



RELIABILITY FIRST

2020 Fall Virtual Workshop

August 25, 2020

Forward Together



ReliabilityFirst

RF Fall Virtual Workshop

Supply Chain and CIP-013

Ray Sefchik
Director, Entity Engagement
August 25, 2020



- **Host – Ray Sefchik, Director Entity Engagement**
 - Opening Remarks
 - Presenters from AEP, Fortress Information Security, NERC, OSI, RF, and SERC
- **Time – 1:00–5:00 PM**
- **Audience Feedback, Questions/Answers, Polls**
 - Slido.com

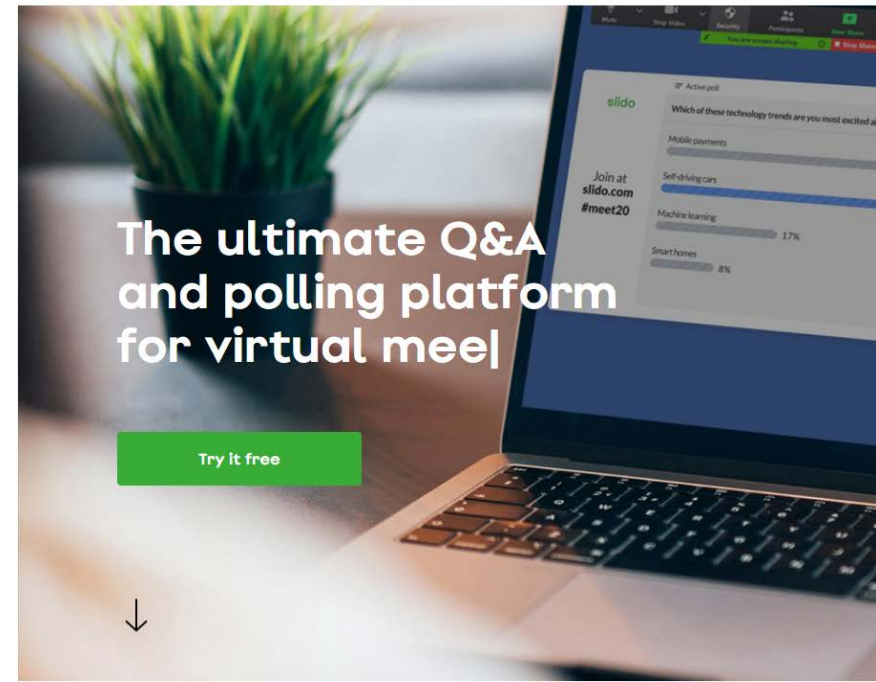
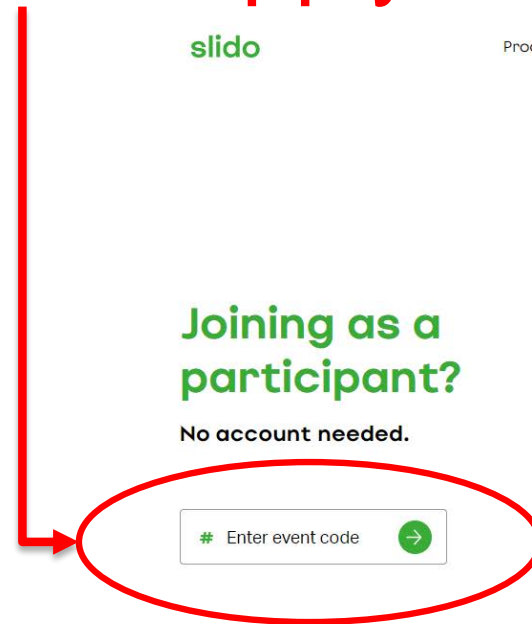
Audience Feedback, Questions/Answers, Polls

➤ SLIDO.com

- Event Code: #RFSupplyChainWS



or



Works with your video conferencing tools, either by embedding Slido or by simply sharing your screen.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Supply Chain Updates

Brian Allen, CIP Assurance Advisor
RF Fall Workshop
August 25, 2020

RELIABILITY | RESILIENCE | SECURITY





- Cyber Security¹
 - Malicious software installed on SCADA offering
 - Unauthorized code found in a firewall solution from a prominent networking hardware company
 - Anti-virus company implicated for an alleged foreign entity backdoor built into security products
- Outbreaks (COVID-19)
 - Large percentage of major companies are seeing supply chain impacts – *Fortune.com 2020*
 - Several major international technology conferences canceled – *cnbc.com 2020*
- Natural Disasters
 - Hurricanes

¹ [NATF White Paper pg.6](#)

- Substation Networking Equipment
 - Two Vendors / 55%
- BES Cyber Systems Operating System
 - One Vendor / 87%
- EMS Vendors
 - Two Vendors / ~60%
- Remote Terminal Unit
 - No vendor more than 20% of market



² [EPRI Supply Chain Risk Assessment Report](#)



- Effective Date: Oct. 1, 2020
 - Pandemic related
- Additional Revisions
 - Open for Comment until September 10
 - Includes Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS)
- 1600 Data Request - Dec. 2019
 - Recommendation to include Low Impact BES Cyber Systems (LIBCS)
 - Project 2020-03
- 2019 SGAS FAQ released February

³ [Supply Chain Risk Assessment: Analysis of Data Collected Under the NERC Rules of Procedure Section 1600 Data Request](#)

- Supply Chain Working Group (SCWG)
 - Released a series of webinars that started in March
 - Several Security Guidelines posted
- ERO Endorsed Implementation Guides
 - [Cyber Security Supply Chain Risk Management Plans](#)
 - [CIP-010-3 R1.6 Software Integrity and Authenticity \(NATF\)](#)
 - [CIP-013-1, R1, R2 - Supply Chain Management \(NATF\)](#)
- NERC/FERC Joint White Paper
 - Help industry with vendor identification
 - Specifically Network Interface Controller
- NERC Compliance and Certification Committee (CCC)
 - Supply Chain Task Force

- Sessions held October 29-31, 2019
 - Previous sessions held in 2018
- Total of 24 Individual Small Group Sessions
 - Small to Large MRREs
- Representation from all regions within the ERO Enterprise
- Two Speakers during General Session \ Webinar
 - EEI
 - NATF
- Live Question and Answer

- Approaches
 - Consulting vs. Internally Built Solution
- Procurements
 - Services vs. Products
- Implementations
 - Risk Matrix vs. Questionnaire
- Applicability
 - Medium and High BES Cyber Systems (BCS)
 - Additional considerations for LIBCS, PACS, EACMS, etc.
- Risk Mitigations
 - Overarching vs. Individualized



- Various Programs
 - CIP-013 is not prescriptive
- Open Source are procurements
- Navigating through resellers
- Cancelled procurements
 - Should evidence be retained?
- Current MSAs used for procurements after Oct. 1, 2020
- Risks must be addressed
 - Purpose of standard is to mitigate risks as appropriate





- The FAQs are:
 - Not intended to establish, modify, or interpret the requirements.
 - Not a substitute for compliance with NERC's Reliability Standards requirements.
 - Agreed upon responses from the ERO Enterprise to commonly asked questions from participants of the SGAS.

- What if a registered entity has a master agreement effective before the effective date of CIP-013-1 (Oct. 1, 2020) which does not include terms associated with CIP-013-1 R1 Part 1.2 and its sub-parts, and purchases products or services after Oct. 1, 2020; do I need to conduct a risk assessment on the vendor?
 - *The risk assessment should be performed on the vendor, product, and/or service as dictated by the SCRM plan. The registered entity's SCRM plan determines where and how the risk assessment is performed. Regarding R1 Part 1.2 and its sub-parts, while the action to renegotiate or abrogate existing contracts is not required, it is expected that mitigations are implemented to address the risks of these elements not being contractually binding on the vendor. All procurements of products or services applicable to high or medium impact BES Cyber Systems after Oct. 1, 2020 would be applicable, under the R1 SCRM plan and R2 implementation.*

- Are existing deployed BES Cyber Systems grandfathered in under CIP-010-3 and CIP-005-6?
 - *Only procurements for applicable BES Cyber Systems that occur on or after the effective date (Oct. 1, 2020) are in scope for the CIP-013-1 procurement planning processes. However, CIP-005-6 (R2 Parts 2.4 and 2.5) and CIP-010-3 (R1 Part 1.6) become effective on Oct. 1, 2020 and apply to all high and medium impact BES Cyber Systems, including existing applicable BES Cyber Systems.*
- What if my vendor will not cooperate with my requests?
 - *An alternative vendor should be considered for the product or service, however, as this is not always possible, remember to reference the 'Note' in R2 which dictates that a vendor's inability to adhere to what is prescribed is beyond the scope of the requirement. While the contract is one means of addressing this concern, if the entity is not willing to abide by the terms and conditions then additional controls and mitigating strategies should be put in place.*

- What should a registered entity do if a vendor is purchased by another vendor?
 - *One approach is to ensure the registered entity's SCRM plan details the process to re-evaluate or reassess the vendor(s). This should include the controls the registered entity deploys to maintain awareness of possible vendor acquisitions. Another is placing "applicable source code and documentation" in escrow held by a trusted third party.*
- What if I buy hardware or software directly from a source without a contract?
 - *Any equipment, software or services acquired on or after Oct. 1, 2020 that will be directly associated with a high or medium impact BES Cyber System is subject to the Supply Chain Risk Mitigation Plan.*

