorizations through centralized or coordinated processes. The Federal Risk and Authorization Management Program (FedRAMP) is intended to facilitate "do once, use many" security assessments and authorizations of cloud services. In the context of EO 14028, successful systems, tools, and procedures may also result in efforts to reduce redundant, resource-intensive evaluation and storage of supply chain artifacts.
- They leverage compliance artifacts from overlapping requirements and programs, streamlining the delta that requires net-new assessment. The Defense Information Systems Agency (DISA) recognizes equivalency between DISA impact level two and FedRAMP Moderate, enabling Authorizing Officials to use artifacts from a FedRAMP-approved package.
- They provide high signal-to-noise and retention of information that supports use cases (such as component transparency for vulnerability analysis). Loss of information between upstream suppliers, where mitigations and remediations are most effective, has significant downstream impact.
- They focus on artifacts that can be generated with automation, exchanged using open machine-readable standards, and transported between supply chain participants automatically and securely. Software development and IT environments operate at a continuously accelerating scale and pace, and effective compliance systems, tools, and procedures would be adapted to that reality.

A U.S. government-facilitated multistakeholder process could work toward defining additional characteristics, of both established and envisioned processes, for an effective approach to assessing

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

compliance at scale in digital supply chains. Such a process should engage producers of artifacts (both proprietary and open source), consumers of artifacts (both direct and indirect), and third-party assessors. There are existing, not mutually exclusive, efforts related to assessing compliance that could help inform this process, including:

- IETF Supply Chain Integrity, Transparency and Trust (SCITT)[3]
- OpenSSF SLSA Attestations[4]
- NIST Open Security Controls Assessment Language (OSCAL)[5]

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 most scenarios, attestations are effective in achieving the goal of awareness and implementation of requirements while minimizing burdens on suppliers and consumer procurement officers. The attestation process ensures suppliers are aware of requirements and consumers receive active acknowledgement from suppliers of conformance. SSDF's intentional flexibility of implementation also makes higher-level attestation processes appropriate (versus consumers having to interpret whether lower-level, implementation-specific artifacts adequately meet the SSDF practice's intent). When lower-level artifacts are required, they should support a specific use case, be producible and consumable at scale with automation, and leverage a standard format (broadly acceptable to both suppliers and consumers) that isn't implementation specific.

To further strengthen the effectiveness of artifact exchange, consumers should also be given guidance on appropriate and inappropriate uses of artifacts. In some cases, using an artifact for a use case it wasn't intended for or making invalid assumptions based on the artifact can lead to negative outcomes and foster mistrust between supplier and consumer rather than fostering increased transparency and communication.

For example, in the near term, the primary use case that Software Bill of Materials (SBOM) is intended to address is discovering software that may be susceptible to a discovered vulnerability. However, given an SBOM, a consumer can easily make incorrect or overly broad assumptions. The presence of a component with known vulnerabilities doesn't necessarily mean the software is vulnerable; the software might not be using the vulnerable part of the component, or it may have mitigations in place that prevent the vulnerability from being exploitable. Ideally the component would still be upgraded to a non-vulnerable version, but other constraints may impact whether or delay when it can happen.

Even more subtly, when comparing two SBOMs, reviewers might find one piece of software that depends on a component with a low severity vulnerability and another that doesn't use any components with known vulnerabilities. At first glance, it might appear that the software with no known vulnerabilities is more secure than the software with a low severity vulnerability, but this could be an incorrect assumption. It's possible that the software with a low severity vulnerability underwent extensive security review, all high severity vulnerabilities were resolved, and the low severity vulnerability was triaged as unexploitable, whereas the

[3] https://github.com/ietf-scitt
[4] https://github.com/slsa-framework/slsa/blob/main/controls/attestations.md
[5] https://pages.nist.gov/OSCAL/

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

software with no known vulnerabilities had no security review and contained several undiscovered high severity vulnerabilities.

With appropriate guidance and context, however, the SBOM is a useful artifact. If reviewers learn of a critical remotely exploitable vulnerability in an open source component and a query of the SBOMs in an asset management system show that only ten out of the thousand applications deployed contain that open source component, then the initial focus of an incident response process has been significantly narrowed, the suppliers of those ten applications can be engaged to determine if the vulnerability is exploitable, and monitoring or isolation of those applications can be increased until they can be patched.

