NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Supply Chain Compliance

Joint ERO and CCC Webinar

Ellen Watkins, NERC Compliance Director, Sunflower Electric

August 27, 2021

RELIABILITY | RESILIENCE | SECURITY




NERC Antitrust Compliance Guidelines and Public Announcement Placeholder

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition. It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Questions and Polling via Slido

- Slido will be used for questions and/or polling
- Vote questions up or down so the most voted on questions could be at the top
- Or, use your camera function on your mobile device and follow this QR Code:

SCTF Roster and Contributors

- Ellen Watkins (SCTF Chair & CCC Member), Sunflower Electric Power Corporation
- Jennifer Flandermeyer (CCC Chair), Evergy
- Scott Tomashefsky (CCC Vice Chair), Northern California Power Agency
- Justin MacDonald, Midwest Energy
- Leigh Mulholland, Capital Power
- Martha Henson, Oncor
- Jody Green, ACES Power
- Rene Free, South Carolina Public Service Authority
- Erin Cullum, SPP
- Lonnie Ratliff, NERC
- Brian Allen, NERC
- Tiffany Whaley, NERC
- Kenath Carver, Texas Reliability Entity, Inc.
- Shon Austin, ReliabilityFirst

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Supply Chain Compliance

Opening Comments

Lonnie J Ratliff, Senior Manager Cyber and Physical Security Assurance, NERC

RELIABILITY | RESILIENCE | SECURITY




Agenda

- ERO Q&A
  - Contracts
  - Relationships to other compliance activities
  - Risk Management
  - Vendor Evaluations/ Audit Provisions or Clauses
  - Supply Chain Risk Management Software
  - Utilizing Risk Framework
- FAQ Dynamic Table and Supply Chain Resources on NERC website
- Closing Comments

Slido Questions

1. Attendee representing registered entity, ERO Enterprise staff, other?
2. For registered entities only: Are you utilizing a third-party service to assist with identification and assessment of vendor cyber security risks?

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Q & A

Moderator:
Leigh Mulholland - Chief Compliance Officer, Capital Power
Panelists:
Brian Allen – CIP Assurance Advisor, NERC
Kenath Carver – Manager, CIP Compliance Monitoring, Texas Reliability Entity, Inc.
Shon Austin – Principal Technical Auditor, ReliabilityFirst

RELIABILITY | RESILIENCE | SECURITY




Questions and Answers

Slido Questions

1. Although renegotiating or abrogating of existing contracts (including amendments to master agreements and purchase orders) is not required; have you or will you renegotiate or abrogate contracts to include required supply chain controls?
2. Do you believe there is confusion with the definition of the term vendor?

