To:
Cybersecurity and Infrastructure Security Agency (CISA),
White House, Office of Management of Budget
Atten: Mitchel.D.Herckis@omb.eop.gov, Shon Lyublanovits, via *central@cisa.dhs.gov*

OpenPolicy comments on

Secure Software Development Attestation Form, ID CISA-2023-0001-0112

Overview

OpenPolicy appreciates the opportunity to provide feedback on CISA's Secure Software Development Attestation Form. OpenPolicy further appreciates the Administration and implementing agencies' continued leadership in promoting the nation's security by supporting the Biden Administration Cyber Executive Order. We would like to express our intent to participate and engage in further proceedings and support the Administration's development of additional software and supply chain security frameworks, standards, and requirements.

OpenPolicy is committed to supporting the implementation of the Executive Order and actively engages with CISA and other implementing agencies. Our documented commitment on the White House webpage reflects our and our members, robust dedication to advancing these initiatives.[1]

OpenPolicy is the world's first policy intelligence and engagement technology platform, aiming to democratize and simplify access to policy engagement for entities of all sizes by leveraging scale and cutting-edge technology, including AI. We strive to make policymaking accessible, affordable, and inclusive for all.

We believe that the open and collaborative nature of the policymaking dialogue is essential to further the implementation of the Executive Order, which can be significantly contributed by the participation of innovative companies and startup developers of the relevant software, specifically innovative companies that develop cutting-edge solutions to identify supply chain and software cyber risk and address them, as the landscape evolves.

Indeed, many, if not most, of the technologies used to support the requirements of the Cyber EO and relevant NIST guidelines (such as NIST SSDF), evaluate the measurements, testing, and

[1]See WhiteHouse page, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/31/what-they-are-saying-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/).

audibility of security posture, and secure software and organizations more broadly, are currently developed by such innovative companies and startups – these are the communities OpenPolicy represents and engages with. Like CISA, we believe that broader participation of such entities is critical for the open nature of stakeholder engagement needed to level the playing field in software and supply chain secure development.

OpenPolicy collaborates and represents leading innovative companies that develop cutting-edge technologies, specifically in the area of security. These companies, of all sizes, include both stakeholders that lead on asset management security and vulnerability management, such as Armis, SBOM and supply chain security companies, such as Cybeats and Finite State, solutions for automated security compliance, such as Kiteworks, and leading startup solutions providers used today by stakeholders globally to measure AI security and safety (e.g. Cranium AI) or to secure and protect from AI attacks (HiddenLayer).

OpenPolicy applauds CISA for its leadership in creating and developing the self-attestation form but would like to offer several key comments:

The requirements of the self-attestation form need to align with upcoming revisions to NIST guidelines and controls and recent CISA-outlined best practices.

First, while the Self-Attestation Form was created to support the implementation of EO 14028, several key related documents that indicate and outline the controls referenced under the form will soon be updated to comport with the threat landscape. For example, the CSF 2.0 revision by NIST may introduce new controls needed to address the current threat landscape and promote better governance for IoT, OT, third-party, and software development. Guidelines have been released on these issues, including by CISA (e.g., "secure by design" and software security best practices). Notably, revisions to SSDF are expected given the evolving AI threat, as outlined under the AI Executive Order. Furthermore, OMB released priorities related to unmanaged assets and IoT for federal agencies and the implementation of the IoT Cybersecurity Improvement Act just this month. While ongoing implementation already calls for self-attestation of contractors' adherence to SSDF, documents will need to be updated to regard unmanaged assets such as OT and IoT amid revisions to the CSF, SSDF, or the recent memos released.

It is, therefore, key that CISA and OMB outline a process to revise required controls as appropriate and further consider a more automated procedure to ensure adherence to the latest controls, to further the security of Federal Systems, and not cultivate adherence to past controls and methods, that may expose the federal system to threats.

While we are pleased with the emphasis on enhanced measurability of outcomes, we believe automation is the key to allowing the attestation method to keep up to date with controls released and support risk management at scale. Automation can also support the complex goal of aligning the implementation of the Cyber Executive Order with the revisions of the ongoing FEDRAMP, FISMA, and NIST documents and the security elements of the AI EO. A further focus on leveraging automation and measurable compliance (e.g., leveraging schemes like OSCAL) can advance risk governance in this respect and increase the ability of CISA and OMB to scale agency measurements, as agencies and auditors can collaborate with solutions providers to automate control measurements.

The CISA proposed form, building on SSDF, serves as a valuable asset for advancing contractors' responsible software development and their ability to manage risks associated with software development. However, with the expansion of the third-party threat landscape, AI threats, and novel software developments AI practices, we expect the supply chain and software secure development best practices will evolve, as demonstrated by the recent ESF Supply Chain Security best practices document. It is vital that the controls are mapped into these critical guidelines and are updated to align with them. Methods of auditing and reviewing mechanisms with the form need to be supported by technology that ensures compliance and secure implementation. As the AI EO guidelines on security are released, we encourage CISA and OMB to implement the relevant revisions to SSDF and related controls into the form.

Finally, we are excited to collaborate with CISA to increase engagement with innovative companies. We note that technology tools for supporting at-scale attestation and measurements of controls are required under the form. Below, we included additional detailed feedback on the self-attestation form.