For higher-risk scenarios, examination of additional lower-level artifacts may be warranted, requiring available expertise to analyze those artifacts, interpret them correctly, understand differences between implementations, and evaluate them against security goals, mission objectives, and the threat landscape. Third-party assessment is generally associated with higher costs but can provide both an independent perspective as well as that expertise. To avoid negating the benefits of higher-cost, increased scrutiny of software products, these higher-risk scenarios should also incorporate more stringent security controls for the deployment and operation of the software.

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

SSDF is designed to give adopters a flexible framework that can be adapted for different business, technical, and threat environments.[6] Third-party assessment of "adequate SSDF practices" without more rigorous definition of adequate would risk inconsistent outcomes. To maintain SSDF's flexibility, which is one of its key advantages, a third-party assessment would need to assess the adequateness of the supplier's chosen implementations and the supplier's execution of those implementations.

Higher-risk scenarios may justify a more complex and higher-cost third-party assessment. For these scenarios, to reduce the risk of overlap or inconsistency, existing third-party assessment programs for software suppliers should be evaluated to determine if they do or could adequately cover the SSDF practices while still allowing the flexibility of implementation they afford. Programs such as FedRAMP, which already incorporates risk levels and conformance assessment, could be leveraged and extended, especially if coupled with broader ongoing efforts to continue modernizing and otherwise improving the program.

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

As we increase the number of artifacts in digital supply chains, it will become increasingly necessary, or at least desirable, to correlate those to make decisions and generate insights. Software and services may be identified with different identifiers in different contexts, such as a SKU in contractual documents and a package identifier in vulnerability databases. Allowing suppliers to provide multiple identifiers with an attestation facilitates correlation of that attestation with other supply chain artifacts, such as SBOM. This approach is consistent with NTIA's guidance on Minimum Elements for a Software Bill of Materials, which

[6] https://csrc.nist.gov/Projects/ssdf#ssdf-use

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft recommends that an SBOM contains "Other Unique Identifiers" to "serve as a look-up key for relevant databases."

Often there is not a one-to-one relationship between the software produced and the software procured. For example, multiple software products may be combined and purchased as a single SKU, and a single software product may be available in multiple different bundle SKUs. Cloud services are often not a single service but a collection of services; these services may be billed independently (for example, storage and compute) and may be built and deployed independently. For these reasons, we encourage flexibility in allowing a single attestation to cover multiple products or a single product to be covered by multiple attestations.

What information do vendors need in advance in order to comply with implementation guidance?

Recent SBOM and Section 4e guidance from NTIA and NIST acknowledges that many operational questions remain to be answered. The answers to those questions will influence the information needed by vendors. Microsoft's prior work on the Security Development Lifecycle (SDL), SSDF, and SBOM allowed us to make progress preparing to demonstrate 4e conformance despite these open questions, but assumptions we made throughout this process may prove to be incorrect as answers are finalized.

Potential variability across agency implementation approaches will also impact vendor readiness. We acknowledge the importance of agencies having discretion to apply NIST's guidance to best meet their mission objectives, technical environment, and threat landscape. However, discretion creates unknowns while agencies translate guidance into their specific requirements. This is further complicated by some requirements being infeasible to apply to products that have already been built or needing to be adopted by upstream suppliers. These complications may result in requirements being unmet until the next version of the product is available.

We encourage NIST and OMB to facilitate implementation pilots between agencies and early vendor adopters of SSDF and SBOM to identify gaps in guidance and implementation challenges and focus on EO objectives. Pilots would generate insights that both agencies and vendors can share to streamline adoption by the broader ecosystem. Microsoft is committed to increasing security and transparency in supply chains, and we would welcome any opportunity to participate in an implementation pilot.

Microsoft remains committed to our ongoing partnership with OMB and NIST, and we welcome future opportunities to collaborate.

Respectfully submitted,

William Bartholomew
Principal Security Strategist, Global Cybersecurity Policy
Digital Diplomacy
Microsoft Corporation