- Is a registered entity a vendor if they are providing non-reliability services for another registered entity (i.e., relay technician, substation maintenance work)?
 - *In this situation, the registered entity providing the non-reliability service could be considered a vendor providing related services. The Supplemental Material on page 12 of CIP-013-1 states, “The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the registered entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority (BA) or Reliability Coordinator (RC) services pursuant to NERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.”*
 - *Same response is applicable to hardware and software.*

- Is open source software in scope for CIP-013-1 and CIP-010-3?
 - *The Supply Chain Standards are silent on terms and conditions for procured products or services that registered entities may install. A registered entity should implement its risk identification and assessment methodology for all procurements and installations of open-source software on applicable BES Cyber Systems.*
- What compliance documentation and evidence should a registered entity create and maintain to comply with CIP-013-1 R1 Part 1.2 and its sub-parts for software that has no associated vendor, such as open source software?
 - *The registered entity may address Part 1.2.1 and Part 1.2.4 by developing one or more internal processes to identify and monitor reputable third-party sources for assessments and reports of applicable open source software incidents or vulnerabilities. The registered entity may consider developing a modified Part 1.2.5 process for acquiring, verifying and authenticating such software and applicable patches, as released by reputable sources (e.g., for software upgrades or security patches for identified vulnerabilities). An example of this could be a completed evaluation that specifically addresses open source technology.*

- A registered entity buys equipment from a vendor with third-party software installed. What are your recommendations for showing evidence of due diligence?
 - *The registered entity should use its SCRM plan to identify and assess the risks associated with the third-party software installed. The results of this analysis would dictate what mitigations are appropriate to address the risks related to the third-party software. Some common forms of evidence include, but are not limited to, checklists or the contents of a change ticket that documents the due diligence performed.*
- What additional frameworks did registered entities consider in development of Supply Chain Risk Management Programs? Furthermore, are entities developing one or more risk assessment questionnaires?
 - *Entities considered NIST, NAGF guidance, NATF guidance, EEI guidance, SOC2, and ISO27001 in developing their SCRM programs. In most cases, registered entities used two risk assessment questionnaires, one for vendors and one for products or services.*

- Would a registered entity be found non-compliant if their SCRM plan included a provision for an after-the-fact risk assessment to be conducted for applicable medium and high impact BES Cyber Systems implemented under emergency situations?
 - *CIP-013-1 is applicable to any procurement, regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions, such as emergency procurements. A registered entity may identify certain hardware, software or services that may be used during emergencies and perform risk assessments in planning for these situations to mitigate the supply chain risk.*
 - *Although the CIP-013-1 Standard does not directly address emergency procurements, the registered entity could consider including language in its R1 SCRM procurement plan that addresses the potential for the use of purchasing cards in emergency situations. The registered entity should document the emergency procurement process in the R1 SCRM procurement plan, along with documentation that registered entity personnel or approved contractors verified after-the-fact risks and mitigations of the procurement.*



- Include procurements beyond the required Medium and High BES Cyber Systems
 - EACMS, PACS, LIBCS, etc.
- Utilize secure hardware delivery
- Apply a Third-party Accreditation Process to evaluate vendors/products
- Create a process to address unsupported or Open-Sourced Technology
- Reference other frameworks provided by NIST, SOC2, and ISO20071, as well as other materials from NATF, NAGF and EEI

- Continual education on Supply Chain through regional workshops
- Regions are open to answering any questions related to CIP-013
- Reference NERC.com's 'Supply Chain Risk Mitigation Program' page often





Questions and Answers

RF Compliance Approach to Supply Chain

Shon Austin
Principal Technical Auditor, CIP
RF Fall Virtual Workshop
August 25, 2020



Learning Objectives

➤ After this presentation, you will understand:

- Purpose, expectations challenges, and **best practices*** of the CIP-013 standard
- R1: Develop a supply chain risk management (SCRM) plan
- R2: Implement the SCRM plan
- R3: Review and approve the SCRM plan

* Best practices are suggested by RF staff but are NOT required by the standard



Each Responsible Entity shall develop a documented supply chain cyber security risk management plan for high and medium impact BES Cyber Systems.



Possible Challenges

- Failure to:
 - Identify cyber security risk(s)
 - Assess cyber security risk(s)
 - Remediate cyber security risk(s)
- Silent on risks to address
- The term vendor is not defined



CIP-013 R1 Part 1.1

One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security 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)



Possible Challenges

- Part 1.1i: Planning for Procuring and Installing
 - Failing to have a process that plans for future acquisitions of products or services that are applicable to BES Cyber Systems
- Part 1.1ii: Planning for Transitions
 - Failing to have a process that plans for future acquisitions of products or services that mitigate vendor transition risks



CIP-013 R1 Part 1.2

Manage the Procurement Controls

- CIP-013-1 Part 1.2.1
- CIP-013-1 Part 1.2.2
- CIP-013-1 Part 1.2.3
- CIP-013-1 Part 1.2.4
- CIP-013-1 Part 1.2.5
- CIP-013-1 Part 1.2.6



CIP-013 R1 Part 1.2

One or more process(es) used in procuring BES Cyber Systems that address the aforementioned procurement controls, as applicable



Possible Challenges

- Failing to address all required process types in the SCRM Plan
- Vendor non-compliance



CIP-013 R2.

Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1



Possible Challenges

Failing to implement the process(es) identified in the SCRM Plan



CIP-013 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



Possible Challenges

- CIP Senior Manager or delegate fail to approve its SCRM Plan
- CIP Senior Manager or delegate approves its SCRM Plan, but without understanding the document



Related Standards/Requirements

CIP-005-7 Part 2.4.

Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)



Possible Challenges

Failing to have a process to monitor active vendor remote access sessions



Related Standards/Requirements

CIP-005-7 Part 2.5

Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access)



Possible Challenges

Failing to have a process to disable active vendor remote access sessions



Related Standards/Requirements

CIP-010-3 Part 1.6.

Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:

- 1.6.1. Verify the identity of the software source
- 1.6.2. Verify the integrity of the software obtained from the software source



Possible Challenges

- Software is not identified on the baseline
- Software source is unknown
- No process to verify the integrity of the software
- Freeware
 - No recognizable source



Questions & Answers

Forward Together  ***ReliabilityFirst***



ReliabilityFirst Fall Virtual Workshop 2020

AEP CIP-013 Supply Chain Program & Fortress Information Security's Asset to Vendor (A2V) Platform

Tuesday, August 25 | 1:50-2:50 PM EST

Featuring Industry Experts:

Jeffrey Sweet

Director of Security Assessments,
American Electric Power



Tobias Whitney

VP Energy Security Solutions,
Fortress Information Security

A tall, modern skyscraper with a red sign that reads "AMERICAN ELECTRIC POWER" is visible in the background. The building is surrounded by trees and a park area with a stone wall and a path.

AMERICAN ELECTRIC POWER

THIRD PARTY RISK ASSESSMENT PROCESS

AUGUST 2020

THIRD PARTY RISK ASSESSMENT PROCESS

- ❖ Where We Were
- ❖ Where We Are
 - ❖ Risk Determination
 - ❖ Risk Rank
 - ❖ Questionnaire
 - ❖ On-site
 - ❖ Contract Supplement
 - ❖ Re-evaluation
 - ❖ Pitfalls
- ❖ Where We Are Going

WHERE WE WERE

Our Problem

- 10's of thousands of third parties
 - Contracts created by a variety of groups
 - No central view of who, what, when, where, or why
- No view of risk
 - Third Parties engaged without consideration of the risk they introduced
 - Did not have any insight into whether they have had a security practice
- Started requiring security language in contracts
 - The first step was to get accountability

WHERE WE ARE

Our Current Program

- Well established, enterprise-wide program
 - Every third party has been evaluated to determine if risk exists
 - All new third parties and third parties who are renewing contracts are being evaluated for level of risk
 - Contract supplements established with many third parties

RISK DETERMINATION

Identifies Vendors Who Have a Probability of Introducing Risk to the Organization

- Short set of 5 questions
 - Unescorted physical access to controlled access area or any access to a critical area?
 - Access to sensitive information, including data collected from customers?
 - Requires any one or combination of following access before, during, or after this engagement effort lifecycle? (Examples: VPN, VDI, firewall changes, RSA token(s) - any type, FTP, network to network connection(s), or any type of remote access)
 - Provide products or services which may affect any NRC and/or NERC CIP regulated environments?
 - Will the third party maintain or share any electronic communications or data such as email, FTP communications, etc. with AEP or AEP personnel?