Minimum requirements within the Secure Software Attestation Form

Controls related to data security and data provenance

While encrypting sensitive data like credentials is a crucial first step, it is essential to recognize that more than encryption is needed in today's complex threat landscape, such as protecting data of use and ensuring robust quantum resistance (in a timeline aligned to federal agency goals), and a holistic data security posture risk mitigation framework. To truly enhance data privacy and security, there is a need to move beyond traditional encryption and embrace a layered approach that takes under consideration other ***high-risk data categories***, integrating *privacy* ***enhancement technologies*** (PETs) and ***utilizing robust data protection technique*****s** like confidential computing. A broader data security risk governance posture, and mapping of available

encryption and PET controls, may be needed to identify which data is exposed and its risk, thereby aligning the Cyber EO implementation with the goals of the AI Executive Order, PET strategy, and the broader goal of transitioning federal agencies to post-quantum resistant environments. Notably, the AI EO already outlines a vision for a more robust data security posture for federal agencies. A more comprehensive data security controls strategy that combines encryption with cutting-edge privacy technologies is vital for robust defense against cyber threats and compliance with legal standards and may be considered for the form and future revisions of SSDF. Such revision is already underway under the AI EO, and its controls should be incorporated accordingly under the Cyber EO form and its revisions.

SBOMs and third-party components

The request for software producers to maintain provenance for internal code and third-party components is an essential aspect of SSDF, which underscores the need for integrating a Software Bill of Materials (SBOM) mechanism as simply tracking component origin falls short of truly leveraging all potential benefits of SBOMs. SBOM is a comprehensive inventory of all components that comprise a piece of software, including details about each component, such as its version, origin, and license information.

Accordingly, integrating the SBOM mechanism would be a significant step towards ***transparency*** and ***accountability*** by using SBOM' 's comprehensive listing of all software components, including versions, licenses, and vulnerabilities, which will further foster accountability in risk management throughout the software supply chain, enabling stakeholders to identify potential risks and dependencies. By readily providing detailed component information, organizations can further scale the process of demonstrating ***compliance with software requirements*** in the form itself.

In the context of supply chain security, an SBOM provides critical insights into the software's risk profile, thereby ***facilitating risk management***. Organizations can assess and proactively mitigate potential risks by understanding the components used. For software that relies on open-source components or third-party libraries, an SBOM is invaluable in managing dependencies effectively. It helps track updates, licenses, and compatibility issues, aligning with the form's primary goals. We understand that CISA and OMB have yet to ***require*** SBOM production explicitly under the form (as opposed to requested) given some expressed concerns on the state of SBOM standardization; The form can be improved, if as part of the form, SBOMs will be described a key best practice for contractors while ***outlining a timeline*** for more robust SBOM requirements. Since 2021, the industry has made significant progress on SBOM production tooling and its preparation towards SBOM at scale production. Additional standards

have been developed and released, and open-source tooling has been made readily available for companies to use and produce SBOMs, along side state-of-the-art solutions. More attention should be given as to when federal agencies, and contractors, should be expected and required to showcase more robust SBOM capabilities, consistent with best practices.

Vulnerability Management Automation and Vulnerability Disclosure Program (VDP) requirements

Additionally, the draft guidance calls for software secure development and build environments, including emphasizing the producer of automated tools or processes to detect security vulnerabilities need for continuously checking and disclosing software vulnerabilities, and promoting vulnerability disclosure programs practices, which is a substantial enhancement compared to the existing framework. These controls align with SSDF but also other key White House memos (such as the ZTA memo), and the requirements for agencies to deploy programs for vulnerability disclosure programs under the IoT cybersecurity improvement act (prioritized in FISMA 2024 priorities and relevant memos), and CISA BOD 22-01.

On this part, we would like to offer the following comments:

Constituent with prior comments, it is key agencies and controls, leverage ongoing automation monitoring and reviewing mechanisms to ensure compliance. Such automation should extend to internal processes for managing VDPs, ensuring vulnerability mitigation is consistent with government (and other) SLA timelines as suggested in the form, and is based on constant risk prioritization (compare to e.g. the KEVV). Such tools can further apply necessary patches and updates to mitigate vulnerabilities or recommend alternative mitigation to reduce risk.

Furthermore, integrating these automated controls and monitoring mechanisms can further ensure a more proactive and responsive approach to software security and internal management of vulnerabilities, leading to a substantial enhancement of controls, and increasing governance and compliance.

Finally, the attestation form should clarify the organization is following best practices for VDP and coordinated vulnerability disclosure such as ISO/IEC 29147 and 30111. This reference is consistent with the IoT Cybersecurity Improvement Act and BOD 20-01. An additional reference should be made to ensure federal contractors add language in the VDP to mitigate potential legal risks, for external security finders and researchers, such as the language provided by disclose.io, otherwise referred to “safe harbor”). This addition aligns with prior Whtie House OMB memos (see e.g. Zero Trust White House memo), federal law and CISA BOD 20-01, as well as CISA “Secure by Design” guidelines.

As the form evolves, we look forward to discussing these proposals with CISA and are available for any questions.

Respectively,

Dr. Amit Elazari, CEO & Co-Founder, OpenPolicy