Fortress

ABSOLUTELY CRITICAL

Software Bill of Materials (SBOM)

Vendor Welcome Kit

Fortress Information Security, LLC
Phone: 855.FORTRESS
250 S. Orange Ave., Suite 500, Orlando, FL 32801

Fortress SBOM Vendor Welcome Kit

About Fortress

Fortress Information Security ("Fortress") provides cyber risk management solutions for mission critical supply chains including services for third-party risk management, product security and risk management, file integrity assurance, continuous monitoring, and remediation to support an overall zero trust security model. Fortress specializes in critical infrastructure sectors and supports major utilities, oil and gas, government defense entities, healthcare and more.

Fortress is working on behalf of the utility industry to create and maintain the North American Energy Software Assurance Database (NAESAD). The NAESAD is a repository of software transparency artifacts for applications used within the energy sector. Software Bill of Materials (SBOMs) are key artifacts that demonstrate secure software development practices.

Fortress also operates the Asset to Vendor Network ("A2V Network"), which is a collaborative, information-sharing network of utilities and utility vendors, which is used by NAESAD to provide secure permissioned sharing.

How does Fortress protect your data?

Fortress Information Security holds SOC 2 Type 2 and NIST SP 800-171 certifications. The Fortress Platform secures data in transit by requiring TLS 1.2+ security protocols. Data at rest is stored on encrypted volumes, and files uploaded to the platform are encrypted a second time at the application-level utilizing AES-256 encryption algorithms. Fortress Platform data access is protected via multi-factor authentication.

What information are we requesting?

We are requesting the following information on your products formatted in one of the two major SBOM formats - CycloneDX or SPDX. We can also provide advice and answer questions on SBOM creation and formats as needed.

Vulnerability Exploitability eXchange (VEX) documents, if available, should also be provided. VEXs are machine-readable documents which explain if a product is affected by a discovered

vulnerability. VEXs may be in CycloneDX v1.4 or Common Security Advisory Framework (CSAF) v2.0 formats.

The Cybersecurity & Infrastructure Security Agency (CISA) has published, now in draft form, the Secure Software Development Attestation Common Form which will also be a requested artifact once published as final.

The tables below list the minimum data requirements to be included in the SBOM and VEX documents.

Product Information			
Product Name	Product Supplier Name	Product Version	Product Identifier
Product Type	Product Description	Product License	Cryptographic Hash of Product File
Download URL of Product			

Component Information			
Component Name	Component Supplier	Component Version	Component Identifier
Component Type	Component Description	Component Licenses	Cryptographic Hash of the Component
Download URL of Component	Version Control System URL	Component Relationships	

Vulnerability Exploitability eXchange (VEX) Information			
Product Name	Product Supplier Name	Product Version	Product Identifier
Vulnerability Identifier	Vulnerability Description	Exploitability Status	Remediation Information
Document Author	Document Timestamp		

Why should you participate?

Open-source libraries and third-party software component dependencies represent a major vector for the propagation of vulnerabilities. Increasingly, asset owners are concerned with what pieces of software are used in products deployed in their systems. Knowledge of what software components are used in a device can aid in remediation strategies in the inevitable event new vulnerabilities are discovered for a particular third-party software library. In addition to cybersecurity concerns, certain customers in the Federal space have restrictions on ‘countries of origin’ for hardware and software they are allowed to use. This restriction applies to software as well and Fortress will use SBOM information provided to generate provenance information when possible.

This is also an opportunity to share VEX (Vulnerability Exploitability eXchange) information. Often the software components found inside software have vulnerabilities associated with them. Without context customers are left with a list of vulnerabilities, often in the hundreds. You are in the best position to provide information on which vulnerabilities, if any, have been tested and found to be exploitable or not.

Fortress

Our Process

Request Kick-Off	NAESAD Access	SBOM Upload	SBOM Analysis	Analysis Report	Share Requests
Welcome email sent to vendor with invitation to schedule kick-off call. Discuss SBOM Creation process and requirements. Discuss SBOM sharing and approvals. Address questions or concerns.	Vendor receives invitation to Vendor Portal. Vendor completes short SBOM questionnaire. Vendor may invite additional collaborators via the Vendor Portal.	Vendor uploads SBOM and/or VEX documents via the Vendor Portal. Vendor continues to provide updated SBOMs as Vendor products receives software updates.	Vendor submits SBOM/VEX documents to Fortress. Fortress analyzes SBOM data for areas of risk, such as vulnerable components.	Fortress provides a copy of the analysis report to Vendor. Fortress provides copy of analysis to requesting Client.	Fortress maintains analysis report for potential client shares. When Fortress receives a share request, Vendor will be informed and may approve or deny sharing.