RISK RANK

Determines the Level of Risk a Third Party Introduces

- Set of ~25 questions that identifies:
 - The amount and type of access a third party has to systems, networks and data
 - Where the third party is accessing from
 - How frequently the third party is accessing the data
 - The sensitivity of the data
 - Whether the third party is developing products or services
 - Whether the third party is providing any type of cloud services
 - Whether they are performing financial transactions for AEP

RISK RANK, CONT'D

- Fourth party involvement in the products or services
- Customer facing services
- Strategic third party
- Number of alternative third parties
- Concentration of the line of business provided by third party
- Questions are answered by the line of business

QUESTIONNAIRE

Asset To Vendor Questionnaire

- Comprehensive Questionnaire
 - Assesses security practices within the third party's environment
 - Deep dive with intent to provide information to other industry participants, when given permission to do so by the vendor
 - Develop information on gaps in expected practices to determine risk
 - Develop “Findings” out of gaps in practices
 - Collects sufficient information to provide value to others in the industry

ON-SITE ASSESSMENT

Validation of the Stated Controls

- Validates information provided in other parts of the assessment
- Provides ability to get a sense of the culture of the company
- Typically done on most critical risk ranked vendors and those who have been breached

CONTRACT SUPPLEMENTS

Accountability for Controls

- Aligns with questionnaire
- Includes specific requirements
- Holds the third party accountable for the practices they state they have
- Develop “Findings” out of areas that cannot be agreed upon

RE-EVALUATIONS

Staying Up-To-Date

- Four Tiers
 - Annual for most critical
 - Semi-Annual less critical
 - Tri-Annual least critical
- Audit – Breach or sense that vendor is not adhering to the supplement
 - Scheduled 30 or more days out, no more than once per year

PITFALLS AND DIFFICULTIES

Continuously Improving the Process

- Time and Resource intensive
 - Approximately 30 – 80 hours for a full assessment
 - Pushback from third parties
 - Be prepared – must have a process to address pushback
 - Risk Mitigation/Remediation
 - Risk Acceptance
 - Risk Transfer
 - Risk Avoidance
 - May need to tell the third party you are no longer willing to do business with them

WHERE WE ARE GOING

Making the Future Brighter

- Building a solution to assist the industry
 - A2V
 - Platform to exchange controls assessment data with other utilities (CIP-013)
 - FIA
 - Ability to validate the source and integrity of software, firmware and patch downloads (CIP-010 – R1.6.1 and R1.6.2)
 - Ability to perform malware analysis of files retrieved
 - Deposited into a central repository for all persons needing code
 - VuINEXT
 - Ability to identify vulnerability, determine availability of patch and process the patch for deployment

A tall, modern skyscraper with a red sign that reads "AMERICAN ELECTRIC POWER" is visible in the background. The building is surrounded by trees with autumn foliage and a grassy park area in the foreground.

AMERICAN ELECTRIC POWER

THIRD PARTY RISK ASSESSMENT PROCESS

AUGUST 2020



FORTRESS

Information Security



OUR MISSION

Secure critical infrastructure by implementing controls-based automation at economies of scale



Approximately 100 employees



Rated in Orlando's "Top 10 Places to Work"



Clients have a direct line to Fortress executives

Making Success Reliable

Fortress Knows Utilities

15%

Securing 15% of US power grid

\$300K

Managing \$300K+ in assets

+

40K

Managing 40K+ vendors

+

CIP-002
to 014

Managing CIP-002 to 014 and other frameworks

Flexible Solutions

- Fortress platform comes preconfigured or customized
- Dedicated developer resources ensure perfect fit
- Existing tools are integrated for complete visibility
- Bridge vendor and asset (IT/OT/IoT/IIoT) risk management



FORTRESS
Information Security

Platform



Fortress Platform Capabilities

1

Out of the box workflows

- Automated Threat Management (ATM)
- Vulnerability, Patch and File Integrity Management
- Complete Supply Chain Solution

2

NERC CIP Standards-based workflows based on NERC's Evidence Request Tool

3

Analytics dashboard and compliance automation geared to reduce security O&M

- Manage real-time security threats while mitigating compliance exposure



Built to Manage CIP Requirements

Foundations

CIP 002-BES Cyber System Categorization

- Identify and Certify BES Assets
- Impact Ratings

CIP 003-Security Management Controls

- Security Awareness
- Physical
- Electronic Access
- CSIRT

CIP 004-Personnel & Training

- Security Awareness
- Identity Confirmation
- Min. Access

Cyber Security Protection

CIP 005-Electronic Security Perimeter

- Perimeter Isolation
- Remote Access
- Monitoring

CIP 007-System Security Management

- Network Access
- Patch Management
- Malware Prevention
- Event Monitoring
- Access Control

CIP 010-Config. Change Mgmt. and Vuln. Assessments

- Configuration Baseline
- Change Monitoring
- Vuln. Assessments

Physical and Supply Chain

CIP 006-Physical Security BES Cyber Systems

- Define Controls
- Monitor Access Controls for Authorized, Unescorted Physical Access
- Alert System

CIP 011-Information Protection

- Identify BES Cyber System Information
- Procedures to Protect Information Storage, Transit and Use

CIP 013-Supply Chain Risk Management

- Vendor Risk Mgmt. Plans
- Remote Access
- Software Integrity
- Known Vulns
- Security Incidents & Exposures

CIP 014-Physical Security

- Risk Assessments of Transmission Stations
- Third Party Verification
- Threats & Vuln. Analysis

Incident Response

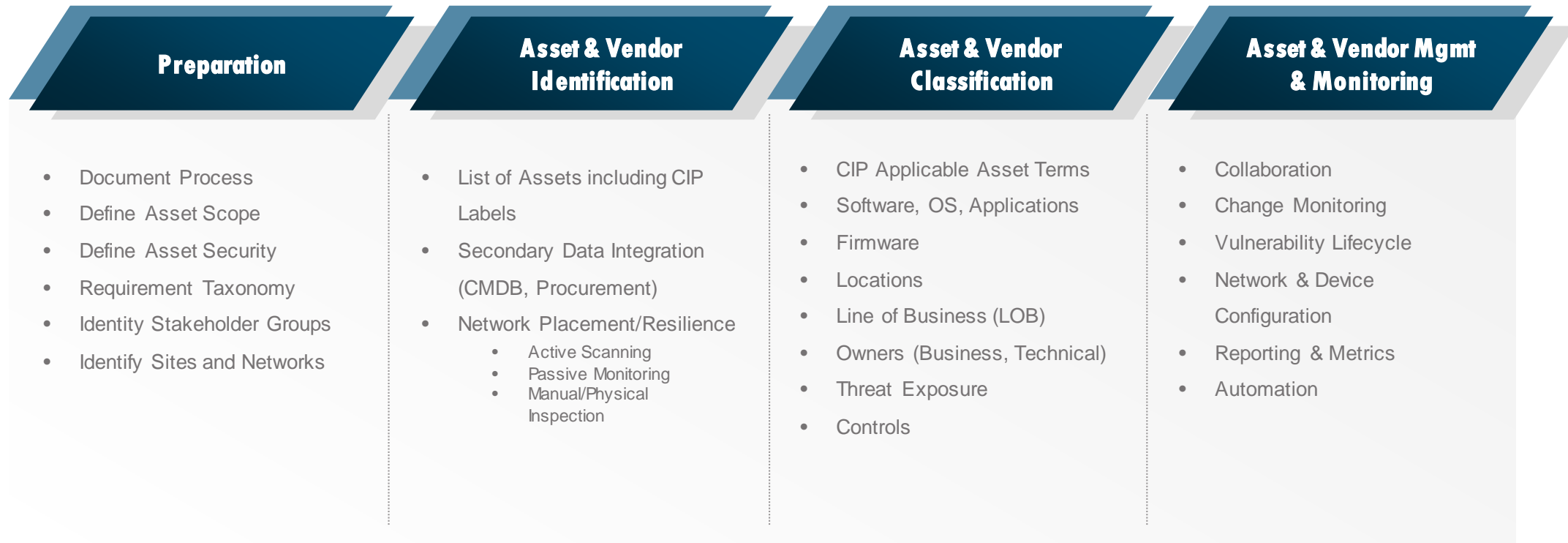
CIP 008-Incident Reporting & Response Planning

- Processes to Identify, Classify & Respond
- Incident Response Group Roles

CIP 009-Recovery Plans for BES Cyber Systems

- Conditions for Activation of Recovery Plans
- Responder Responsibilities

Asset to Vendor Management – “A2V”



Managed Services

Fortress provides vendor and product assessments, resolution and program management.

Services can be interchanged throughout the contract.

Software

Fortress Platform integrates with leading security platforms and procurement systems.

It features risk management orchestration through workflow, approvals, dashboarding, customized reports and vendor portal.



Exchange

Asset to Vendor Network is the only exchange that is utility focused, offers royalties, provides both product and vendor assessments.

Data

Fortress subscribes to dozens of data sources and has a team of 30 research analysts that enable data-driven solutions and comprehensive monitoring.

These solutions cover financial, legal, regulatory, safety, compliance, cybersecurity, country, fourth party and reputation risks.

NERC CIP Standards: Supply Chain Risk Management

- CIP-013-1: “One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security 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).”
- CIP-010-3: Software Identity & Integrity
- CIP-005-6: Detect and Disable Vendor Connections (including system-to-system)

All Reliability Standards		Standards Filed and Pending Regulatory Approval	
Mandatory Standards Subject to Enforcement		Standards Pending Regulatory Filing	
Standards Subject to Future Enforcement		Inactive Reliability Standards	
		Pending Inactive Reliability Standards	

Standards Subject to Future Enforcement

Standard Number	Title	Contains Retired Requirements	Related Information
§(BAL) Resource and Demand Balancing (1)			
§(CIP) Critical Infrastructure Protection (5)			
CIP-005-6	Cyber Security — Electronic Security Perimeter(s)		Related Information
CIP-008-6	Cyber Security — Incident Reporting and Response Planning		
CIP-010-3	Cyber Security — Configuration Change Management and Vulnerability Assessments		Related Information
CIP-012-1	Cyber Security – Communications between Control Centers		
CIP-013-1	Cyber Security - Supply Chain Risk Management		Related Information
§(PER) Personnel Performance, Training, and Qualifications (1)			
§(PRC) Protection and Control (3)			
§(TPL) Transmission Planning (3)			

home | account log-in/register | legal and privacy/trademark policy | site map | careers | contact us

Atlanta Office | 3353 Peachtree Road NE, Suite 600 North Tower Atlanta, GA 30326 | 404.446.7560

Data-Driven Risk Ranking - Process

When you need instant visibility

DDRR was developed to overcome the challenge experienced by many third-party risk management programs – “Where do I even start?”