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Supply Chain FAQ Table

Brian Allen, CIP Assurance Advisor, NERC

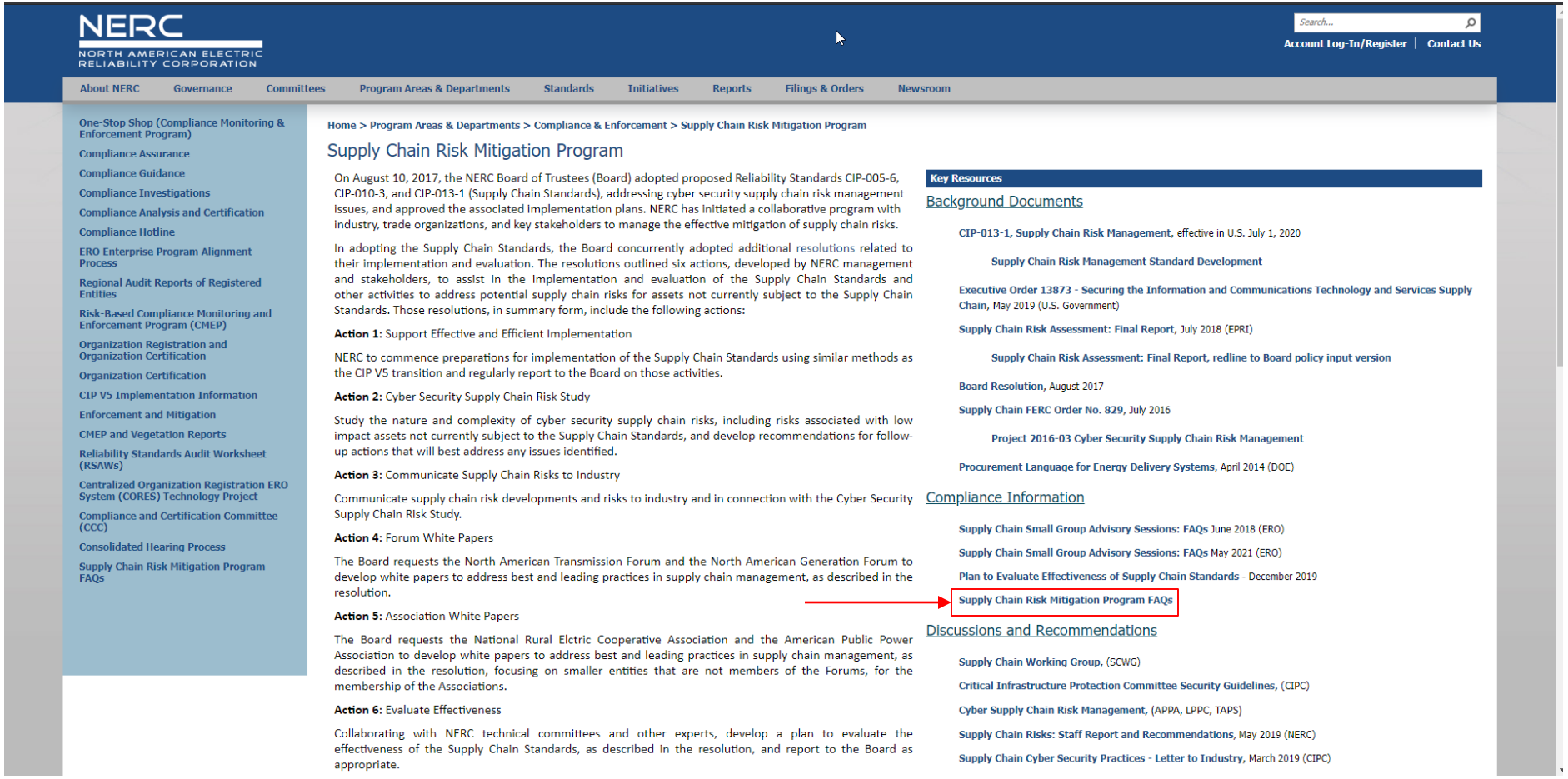
RELIABILITY | RESILIENCE | SECURITY




FAQ Table


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Search...
Account Log-In/Register | Contact Us
About NERC
Governance
Committees
Program Areas & Departments
Standards
Initiatives
Reports
Filings & Orders
Newsroom
Align Project
COVID-19 Activities
Electromagnetic Pulses Task Force
ERO Enterprise Program Alignment Process
Standards Efficiency Review
Supply Chain Risk Mitigation Program
The vision for the Elect
ise, which is comprised of NERC and the six Regional Entities, is a highly reliable and
secure North American
to assure the effective and efficient reduction of risks to the reliability and security
of the grid.
RELIABILITY | RESILIENCE | SECURITY
Headlines & News
Bulk Power System Remains Highly Reliable, NERC Report Highlights Key Challenges
August 17, 2021
Four Interdependent Risks to BPS Reliability Identified in Reliability Risk Priorities Report
August 13, 2021
Board Approves 2022 Budgets, Accepts State of Reliability and RISC Reports
August 12, 2021
EPRI and NERC Collaborate to Enhance Electric Grid Resilience and Reliability as U.S. Transitions to Cleaner Energy
July 21, 2021
Robb, NERC Staff to Participate in 2021 IEEE Power & Energy Society General Meeting
July 21, 2021
ERO Enterprise Deploys Release 2 of Align across Industry
July 19, 2021
Newsroom Archives | Follow on Twitter @NERC_Official | Follow on LinkedIn
Calendar
Standards
Reliability Assessment & Performance Analysis
Board of Trustees
Reliability Risk Management
Compliance
System Operator Certification and Continuing Education
View All Events
Standards
NERC's Standards program ensures the reliability of the bulk power system by developing quality reliability standards in a timely manner that are effective, clear,
Electricity ISAC
malicious virus; Install;
E-ISAC gathers security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity
Reliability Assessment & Performance Analysis
The Reliability Assessment and Performance Analysis program assesses, measures and investigates historic trends and future projections to improve bulk power

