



TECHNOLOGY & INNOVATION

Cybersecurity

Valued partners,

As cyber threats and incidents increase exponentially year over year, TVA is prioritizing the defense of our supply chain. TVA is implementing best practices to secure our supply chain and to comply with federal mandates. In the coming weeks, we will be working with our vendors to collect attestations of secure development practices and software bills of materials (SBOM) in adherence with Office of Management and Budget (OMB) Memoranda [M-22-18](#) and [M-23-16](#). Formal requests for these documents will be sent to you by our partner in this area, Fortress Information Security ([Fortress](#)).

We have partnered with Fortress to use the Fortress Cyber Supply Chain Risk Management (C-SCRM) and SBOM platforms where Software Producers can digitally upload the self-attestation using Cybersecurity & Infrastructure Security Agency's (CISA) forthcoming "[Common Form](#)" format and machine-readable SBOMs. This will be a requirement moving forward to supply TVA with software, services like SaaS, PaaS, or IaaS, any devices containing firmware, etc. We believe that this up-front TVA-vendor collaboration will facilitate future procurement activities, creating efficiencies in future process.

Key things to know about this request:

- Fortress will be reaching out to formally request self-attestation of secure software development practices as soon as it is published by CISA. The form allows software vendors to attest that their development processes align to the NIST secure development framework [NIST SP 800-218](#).
- You will receive an email or letter directly from Fortress, formally kicking off this collection. The attestation must be signed by either the company CEO, CFO, or organizational equivalent.
- **NOTE:** If you are not the correct contact in your organization for this request, please reply to the email address below with the correct contact information for future communications and outreach.
- At that time, we will also be requesting that you provide TVA with an SBOM for your software products. Additional details about what's included in an SBOM can be found [here](#).
- For those that cannot attest, we will engage in further discussions and encourage you to reach out to us.
- Monitor the [TVA Supplier Connection's website](#) for further updates and more detailed information.

Once TVA launches this outreach upon CISA's release of the Common Form, we will have a small window to collect responses. **For software critical to TVA's business, we will have 90 days to collect an attestation. For all other software, we will have 180 days.** We appreciate your timely response.

For any questions or concerns you have for us, please contact TVA Cybersecurity Supply Chain Risk Management CSCRM@tva.gov.

TVA Cybersecurity