Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Robert J. Costello
Chief Information Officer
Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Submitted electronically at: www.reginfo.gov/public/do/PRAMain

December 15, 2023

RE: Request for Comment on Secure Software Development Attestation Common Form (Docket No. CISA-2023-0001)

Microsoft is grateful for the opportunity to comment on the second public draft of the Secure Software Development Attestation Common Form (Attestation Form) and we appreciate that this draft incorporates feedback we provided on the first draft.

We have enclosed our feedback on the second public draft, which includes some suggestions for further improvement, such as reducing burden by reinstating the ability of the CEO to delegate signing authority, supporting risk-based response to vulnerabilities, allowing SBOMs to fulfill the provenance requirement, and addressing some potential gaps and ambiguities in the form.

We hope that our feedback will be helpful for the finalization of the form and the implementation of the Executive Order 14028 on Improving the Nation's Cybersecurity. We look forward to continuing our collaboration with CISA to enhance the security and transparency of software products and services and supporting the successful adoption of the form.

Regards,

William Bartholomew
Principal Security Strategist
Customer Security & Trust

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Microsoft's Feedback on Second Public Draft

1. **Allow the CEO or COO to delegate signing authority** to the employees closest to developing the products, verifying their compliance, and participating in the Federal government sales process.
    a. Because the Attestation Form will need to be signed whenever new versions of products are released, and in some cases (such as when additional artifacts are requested) will be agency-specific, it is not practical to require CEO or COO signature for each instance.
    b. To allow the business to respond quickly to customer, partner, and market demands, Microsoft delegates signing authority – through defined company policy – to authorized full time employees based on the type of artifact being signed and the business group it relates to.
    c. Delegation does not imply lower importance, instead, it puts signing in the hands of people with direct insight into, and responsibility for, the security outcomes. This leads to the compliance artifacts better reflecting reality, rather than being a check-the-box compliance activity.
    d. Companies with broad product and service portfolios will often have dedicated organizational units responsible for the governance, risk, and compliance requirements, and oversight of their execution, for specific product lines. Designated employees, often but not always Corporate Vice Presidents, in those organizational units are authorized to sign compliance artifacts related to their products on behalf of the company.
2. **Allow risk-based policies when responding to vulnerabilities**, consistent with existing Federal guidance, international standards, and industry practices.
    a. The use of "address[es]" in "has a policy or process to address discovered security vulnerabilities" and "accepts, reviews, and addresses disclosed software vulnerabilities" implies that all vulnerabilities must be mitigated.
    b. The severity, probability, and impact of a vulnerability, and the cost and risk of remediating it, vary greatly and often are not correlated. For example, a potential denial-of-service attack (DoS) for a single-user application or that requires physical access to exploit may be low

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

priority in most scenarios, and remediating it would divert limited resources from higher priority activities.

c. Manufacturers use assessment and triage policies and processes that take these factors into account to decide when, and if, to patch a vulnerability and when to release that patch. Likewise, consumers take similar factors into account to decide when, and if, to apply patches.
d. This approach is reflected in Federal guidance, international standards, and industry practices, such as:
    i. NIST *SP 800-218 (SSDF 1.1)* RV.2.2 "Analyze each vulnerability to gather sufficient information about risk to plan its remediation or other risk response."
    ii. NIST *SP 800-53 Revision 5 (Security and Privacy Controls for Information Systems and Organizations)* RA-5 "Organizations have many options for responding to risk including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk."
    iii. SAFEcode *Fundamental Practices for Secure Software Development, Third Edition* "The findings from these artifacts [findings related to the product's security (or lack thereof)] must be tracked and action taken to remediate, mitigate or accept the respective risk."