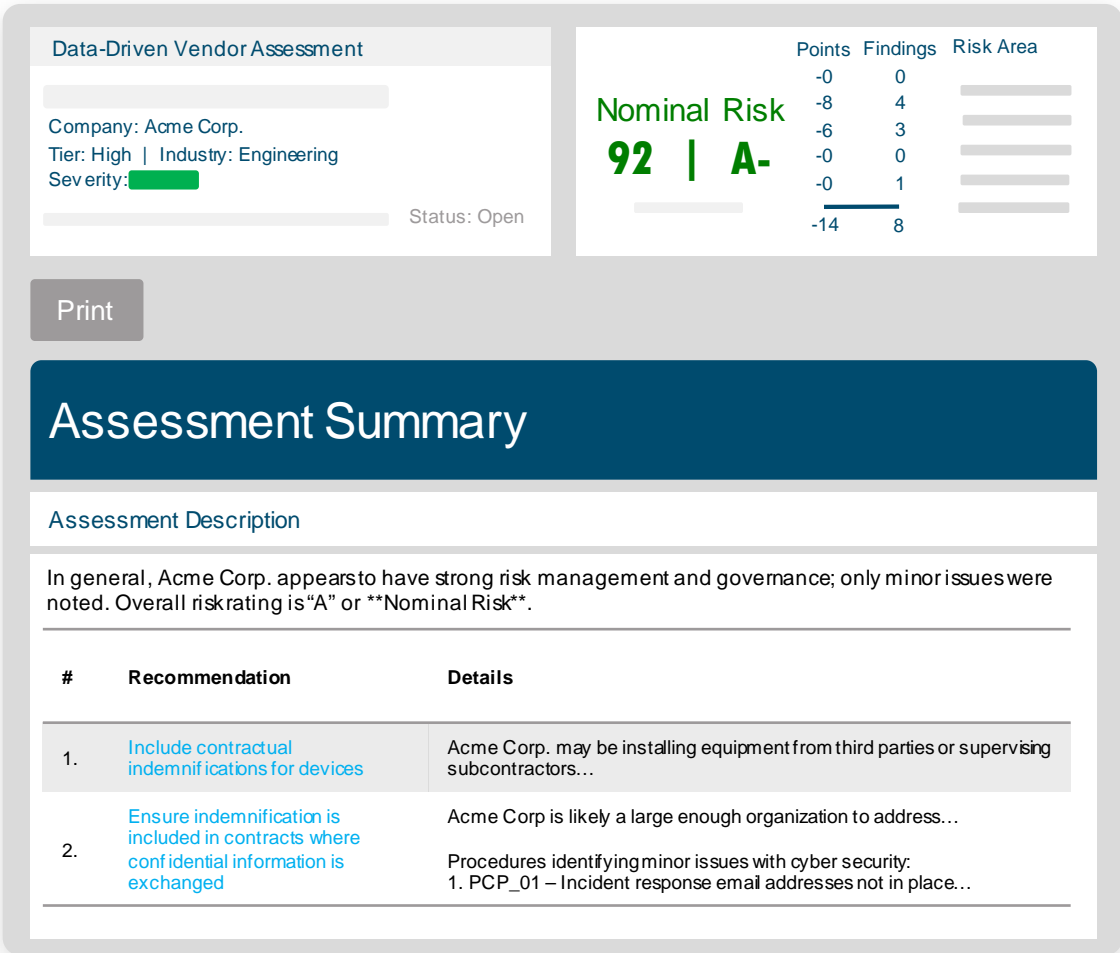
Metrics	Manual Risk Rank	Data-Driven Risk Rank	Improvement
Cycle Time	30-day industry avg	Days to process	20x faster delivery
Frequency	Annually	Quarterly	4x more up-to-date
Accuracy	90% assumed*	83%	Trade-off
Projected Coverage	50%	100%	2x more coverage



*Even the manual risk ranks are subject to some error

Data-Driven or Controls-Based Vendor Assessments

- 1 Risk Management Personnel
- 2 Public Cybersecurity Posture
- 3 Web Scanner Results
- 4 Negative News, Compliance, Sentiment
- 5 Financial Position and M&A
- 6 Privacy Incidents & Policies
- 7 Fourth Party Incidents



Product Assessments

Inherent Risk, Vulnerability and Patching Cadence, Security Controls Capabilities

Product Assessment

Date: Thu Oct 15, 2020

Product Details

Detail 1	Text
Detail 2	PC
Company	Acme
Assessor	Joe Miller
Date	10/15/20
Status	<div></div>

Assessment Risk Areas


Moderate Risk
78 | C

Product Risk Profile

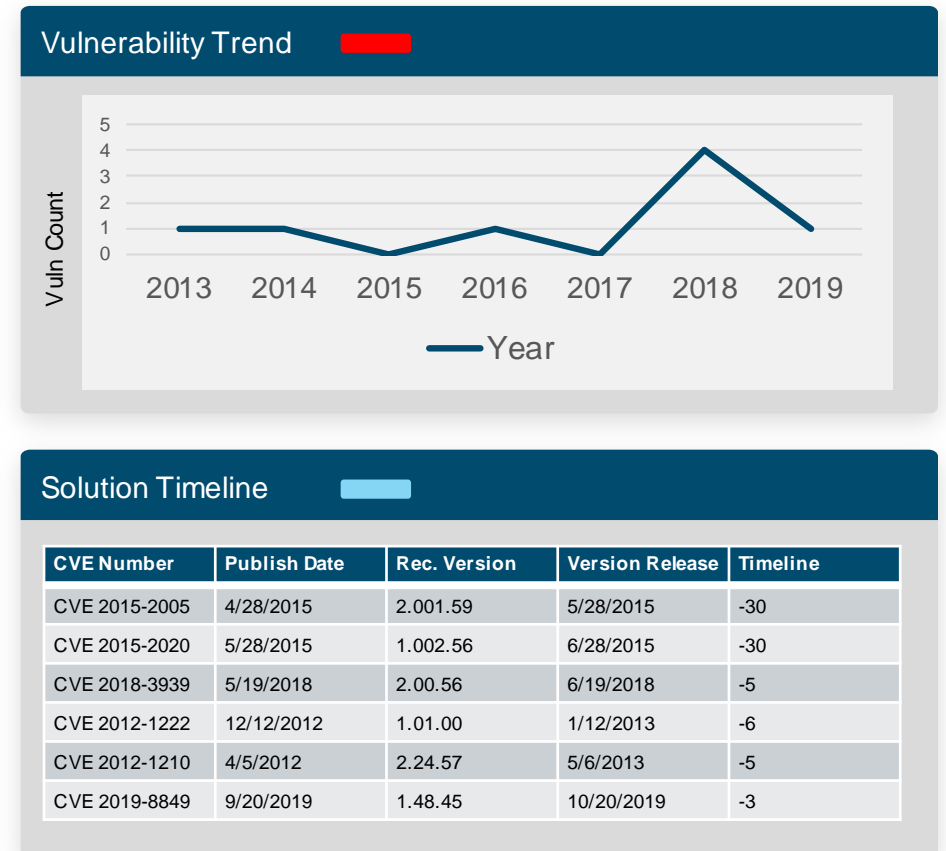
Risk Profile 2

Risk Profile 3

Product Description



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.



Executive Order: Supply Chain

Understanding the Utility Challenge and Call for Action



Current State Utility Challenges

- Focused on achieving compliance to CIP-013 (compliance begins 10/1/20)
- EO expands the scope of utility preparation (requires low impact to be addressed)



The EO's 4-Pillar Approach

- Prohibit foreign adversaries from supplying BPS as it pertains to national security and critical infrastructure.
- Secretary can prequalify suppliers for BPS use
- Identify assets on the system that are at risk/vulnerable today (at risk equipment will be replaced/mitigated)
- Establishment of a task force that will develop infrastructure procurement policies



Opportunity – Call for Action

- Industry to begin evaluating where foreign adversarial products are used on the grid
- Leveraging tools that can provide vendor and product clarity, transparency and provenance

