FAQ for Secure Software Attestations and Software Bill of Materials Requests

The purpose of this Frequently Asked Questions (FAQ) document is to address common questions regarding TVA's request for Secure Software Development Framework (SSDF) Attestation and Software Bill of Materials (SBOM) documentation.

Q: I received a request from TVA via cscrm.fortress@tva.gov to access a vendor survey and attest to secure software practices. Is this a legitimate request?

A: Yes, this is an official request from TVA in response to EO 14028 and the subsequent OMB Memos.

Q: Who is Fortress Information Security?

A: TVA has partnered with Fortress Information Security to help collect attestations and SBOMs; Fortress is authorized to collect signed attestation forms on behalf of TVA.

Q: Why is TVA requesting Secure Software Attestations?

A: In May 2021, the Biden Administration issued an Executive Order on Improving the Nation's Critical Infrastructure (EO 14028). The EO's goals included improving cybersecurity standards and software supply chain security for US federal agencies, expanding public/private partnerships, and improving transparency and information sharing. We support the U.S. government's directives to improve critical infrastructure and to address complex multidimensional cybersecurity challenges affecting the world. Resulting from the EO, US federal agencies are obligated to align with the Secure Software Development Framework (NIST SP 800-218) and to direct software producers to either self-attest to product conformance or have an independent Third-Party Assessment Organization (3PAO) attest on the software producer's behalf. Software vendors that cannot attest to meeting the requirements may instead provide TVA with a Plan of Action and Milestones (POA&M).

Q: What is a secure software attestation?

A: Secure software development attestations or "software attestations" are signed forms whereby a software producer or an independent third-party assessor attests that the software producer consistently uses the secure software development practices outlined in the U.S. government's Secure Software Development Attestation Framework.

Q: If my software/product has not undergone a major version upgrade since Sept 2022, do I still need to provide an attestation?

A: No, you don't need to provide an attestation for software that hasn't had a major version upgrade since September 14, 2022. Attestation is required for: (1) software developed after September 14, 2022; (2) software developed before September 14, 2022, that has since undergone major version upgrade; and (3) software in which the producer delivers continuous changes to the software code, such as software-as-a-service (SaaS) products and other products using continuous delivery/deployment models. However, if your organization is able to attest to secure software development practices for software that predates the September 14, 2022 date, TVA will gladly accept your attestation. Attesting early will lessen the burden on both TVA and your organization during future solicitations and contracting opportunities.

Q: How do I complete this request in Fortress?

A: Follow the instructions in the original email request to access the platform. The SSDF Attestation request will walk you through a questionnaire to document your company's Attestation. For SBOM requests, you can also find additional information here.

Q: Do I need to provide an SBOM? Is it required?

A: For on-premises and desktop software, TVA is requiring a SBOM for all new technology procurements. For SaaS and other cloud-based or hybrid installations, TVA is prioritizing SBOMs based on risk. TVA may request working with your product team and our product team(s) to establish a baseline for the components, modules, and connections that should be included in a SBOM for SaaS and other cloud-based installations.

Q: TVA does not have a current support/maintenance agreement for our software, do we still need to provide an attestation?

A: Yes. The attestation requirement is not predicated on an active support/maintenance agreement being in place. If the software is in scope of the compliance date (Sept 14, 2022), then the requirement must be met.

Q: Is there an NDA available to support this sharing of information?

A: Yes. TVA can provide a multi-party NDA upon request.

Q: Who is allowed to attest to secure software practices in my company?

A: Software attestation forms must be signed by the Chief Executive Officer (CEO) or the Chief Operating Officer (COO) of the software producer or their designee who has the authority to attest. Alternatively, your organization may engage an accredited Third-Party Assessment Organization (3PAO) to assess your software security and issue a formal report with their findings. Such assessments "must use relevant NIST Guidance that includes all elements outlined" in CISA's attestation form and be attached to the CISA self-attestation form.

Q: How will the software attestation be used?

A: The government will use software attestations to determine if it should purchase or continue using certain software. Additionally, OMB will collect metrics from federal agencies in order to monitor and audit compliance with the directive.

Q: How will TVA protect my company's software attestation and/or SBOM?

A: TVA will handle the information within the attestation and/or processes with appropriate security measures. Please note that once software attestations are uploaded to CISA's repository, all federal agencies will have access to the documentation and will be considered publicly available within CISA's searchable repository.

Q: Who can I contact if my company has further questions?

A: Please contact your TVA Contracting Officer, TVA Technology & Innovation (T&I) representative, or primary TVA point of contact for initial questions. If you do not have an established TVA point of contact, please contact CSCRM@tva.gov.