ASSET
TO VENDOR
NETWORK

Prepare for CIP-013 with A2V security and compliance solutions

The **Asset to Vendor Network** for power utilities is a collaborative platform for sharing vendor and product assessments and vulnerability patch validations to enhance security and expedite compliance.

EASIER

Streamlined to emerging industry requirements

FASTER

Information is instantly and continuously updated

BETTER

Satisfies emerging guidance on implementing compliance standards

How A2V Works

Risk Identification

- Utility determines the appropriate assessment level for the vendor or product
- A2V offers risk ranking analytics for easy, fast prioritization

Assessment Selection

- Utility submits the list of vendors requiring assessments
- Assessment status: Available, and Scheduled or Not Yet Scheduled is appended with respective dates
- Utility purchases available assessments. if unavailable, utility has the option to master a new assessment

Vendor Engagement

- Consent to share assessments is obtained by A2V from vendors
- For new assessments, A2V works with vendors to complete them
- Mastered assessments generate royalties of 75%, 65% and 50% on the 1st, 2nd and 3rd+ sales, respectively
- Completed assessments are downloaded into the utility’s instance of the Fortress Platform, the A2V compliance system

FORTRESS
Information Security

A2V Technical Details

A2V is the comprehensive solution

FORTRESS PLATFORM (FP)

(A2V System of Record)

- Risk identification tracking
- Vendor portal for secure exchange
- Vendor, product and service tracking
- Incident and access notice, and controls documentation
- Questionnaire, response and document management
- Vulnerability findings, workflow and remediation tracking
- Dashboards for executive insights
- Deployed on-prem or in cloud

ASSESSMENT SERVICES

- Vendor controls and product assessments
- Data-driven assessments (no vendor interaction, satisfying emerging guidance when assessments may not available)

CONTINUOUS MONITORING

- Threat Intel
- Breach notifications
- Foreign ownership alerts

FILE INTEGRITY APPLICATION

(also addressing CIP-010-3 R1.6.2) - Compare downloaded patches with pre-validated hashes

Build, buy or partner?

	In-House	Assessment Outsourcer	Fortress with A2V
Cost	$150k	$200k	$140k*
Comprehensive compliance platform with workflow, signoff, risk mitigation, reports demonstrating NERC compliance	- (spreadsheets and email)	Limited	Yes
Advisory tailored to industry	-	-	Yes
Product assessments	Yes	-	Yes
Open/private source assessments	-	-	Yes
Continuous monitoring	-	-	Add-on
File authenticity & integrity verification	Not included in cost	-	Add-on

*Scenario based on up to 200 vendors.

A2V assessments are comprehensive

	SOC 2 Type 2	Standardized Controls Assessment	Product Assessment	A2V Assessment
Data management controls	Yes	Yes	-	Yes
Results are validated	Yes	-	-	Yes
Auditor Independence	-	- (n/a - no auditor)	- (n/a - no auditor)	Yes
NATF draft supplier criteria	40% overlap	65% overlap	unknown	Yes
Continuous monitoring and alernative research*	-	-	-	Yes
Product CIP information	-	-	Yes	Yes
Product security assessment	-	-	Partial (only what vendor provides)	Yes
File integrity and authenticity	-	-	-	Yes

*Product non-conformance/counterfeit alerts, vulnerablities, vendor regulatory, compliance, negative news, cyber posture, privacy, financial, etc

CIP-013 Requirements	A2V Solutions
R1 Each Responsible Entity shall develop one or more documented supply chain cybersecurity risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include: **1.1.** One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cybersecurity risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).	Assessments, monitoring, FP for risk assessment to remediation
1.2. One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable: **1.2.1.** Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cybersecurity risk to the Responsible Entity;	FP vendor portal and findings workflow
1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cybersecurity risk to the Responsible Entity;	
1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;	
1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;	FP vendor portal, Monitoring
1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and	File Integrity Application
1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor.	FP control finding workflow
R2 Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1	
R3 Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	