FAQ Table



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Search...
Account Log-In/Register | Contact Us

About NERC | Governance | Committees | Program Areas & Departments | Standards | Initiatives | Reports | Filings & Orders | Newsroom

- One-Stop Shop (Compliance Monitoring & Enforcement Program)
- Compliance Assurance
- Compliance Guidance
- Compliance Investigations
- Compliance Analysis and Certification
- Compliance Hotline
- ERO Enterprise Program Alignment Process
- Regional Audit Reports of Registered Entities
- Risk-Based Compliance Monitoring and Enforcement Program (CMEP)
- Organization Registration and Organization Certification
- Organization Certification
- CIP V5 Implementation Information
- Enforcement and Mitigation
- CMEP and Vegetation Reports
- Reliability Standards Audit Worksheet (RSAWs)
- Centralized Organization Registration ERO System (CORES) Technology Project
- Compliance and Certification Committee (CCC)
- Consolidated Hearing Process
- Supply Chain Risk Mitigation Program FAQs

Home > Program Areas & Departments > Compliance & Enforcement > Supply Chain Risk Mitigation Program

Supply Chain Risk Mitigation Program

On August 10, 2017, the NERC Board of Trustees (Board) adopted proposed Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 (Supply Chain Standards), addressing cyber security supply chain risk management issues, and approved the associated implementation plans. NERC has initiated a collaborative program with industry, trade organizations, and key stakeholders to manage the effective mitigation of supply chain risks.

In adopting the Supply Chain Standards, the Board concurrently adopted additional resolutions related to their implementation and evaluation. The resolutions outlined six actions, developed by NERC management and stakeholders, to assist in the implementation and evaluation of the Supply Chain Standards and other activities to address potential supply chain risks for assets not currently subject to the Supply Chain Standards. Those resolutions, in summary form, include the following actions:

Action 1: Support Effective and Efficient Implementation

NERC to commence preparations for implementation of the Supply Chain Standards using similar methods as the CIP V5 transition and regularly report to the Board on those activities.

Action 2: Cyber Security Supply Chain Risk Study

Study the nature and complexity of cyber security supply chain risks, including risks associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address any issues identified.

Action 3: Communicate Supply Chain Risks to Industry

Communicate supply chain risk developments and risks to industry and in connection with the Cyber Security Supply Chain Risk Study.

Action 4: Forum White Papers

The Board requests the North American Transmission Forum and the North American Generation Forum to develop white papers to address best and leading practices in supply chain management, as described in the resolution.

Action 5: Association White Papers

The Board requests the National Rural Elctric Cooperative Association and the American Public Power Association to develop white papers to address best and leading practices in supply chain management, as described in the resolution, focusing on smaller entities that are not members of the Forums, for the membership of the Associations.

Action 6: Evaluate Effectiveness

Collaborating with NERC technical committees and other experts, develop a plan to evaluate the effectiveness of the Supply Chain Standards, as described in the resolution, and report to the Board as appropriate.

Key Resources

Background Documents

- **CIP-013-1, Supply Chain Risk Management**, effective in U.S. July 1, 2020
- **Supply Chain Risk Management Standard Development**
- **Executive Order 13873 - Securing the Information and Communications Technology and Services Supply Chain**, May 2019 (U.S. Government)
- **Supply Chain Risk Assessment: Final Report**, July 2018 (EPRI)
- **Supply Chain Risk Assessment: Final Report, redline to Board policy input version**
- **Board Resolution**, August 2017
- **Supply Chain FERC Order No. 829**, July 2016
- **Project 2016-03 Cyber Security Supply Chain Risk Management**
- **Procurement Language for Energy Delivery Systems**, April 2014 (DOE)