Process Milestones

Request Kick-Off

Duration:	Email and Call (30 Minutes)
Participants:	<u>Vendor Participants:</u> - Product Security Manager - Information Security Manager - Information Security Compliance Manager <u>Fortress Participants:</u> - Fortress Vendor Risk Analyst - Fortress Risk Assessor
Details:	The purpose of this kick-off call is to present the Fortress SBOM process, discuss SBOM document creation, introduce the NAESAD where SBOM and VEX documents can be uploaded, discuss SBOM sharing and approval process, and address any questions or concerns. We also ask that the contacts be validated to ensure we provide access to the appropriate individuals at your organization to upload the documentation. We will also introduce the NAESAD and request your consent for participation. See the 'NAESAD' section below.

NAESAD Access

Duration:	Immediately following kick-off call
Participants:	Vendor Participants: - Product Security Manager - Information Security Manager - Information Security Compliance Manager Fortress Participants: - Fortress Vendor Risk Analyst - Fortress Risk Assessor
Details:	The Fortress Security Analyst will initiate the SBOM process and send an invitation to the confirmed vendor contacts. The invitation email will come from 'noreply@fortressinfosec.com' – please check your spam folder. You will click on the link in the email to access NAESAD. For first-time access, you will need to create a password.
Notes:	Invitation emails are unique to each user. If additional contributors are required, they can be added through the 'Invite Contributors' button in the Vendor Portal.

SBOM Upload

Duration:	Ten (10) business days are provided to upload the requested SBOM and VEX documents
Participants:	Vendor Participants: - Information Security Manager - Information Security Compliance Manager
Details:	A SBOM is a machine-readable list of the components in a piece of software. Fortress uses the data from SBOMs to inform on areas of risk, such as potential vulnerabilities, outdated components, presence of code contributions from adversarial countries, license information, as well as checks on malware, and component integrity. A Vulnerability Exploitability eXchange (VEX) is a machine-readable companion document to an SBOM which explains if a product is affected by a discovered vulnerability. VEXs explain if a potential vulnerability is exploitable in a product and why. The requested fields for these documents are based on standards developed by from the National Telecommunications and Information Administration (NTIA), National Institute of Standards and Technology (NIST), and Cybersecurity and Infrastructure Security Agency (CISA). Complete depth may not always be feasible, especially as SBOM practices are still new to many companies. When an SBOM cannot convey the full set of components, it should explicitly acknowledge the “known unknowns,” so consumers can easily determine the difference between a component with no further dependencies and a component with unknown or partial dependencies. A completed SBOM and supporting documentation such as a VEX should be submitted via your Trust Center dashboard. To provide relevant analysis of a product’s components we ask that certain data fields be included in an SBOM or VEX, respectively. The table below includes standard data fields to include, but is not limited to:

SBOM Data Field	Description
Metadata	
Timestamp of the SBOM	The exact time that the SBOM was generated. A timestamp is an unambiguous way to remove confusion about which version of an SBOM is being referenced.
Author or Tool Which Made the SBOM	The people or tools which created the SBOM document
Product Data	
Product Name	Name of the product that is the subject of the SBOM.
Product Supplier Name	Supplier of the product that is the subject of the SBOM.
Product Version	Version string for the product that is the subject of the SBOM.
Product Identifier	A unique product identifier, specifically a specifically a Common Platform Enumeration (CPE), a Package URL (PURL), or both.
Product Type	For example: device, application, library, framework, service, container image, file, firmware, or operating system.
Product Description	Short description of the product and/or features.
Product Licenses	License information on the product.
Cryptographic Hash of the Product File	For example, SHA-256, SHA-1, or MD5 hash of the software package.
Download Location of the Product File (Typically a URL)	A URL where the product can be downloaded.
Component Data (Per Component)	
Component Name	Common name by which the component is known.
Component Supplier Name	Supplier name for the component. For an open-source component this may be the name of the project.
Component Version	Component version string.
Component Identifier, specifically a Common Platform Enumeration (CPE) or a Package URL (PURL), or Both	Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices. A Package URL (PURL) can be used to uniformly identify and locate a software package across programming languages, package managers, packaging conventions, tools, APIs, and databases.
Component Type	For example: device, application, library, framework, service, container image, file, firmware, or operating system.
Component Description	Short description of the component and/or features.
Component Licenses	The license(s) which apply to the component.
Download Location of the Component	A URL of where the component was downloaded.
Cryptographic Hash of the Component	For example, SHA-256, SHA-1, or MD5 hash of the software package.
Version Control System Location	Typically, a GitHub or similar URL for open-source components to track and manage changes to files over time.
Component Relationship Information	The relationships between components, as well as between a component and the product itself. For example, a relationship of “depends on” can describe how components are dependent on other components in the product.