Executive Order

Foreign Adversarial Affiliations of BPS Vendors

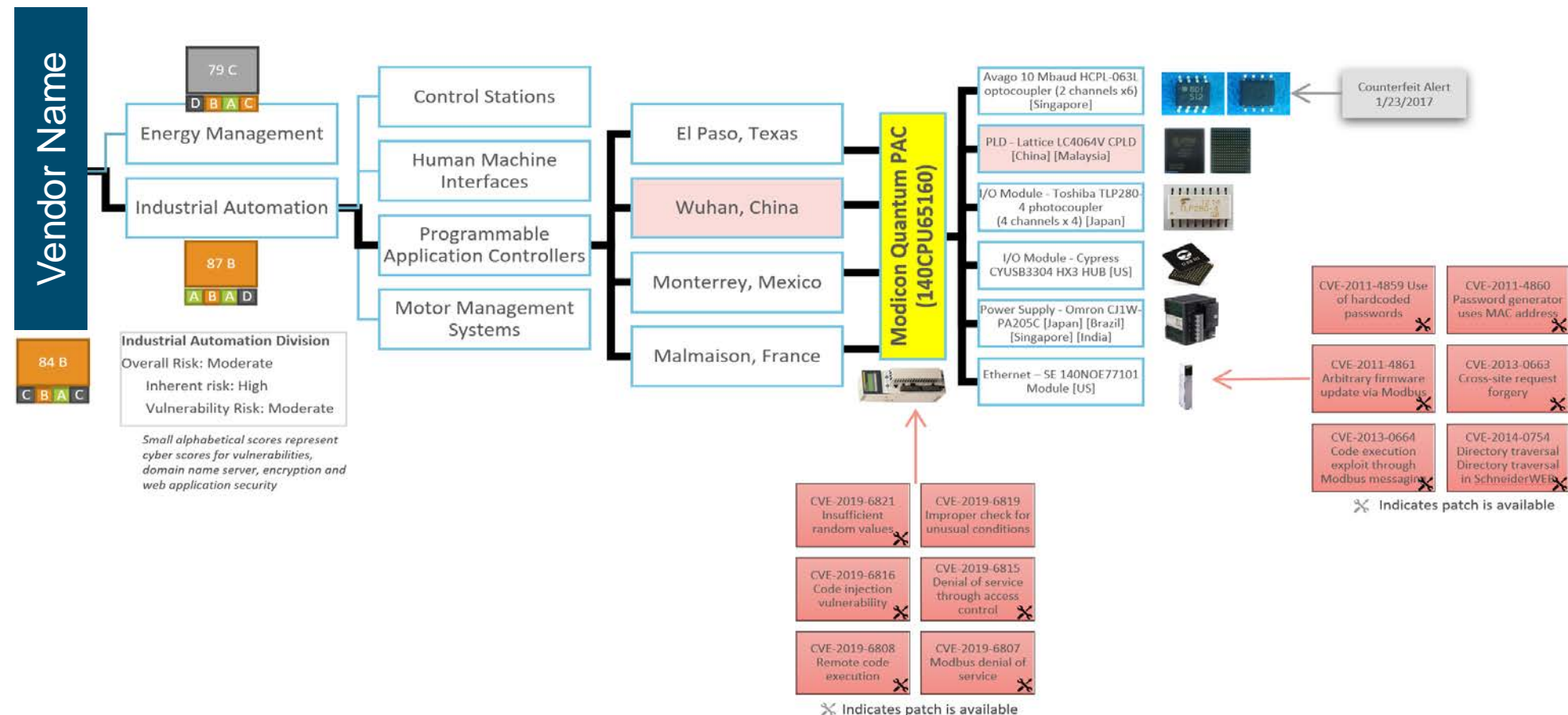
What is FOCI:

- Foreign
- Ownership
- Control
- Influence

Company	Watchlist	Cyber Presence	Physical Presence	Corporate Families	Foreign Ownership	Merger & Acquisition	Manufacturing Locations
Vendor 2	N	N	China	China	N	N	China
Vendor 3	N	N	China/Russia	China/Russia	N	N	China
Vendor 4	N	N	China/Russia	China/Russia	N	China	China
Vendor 5	N	N	N	N	N	N	N
Vendor 6	N	N	N	China	N	N	N
Vendor 7	N	China	N	N	N	N	N
Vendor 8	N	China	China/Russia	China/Russia	N	N	China/Russia
Vendor 9	N	N	China	China/Russia	N	N	China
Vendor 10	N	N	China	China/Russia	N	N	N

Product Level Provenance - Example

Bulk-Power Systems





FORTRESS
Information Security



Tobias Whitney

Vice President – Energy Solutions

(407) 325-5543

[Assettovendor.com/marketplace](https://assettovendor.com/marketplace)

twhitney@fortressinfosec.com

Fortress Information Security

189 S. Orange Ave., Suite 1950

Orlando, FL 32801

fortressinfosec.com

Thank you!

AssetToVendor.com

(407) 573-6800

Sales@AssetToVendor.com



Forward Together  ReliabilityFirst

SUPPLY CHAIN AND CIP-013 WORKSHOP

AFTERNOON BREAK

WE'LL BE BACK IN 10 MINUTES!

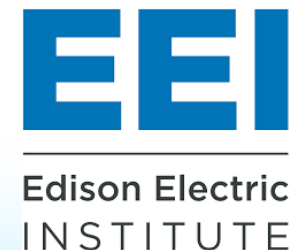




OSI Approach to CIP-013 & Supply Chain Security

Industry Participation & Approach to Supply Chain Security

- **NERC CIP-013 Drafting Team**
 - Participation as a vendor with the drafting team at multiple meetings prior to CIP-013 approval
- **NERC – SCWG Supply Chain Working Group**
 - OSI participation in the SCWG meetings and short papers
- **NATF - North American Transmission Forum**
 - Vendor participation in the development of the NATF Criteria
 - OSI responses to the NATF CIP-013 “Criteria” with OSI responses – Jan.2020
 - OSI responses to the NATF Energy Sector Supply Chain Risk Questionnaire – June 2020
- **EEI – Edison Electric Institute**
 - OSI Adoption of the EEI CIP-013 Procurement Language - May 2020



Adoption of ISO-27001

- OSI Has adopted the ISO-27001 security framework
- Independent auditing for CIP-013 and Supply Chain Security is critical for vendors
- ISO-9001 Quality Standard has been used by equipment suppliers for 30+ years
- ISO-27001 is a globally recognized standard for cyber security and information protection
- 27001 has controls that directly map to NIST Cyber Security Controls as documented by NIST
- ISO offers a certification program that requires annual auditing by independent accredited auditors



<https://www.iso.org/isoiec-27001-information-security.html>

ISO-27001 Prescriptive Requirements

- ISO-27001 and its appendix 27002 include prescriptive requirements for:
 - Risk Assessment and risk management/mitigation as the core foundation
 - Detailed policies, procedures and tools for the protection of operational IT systems
 - E.g. anti-malware, network segregation, firewall rules, access procedures, new software assessment
 - Secure software development requirements including:
 - source code protection, secure development training, software testing, vulnerability management
 - Background screening requirements of all employees
 - Classification & protection of sensitive data – customer information, trade secrets etc.
 - Role based access (e.g. to OSI customer assets & information)
 - Access & notification procedures for employee changes (e.g. termination, role change)
 - Third party supplier security assessments & agreements

27002 Requirements: https://webstore.ansi.org/preview-pages/ISO/preview_ISO+IEC+27002-2013.pdf

What does ISO-27001 Certification Entail?

- ISO Certification can only be granted by accredited independent auditors (e.g. British Standards Inst., TUV)
- Review of risk assessment, tracking and mitigation mechanisms to monitor critical organizational risks
- Ongoing security metrics and improvement are tracked (e.g. phishing exercises, security incidents)
- ISO auditors examine policies, procedures and sample evidence for the annual review period
- Annual audits require resolution of any findings within specified timelines or certification is revoked
- NERC auditors and your compliance team can trust that security policies & procedures are followed



OSI Supply Chain Security Framework based on ISO-27001

- OSI Framework covers OSI 27001 implemented policies & procedures for CIP-013 relevant areas of operation:
 - Secure Software Development Lifecycle
 - Employee Personal Risk Assessments
 - Notification of cyber incidents
 - Notification of employee terminations
 - Third Party Supplier screening
 - Vulnerability Management
 - Protection of sensitive data (e.g. BCSI)
 - Secure software delivery
 - Secure remote access to entity systems
 - Copy of ISO-27001 auditor report & certification



Where? OSI Secure Members Website: CIP-013 Page













Supply Chain Security / CIP-013

This portal provides our customers with the most recent news and documentation related to Supply Chain Security as required by the NERC CIP-013 standard which becomes effective July 1, 2020. We believe that this information will also be helpful to our many OSI customers who are not required to meet the NERC CIP-013, but may be concerned about Supply Chain Security.

Please contact CIP13@osii.com if you have any questions.

Documentation

	New		Upload		Share
✓		Name	Modified	Modified By	
		CIP-013_Advisory_DEC2019	... March 5		
		OSI_27001_Cert_IS_712855	... May 11		
		OSI_CIP-013_Approach	... April 29		
		OSI_Model_Contract_Language	... June 16		
		OSI_Responses_to_NATF_Criteria	... July 15		
		OSI_Supply_Chain_Security_Framework	... May 13		

Drag files here to upload

How does OSI Meet CIP-013 Requirements?

- R1.1 - methods to identify and assess cyber risks for new vendor equipment & software
 - Implementation of ISO-27001 Supply Chain Security Framework
 - NATF Criteria Responses
 - Responses to the NATF Energy Sector Supply Chain Risk Questionnaire
 - OSI Framework sections 1, 2, & 3
- R1.2.1 – Notification of vendor cyber incidents
 - 27001 Policies requiring OSI notification of affected customers
 - OSI contractual language includes this requirement
 - OSI Framework section 21
- R1.2.3 - Notification by Vendors when remote access should no longer be granted
 - Established 9001 procedure in May 2016 and now 27001 policy
 - Notification to customers of OSI employee terminations
 - Specific notification examples were independently audited by British Standards Institute March 2020
 - OSI Framework sections 8, 9, & 10

How does OSI Meet CIP-013 Requirements?

- R1.2.4 - Disclosure by vendors of known vulnerabilities related to the products or services
 - Established 27001 Vulnerability Management Policy based on software industry approach “Coordinated Vulnerability Disclosure”
 - Requires notification to all customers of a product vulnerability once a mitigation is available
 - OSI Framework section 24
- R1.2.5 – Verification of vendor software authenticity and integrity
 - Established 27001 Secure Software Delivery policy, procedure and “SVT” tool
 - OSI Framework section 13
- R1.2.6 – Coordination of controls for i) Vendor-initiated Remote Access and ii) system to system remote access
 - 27001 Remote Customer Access policy, procedure and platform
 - OSI Framework section 10

How does OSI Meet CIP-013 Requirements?