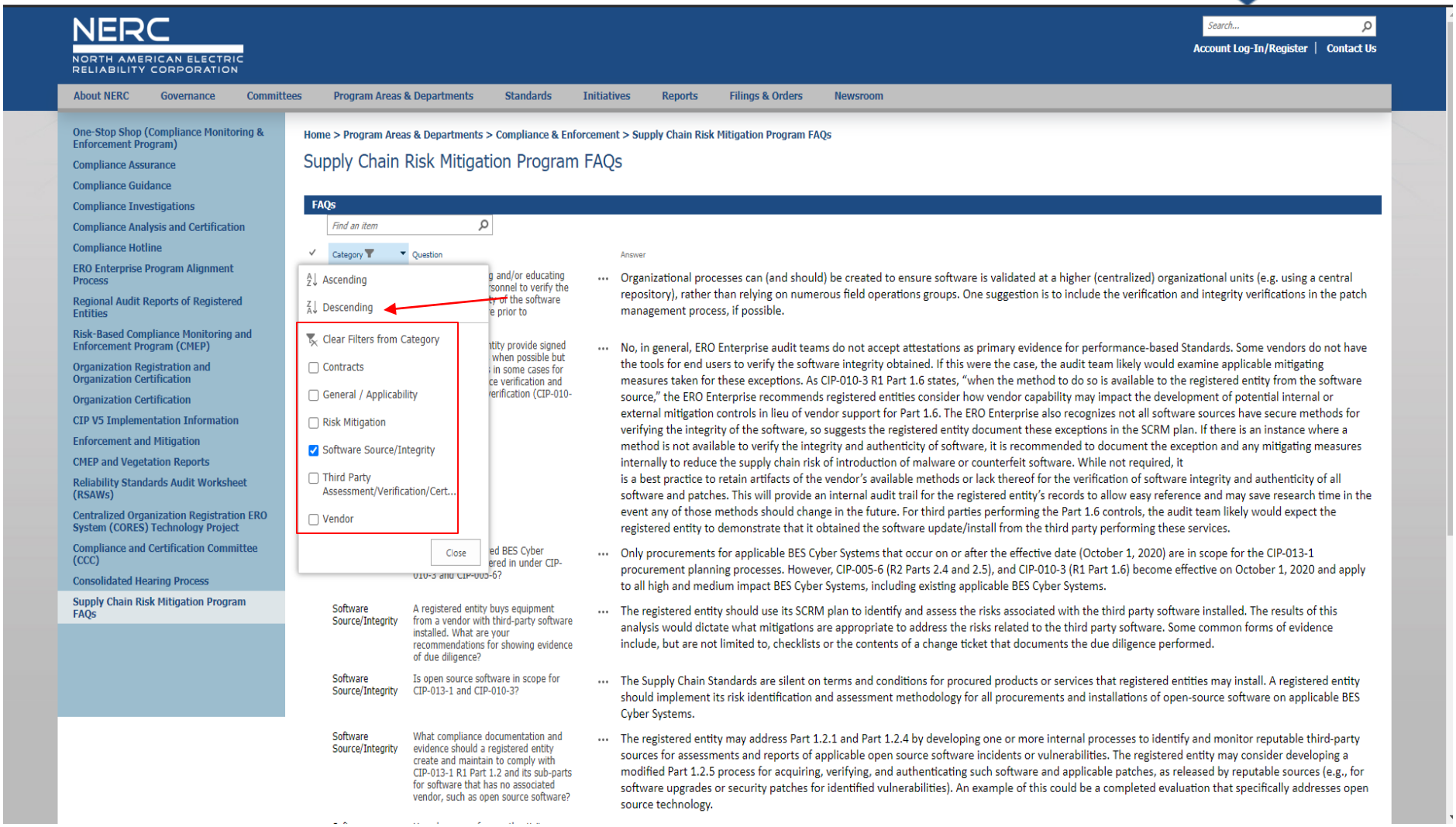
Compliance Information

- **Supply Chain Small Group Advisory Sessions: FAQs** June 2018 (ERO)
- **Supply Chain Small Group Advisory Sessions: FAQs** May 2021 (ERO)
- **Plan to Evaluate Effectiveness of Supply Chain Standards** - December 2019
- **Supply Chain Risk Mitigation Program FAQs**