VEX Data Field	Description
Metadata	
Timestamp of the VEX	The exact time that the VEX was generated. A timestamp is an unambiguous way to remove confusion about which version of an SBOM is being referenced.
Author or Tool Which Made the VEX	The people or tools which created the VEX document.
Product Data	
Product Name	Name of the product that is the subject of the VEX.
Product Supplier Name	Supplier of the product that is the subject of the VEX.
Product Version	Version string for the product that is the subject of the VEX.
Product Identifier	A unique product identifier, specifically a specifically a Common Platform Enumeration (CPE), a Package URL (PURL), or both.
Exploitability Data	
Vulnerability Identifier	Typically, a Common Vulnerabilities and Exposures (CVE) number or GHSA ID.
Vulnerability Description	A description of the vulnerability as provided by the source.
Exploitability Status	Lists if the product is affected by the vulnerability. For example, “not_affected.”
Remediation Information	Details on how to handle or fix a vulnerability, if available.

Notes:	During this process, the Fortress team is available to assist with any questions and address any concerns you may have. We can also provide examples of SBOMs and VEXs.

SBOM Analysis

Duration:	~1 Business Day to complete analysis
Participants:	Fortress Participants: - Fortress Vendor Risk Analyst - Fortress Risk Assessor
Details:	During this time the Fortress Security Analyst may inspect the SBOM for indicators of completeness of the SBOM and/or VEX and adherence to SBOM format schema standards (i.e., CycloneDX or SPDX). Fortress will analyze SBOM data for areas of risk, for example, potential vulnerable components.
Notes:	There may be follow-up questions and/or potential findings identified during this stage of the process.

Analysis Report

Duration:	<1 Business Day to receive
Participants:	Vendor Participants: - Product Security Manager - Information Security Manager - Information Security Compliance Manager Fortress Participants: - Fortress Vendor Risk Analyst - Fortress Risk Assessor
Details:	After any data updates and the SBOM is analyzed, you will be provided with an overview of potential findings. For example: - The number and severity and of potential vulnerabilities affecting components. - An overview of the number of components which are a minor or major version behind. - Checks hash values of components and compares them to previously known values. - Checks for signs of malicious components. - When available, we look at contributors to the software, both commercial and open source, tell you about their geographic location and list if a code contribution came from certain countries with an adversarial relationship with the U.S.
Notes:	You will have the opportunity to respond to identified findings, provide additional context, explain mitigating controls as applicable, and/or a plan and timeline for remediation. Your comments will be provided to customers who request your SBOMs, and you authorize, to be shared with them.

Share Requests

Duration	Within 3 Business Days
Participants:	Vendor Participants: - Product Security Manager - Information Security Manager - Information Security Compliance Manager Fortress Participants: - Fortress Vendor Risk Analyst - Fortress Risk Assessor
Details:	Once your SBOM is in the system, a mutual customer can request you to share your SBOMs with them. When requests are made, you will receive a notification alerting you to the request. You can review and approve or deny requests to share SBOMs with requestors. Approvals are granted on a per user basis. During your product's support cycle, we expect patches or software updates. We ask that, as your product is updated, these new versions are uploaded as well so your customers have the most up-to-date version of the SBOM for the product they're using.
Notes:	Major version changes necessitate a new SBOM. SBOMs for minor version updates or patches may be uploaded as well.

What's Next?

Once the SBOM is uploaded and analysis is completed, a copy of the report will be provided to you in the vendor portal. You will be provided with a listing of the products and versions we are looking for on behalf of our mutual customers.

- Verify Points of Contact.
- Upload SBOMs for Specific Products.
- Review Share Requests.
- Upload new SBOMs as product versions change.

If not already a participating member, consent to joining the NAESAD: complete the non-disclosure and sharing agreement.