- R2 - Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts
 - Adoption of EEI Model Procurement Language
 - Downloadable from OSI CIP-013 website
 - Copy included in OSI Framework section A4

Our Supply Chain Security Philosophy



- All OSI software & hardware is developed in the U.S. under strict security guidelines & procedures
- Hardware product manufacturing/assembly at U.S. suppliers with oversight by U.S. employees
- OSI is committed to supply chain security for all components of our products & systems
- General corporate philosophy is to minimize our supply chain footprint
- Our approach to supply chain security is pragmatic and based on assessed risk
- All suppliers are vetted and monitored to ensure they meet OSI security criteria
- We value our continued partnership with industry groups to achieve common sense supply chain security
- Questions? Contact CIP13@osii.com



The background image shows a harbor scene. On the left, a tall, grey lighthouse stands on a rocky outcrop. In the center, a large container ship is docked at a pier. To the right, a smaller blue and white boat with the number '22' on its side is moving across the water. The sky is blue with scattered white clouds. A semi-transparent purple banner covers the middle section of the image, containing the text.

Welcome

SUPPLY CHAIN ONLINE LEARNING

Banna Underland, Technical Writer & Training Coordinator, SERC

Lew Folkerth, Principal Reliability Consultant, RF

RF Fall Virtual Workshop

August 25, 2020

TOPICS

Background



Online Learning
for SERC
Assistance

Collaboration



SERC and RF

Supply Chain



What's the BIG
DEAL?

SCRM Modules



Current and
Future



We always welcome questions!



BACKGROUND

Online Learning for SERC Assistance

Early Days of the Program

Goal: Provide Value for Entities

Method: Entity Request (for
assessment, coaching, training, etc.)

Online Learning Modules as Option for
Training

Aspiration: High Level of Expertise

ONLINE LEARNING PROGRAM



18+

COURSES

We add new courses, on average, every other month.



427

COURSES TAKEN

2018 – 69
2019 – 126
2020 – 232*
(*through July)



192

CERTIFICATES

Not everyone who takes a course requests a certificate.

RF and SERC Working Together

Supply Chain - Important topic with many subtopics

Small group at SERC

RF has excellent reputation with lots of expertise and experience

Let's work together!



A black quadcopter drone is shown in flight against a bright blue sky with scattered white clouds. The drone is carrying a gold-colored metal shopping cart suspended from its underside by four purple chains. The cart is empty and has a black rectangular object, possibly a tablet or a small screen, attached to its side. The sun is visible in the upper right corner, creating a lens flare effect. A purple horizontal band runs across the middle of the image, containing the text.

SUPPLY CHAIN: WHAT'S THE BIG DEAL?

SUPPLY CHAIN

Why has there been so much time and effort spent on this topic?



Reliability Standards

New: CIP-013-1

Changes: CIP-010-3 and CIP-005-6



Organizational Impact

Affects many groups throughout the organization beyond the “normal” Compliance Department



Threats

Many attacks can come through the supply chain. Everyone in the organization should be aware and alert.



GOAL

**SECURING THE SUPPLY
CHAIN**

SCRM Modules: Current and Future

New Releases:

- Supply Chain Risk Management Overview
- Supply Chain Standards: Past, Present, Future

Planned:

- Supply Chain Risk Management Plan
- Supply Chain Risk Management Standards Implementation
- Vendor/Supplier Management
- Procurement: Services and Contracts
- Procurement: Products, Contracts, Master Agreements
- et al.

Access to the Courses

Links to all courses are available on the SERC website: www.serc1.org

The screenshot shows the SERC Reliability Corporation website. At the top, there is a navigation bar with links: Contact Us, My Profile, Login, and a Search box. Below this is a secondary navigation bar with links: About SERC, Program Areas, Committees, and Outreach. The Outreach link is highlighted, and a dropdown menu is visible. The dropdown menu contains the following items: Assistance, Events Calendar, Q&A and Lessons Learned, Newsroom, Registered Entity Forum, SERC101, and Resource Library. The Resource Library link is circled in red. To the left of the dropdown menu, there is a large banner for 'HURRICANE PREPAREDNESS' with a 'View Resources' button. Below the banner, there is a calendar and a section titled 'UPCOMING EVENTS' with a list of events and a 'VIEW ALL' link.

SERC Reliability Corporation

Contact Us My Profile Login Search

About SERC Program Areas Committees Outreach

Assistance
Events Calendar
Q&A and Lessons Learned
Newsroom
Registered Entity Forum
SERC101
Resource Library

HURRICANE PREPAREDNESS
View Resources

CALENDAR

UPCOMING EVENTS

- » Aug 25 - 27, 2020 System Operator Conference #3 - CANCELLED;
- » Aug 25, 2020 PRC-006-SERC Standards Drafting Team Meeting;
- » Aug 27, 2020 Finance and Audit

VIEW ALL

From the
Outreach menu,
select **Resource
Library**

THANK YOU

Banna Underland
bunderland@serc1.org

Lew Folkerth
lew.folkerth@rfirst.org



Supply Chain Risk Management Self-Assessment Tool

Brian Hallett
Principal Reliability Consultant, Entity Engagement
RF Fall Virtual Workshop
August 25, 2020



Agenda

- **Mission and Objectives**
- **Modules for Business Needs**
- **Module #1 Details**
- **Other Self-Assessment Tools**
- **How to Get Started**



Mission and Objectives

- **Provide the ERO with a tool that allows Entities to self-assess their Supply Chain Risk Management capability**
- **Develop a tool and process to supplement work already completed by NATF**
- **Continue development to Model-based tools to drive continuous improvement**

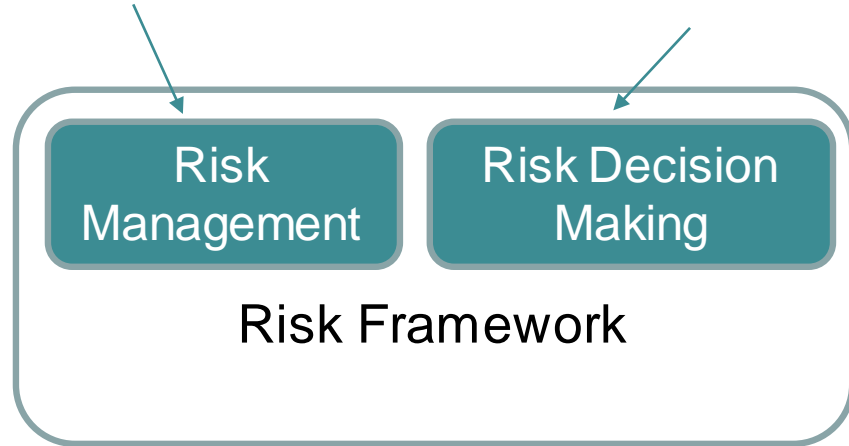


Modules

NIST-800-39/CIP-013
Self-Assessment
(Module 1)

NATF criteria-based
vendor assessment
(Module 2)

Cyber Resiliency
Assessment Tool
(Module 5)



Existing CMMI
material
(Module 3)



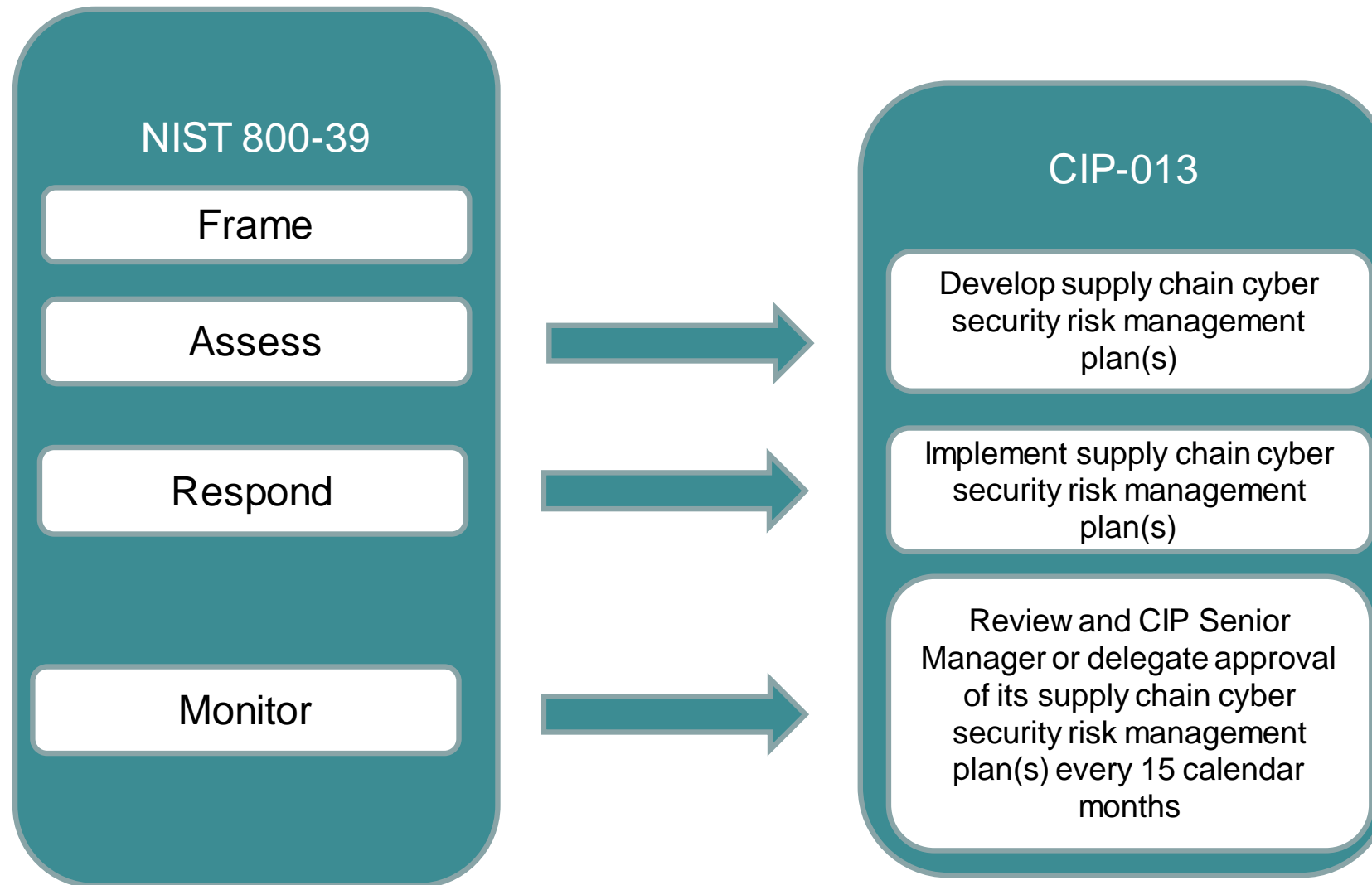
Existing CMMI
material
(Module 4)