3. **State that SBOMs meeting the *NTIA's Minimum Elements for a Software Bill of Materials* fulfill the provenance requirement.**
    a. The NTIA's *Minimum Elements for a Software Bill of Materials* states that "At a minimum, all top-level dependencies must be listed with enough detail to seek out the transitive dependencies recursively."
    b. The Attestation Form states that "Establishing and maintaining processes for producing and maintaining a current SBOM may be utilized by the software producer as a means of documenting compliance with certain minimum requirements," but it does not specify which requirements.
    c. The Attestation Form also requires that "The software producer maintains provenance data for internal and third-party code incorporated into the software," but it does not define provenance data.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

   d. Explicitly stating that SBOMs meeting the NTIA's *Minimum Elements for a Software Bill of Materials* fulfill the third-party provenance requirement will reduce ambiguity and encourage production of SBOMs.

4. **Allow attesting for a version range** (such as, a major version or a major and minor version), rather than having to attest to a specific version. We believe this is the intent, but that should be clarified in the instructions.
   a. For example, Microsoft Windows has new updates at least monthly and each of these should not require a new attestation.
   b. Allowing organizations to choose the scope that they're attesting to allows them to balance the burden and risk based on their organizational and engineering processes.
5. **Remove the "publicly available" restriction** from "software that is freely obtained".
   a. This restriction limits organizations' ability to provide Federal agencies with private beta or previews for them to evaluate and provide feedback on. This software may be incomplete, provided as-is, and intended to be tested or evaluated in an isolated environment, and would not be considered in scope of our compliance programs.
   b. This restriction may hamper the ability for organizations to provide Federal agencies with one-off scripts and tools during incident response engagements.
   c. Restricting "software that is freely obtained" is inconsistent with the intent to use of Federal purchasing power to influence vendor behavior.
6. **Remove the "directly" restriction** from "software that is freely obtained". The use of "directly" may inadvertently require freeware and open source delivered via common, even typical, means to require submission of an Attestation Form.
   a. Freeware and open source are often distributed through third-parties, such as collaboration platforms, package repositories, software mirrors, etc.
   b. Open source is often bundled and delivered together, such as operating system distributions and container images.
   c. If the intent is to require submission of an Attestation Form for freeware or open source delivered as part of a commercial transaction, explicitly excluding that scenario from the exception would be preferrable.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

7. **Define minimum requirements for agencies' protection of submitted information.**
    a. The Attestation Form relies on "agency-applicable SORN".
    b. This reliance makes the Attestation Form agency-specific, providing submitters with differing protections for the same information depending on the agency it is submitted to.
    c. This reliance doesn't establish a consistent baseline of protection for the submitted information, especially for additional artifacts that may be requested by the agency. This also creates uncertainty when a manufacturer is proactively publishing an Attestation Form, or when it is being provided via a third party (such as a reseller).
    d. The agency-specific nature of this reliance may also impede Government-wide sharing of the submitted Attestation Forms, as required by OMB M-22-18: "In consultation with GSA and OMB, CISA will establish a program plan for a Government-wide repository for software attestations and artifacts with appropriate mechanisms for information protection and sharing among Federal agencies."
8. **Define "relevant NIST guidance"** in "assessor used relevant NIST guidance" to increase consistency for manufacturers, 3PAOs, and agencies.
    a. Leaving this undefined may result in 3PAOs choosing differing NIST guidance or agencies accepting or rejecting assessments from 3PAOs based on which NIST guidance they selected.
9. **Acknowledge potential limitations to notifying all impacted agencies**.
    a. When a manufacturer provides the software and Attestation Form directly to agencies it is reasonable to notify them of material changes.
    b. However, manufacturers often provide software to agencies indirectly, through resellers, contractors, and other manufacturers. In these scenarios, and likely others, a manufacturer may not have a complete list of the agencies that need to be notified.
    c. Because of these limitations, manufacturer's notification obligations should be best-effort and the Government should use the Government-wide repository required by OMB M-22-18 to improve dissemination of notifications to applicable agencies.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

10. **Change "with all elements in this form" to "with the requirements outlined in Section III"** to reduce ambiguity.
11. **Reference *OMB Memorandum M-23-16* in the Authority section**, as M-23-16 provides important clarifications to *OMB Memorandum M-22-18*.
    a. The remainder of the form references both Memorandum in tandem, and not including *OMB Memorandum M-23-16* in the Authority section may imply that it is less authoritative.