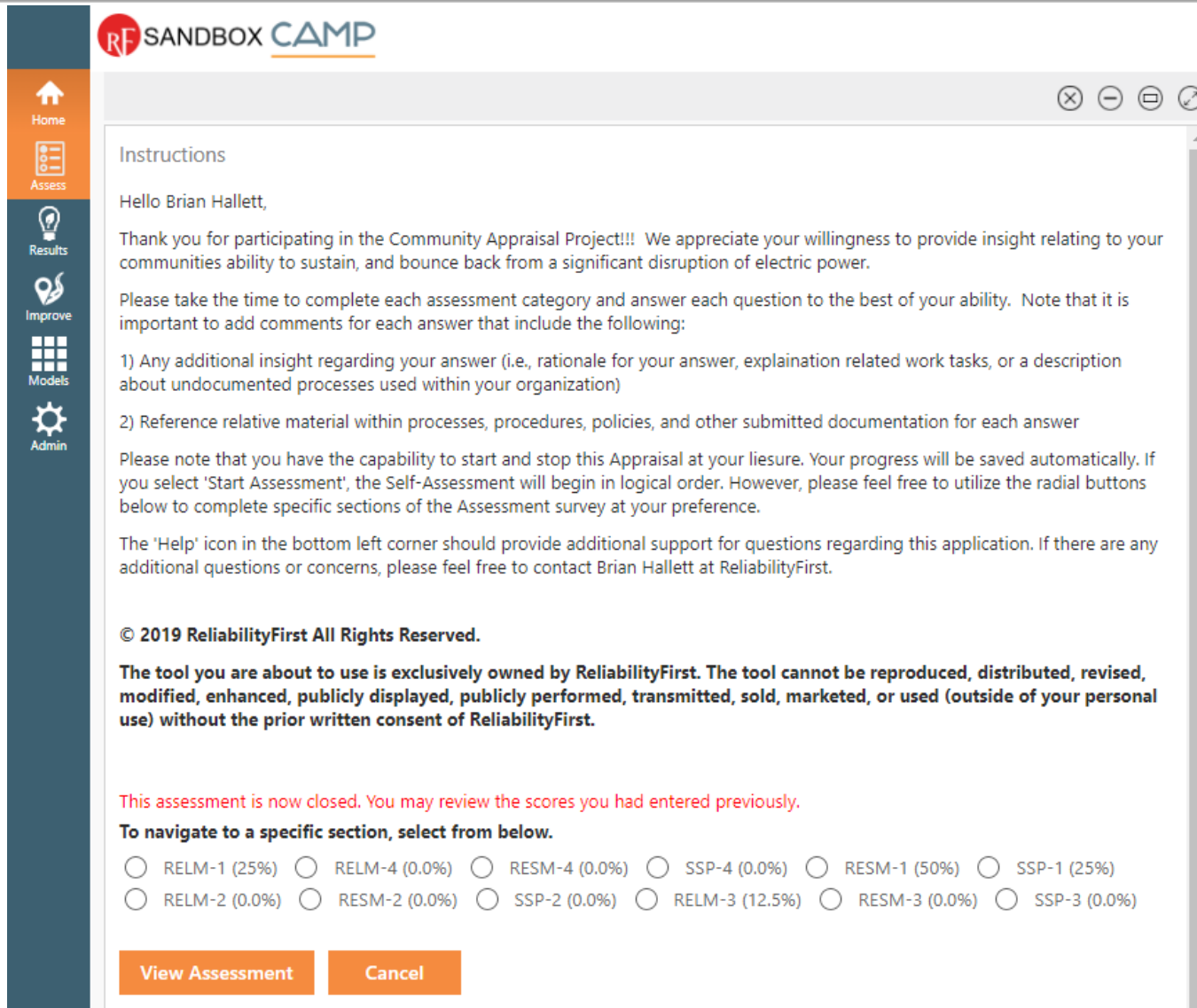
Module #1 Details

- **Largely based on NIST 800-39, NIST 800-161**
- **Applied to different levels of an organization**
 - Tier 1 – Organization Level
 - Tier 2 – Business Process Level
 - Tier 3 – Information System Level
- **Closely aligned with Requirements of CIP-013**

Module #1 Details (cont'd)



CAMP TOOL



RF SANDBOX CAMP

Instructions

Hello Brian Hallett,

Thank you for participating in the Community Appraisal Project!!! We appreciate your willingness to provide insight relating to your communities ability to sustain, and bounce back from a significant disruption of electric power.

Please take the time to complete each assessment category and answer each question to the best of your ability. Note that it is important to add comments for each answer that include the following:

- 1) Any additional insight regarding your answer (i.e., rationale for your answer, explanation related work tasks, or a description about undocumented processes used within your organization)
- 2) Reference relative material within processes, procedures, policies, and other submitted documentation for each answer

Please note that you have the capability to start and stop this Appraisal at your liesure. Your progress will be saved automatically. If you select 'Start Assessment', the Self-Assessment will begin in logical order. However, please feel free to utilize the radial buttons below to complete specific sections of the Assessment survey at your preference.

The 'Help' icon in the bottom left corner should provide additional support for questions regarding this application. If there are any additional questions or concerns, please feel free to contact Brian Hallett at ReliabilityFirst.

© 2019 ReliabilityFirst All Rights Reserved.

The tool you are about to use is exclusively owned by ReliabilityFirst. The tool cannot be reproduced, distributed, revised, modified, enhanced, publicly displayed, publicly performed, transmitted, sold, marketed, or used (outside of your personal use) without the prior written consent of ReliabilityFirst.

This assessment is now closed. You may review the scores you had entered previously.

To navigate to a specific section, select from below.

☐ RELM-1 (25%) ☐ RELM-4 (0.0%) ☐ RESM-4 (0.0%) ☐ SSP-4 (0.0%) ☐ RESM-1 (50%) ☐ SSP-1 (25%)

☐ RELM-2 (0.0%) ☐ RESM-2 (0.0%) ☐ SSP-2 (0.0%) ☐ RELM-3 (12.5%) ☐ RESM-3 (0.0%) ☐ SSP-3 (0.0%)

View Assessment **Cancel**

← Intro + Instructions

← Room to describe sampling:
“who should fill out what tabs”

← “Focus Area” selection



CAMP TOOL (cont'd)

REL-1 - Survey

2020

RELM Objective 1: Perform Relationship Management

Activity 1: Identify and Prioritize relationships that may impact ability to meet objectives
How well does your organization/community identify and prioritize relationships with contractors/partners/businesses that directly impact the community's preparedness for a sustained power outage?

It is important for a community to identify and prioritize its emergency preparedness relationships (also called external interdependencies) – that is, its assets or services that can be affected by the actions or inaction of an outside entity (such as a third-party vendor or consultant). Examples of external interdependencies (or relationships that need to be managed) include outsourcing one of the organization's services, such as electric service, to an outside firm or entity. Another example could include the deployment of a vendor product to manage the law enforcement/emergency dispatch. To identify its critical relationships, a community can examine all of its assets and services to determine 1) a list of its assets that are controlled or affected by outside entities and 2) a list of its services that are directly or indirectly affected by outside entities. After a community or organization identifies its external interdependencies and relationships, it can prioritize them to focus the most resources on those relationships that most directly impact the preparedness and resiliency goals. It is useful for a community or organization to create criteria to follow when prioritizing relationships.

0. Organization does not identify or prioritize external contractors/vendors/businesses that play a role in preparedness or resiliency.

30. The identification and prioritization of external interdependencies is generally performed by either a person in a specific role, or by someone who is well networked, however their methods are not documented.

70. The process of identifying and prioritizing external interdependencies is documented, and executed by someone in a defined role.

90. Identification and prioritizing outreach with critical interdependencies is documented and evaluated annually to ensure the process is meeting the overall goal of the organization/community.

Thermometer: 0 30 70 90 85.00

Activity 2: Assess and Mitigate risks associated with critical relationships
How well does your community identify, assess, and eventually mitigate the risks associated with external partners or vendors?

0. Risk identification, assessment, and mitigation is not performed, or performed inconsistently

30. Activity performed in an ad-hoc manner. Some risks are identified and assessed by available resources, but does not follow a clear criteria and lacks documentation. If risk mitigation is occurring, it is inconsistent.

70. Both existing and emerging risks are identified and assessed according to clear, documented criteria, although the assessment of some types of risks is still predominately qualitative. Risk mitigation is tracked to closure, however, no internal audits or 3rd party reviews are performed.

90. Both existing and emerging risks are identified and assessed with fully quantitative impact analysis. Risk mitigation is tracked to closure, with either internal audits or 3rd party reviews.

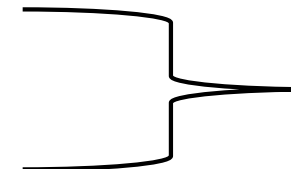
Thermometer: 0 30 70 90



Activity question



Detailed description of activity



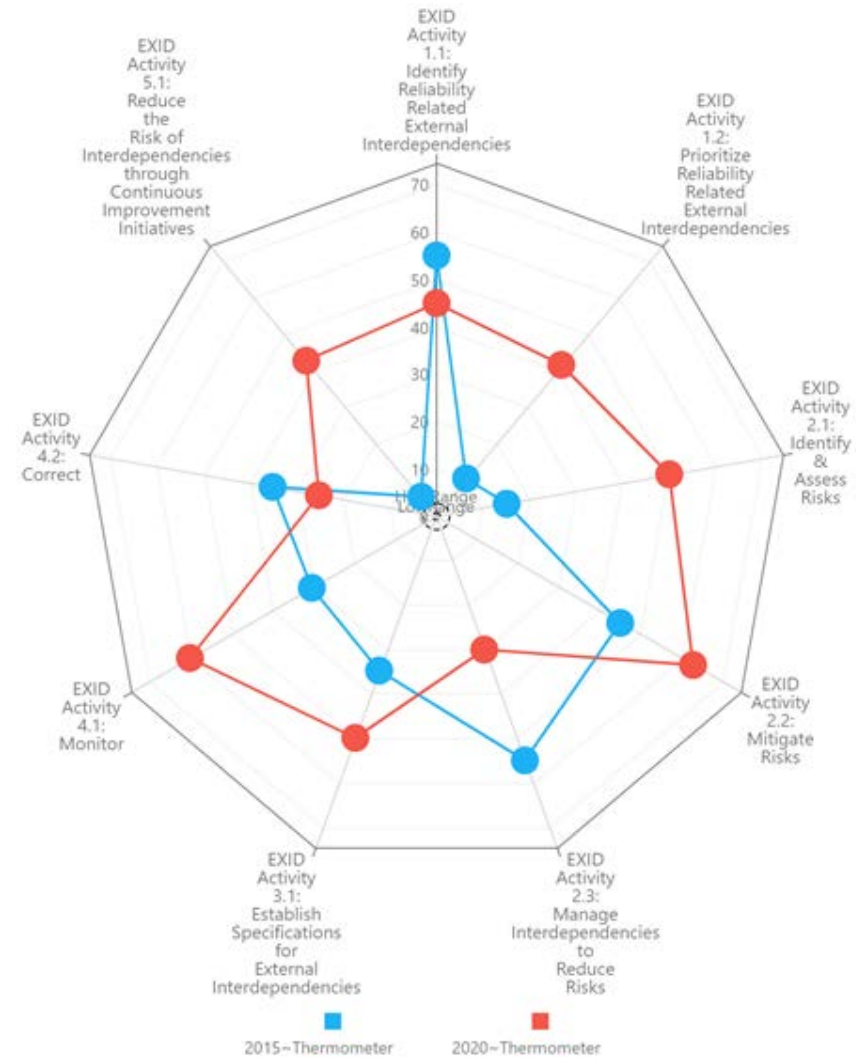
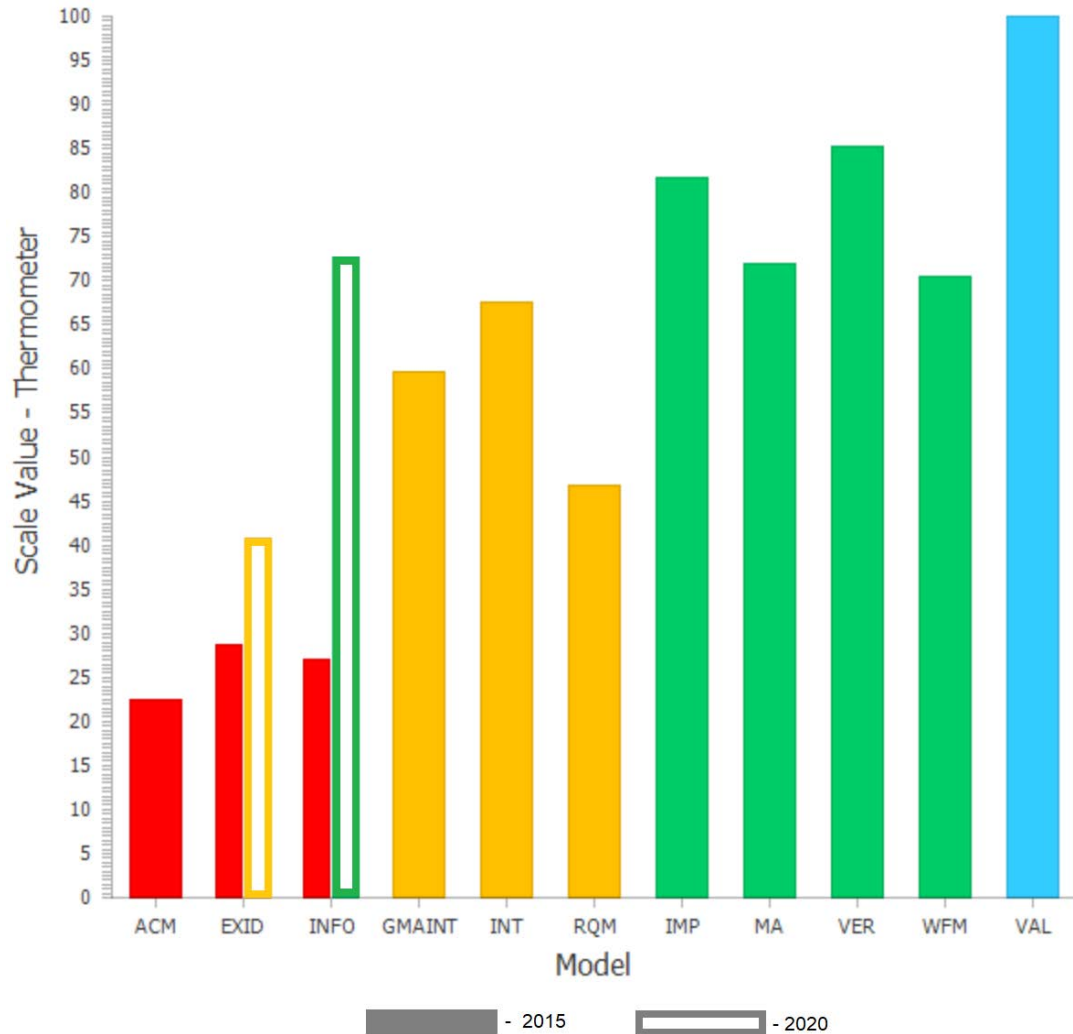
Thermometers for self-scoring guidance



Comment field to add context and supporting information to score



CAMP TOOL (cont'd)




Self-Assessment Tools

- **RF Management Practices — Available Now**
- **Cyber Resiliency Assessment Tool — Available Now**
- **Supply Chain Risk Management — Coming Soon!!!**
- **Community Appraisal for Resiliency Effectiveness — Under Development**



Contact Entity Engagement



 **RELIABILITYFIRST**


ABOUT US

PROGRAM AREAS

KNOWLEDGE CENTER

COMMITTEES




HOME > PROGRAM AREAS > ENTITY ENGAGEMENT

ENTITY ENGAGEMENT

ReliabilityFirst is committed to sharing our expertise, and leveraging the expertise of our entities to enhance our practices surrounding risk identification, mitigation, and prevention.

The Entity Engagement department provides outreach to entities in these areas, in the form of compliance monitoring, enforcement, operational analysis & awareness, registration & certification, engineering & system performance, resilience & risk, risk analysis & mitigation, and standards. If you have questions or are interested in an Entity Engagement activity, please visit our [Contact Us](#) page.

ARTICLES



COMPLIANCE MONITORING

ENFORCEMENT

ENTITY ENGAGEMENT

OPERATIONAL ANALYSIS & AWARENESS


REGISTRATION & CERTIFICATION


ENGINEERING & SYSTEM PERFORMANCE

RESILIENCE & RISK

RISK ANALYSIS & MITIGATION

STANDARDS





VISITS

REGULATORY DISCRETION EVALUATIONS

INTERNAL CONTROLS EVALUATION

SECURITY EVALUATION

STANDARDS EVALUATION

LATEST NEWS

March 24, 2020

Regulatory Discretion for COVID-19 Impacts [READ MORE](#)



Questions & Answers

Forward Together



ReliabilityFirst

WRAP-UP AND WHAT'S NEXT AT RELIABILITYFIRST



Save the Date – Insider Threats Workshop

- **September 30, 2020 8:00 a.m. – 12:00 p.m.**
- **Insider Threat risk management, trends, program management, best practices, lessons learned, and resources**
- **Intended Audience**
 - Physical Security Managers
 - Cyber-Security Managers
 - Vendor / Supply Chain Managers
 - Human Resources (HR) Managers and Administrators
 - Privacy Attorneys
- **Guest Presentations from**
 - CERT National Insider Threat Center
 - FERC & NERC
 - PJM & MISO