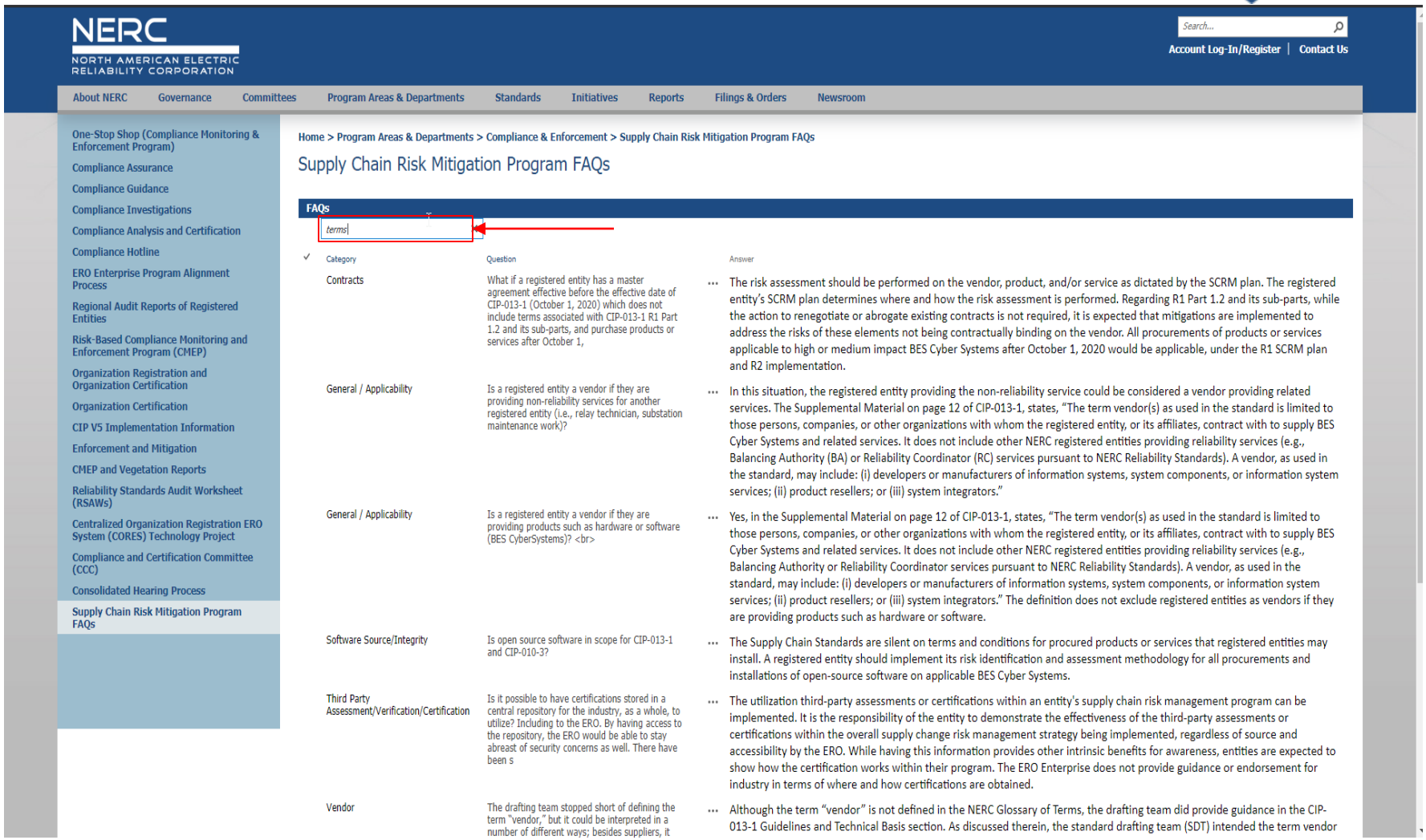
Discussions and Recommendations

- **Supply Chain Working Group**, (SCWG)
- **Critical Infrastructure Protection Committee Security Guidelines**, (CIPC)
- **Cyber Supply Chain Risk Management**, (APPA, LPPC, TAPS)
- **Supply Chain Risks: Staff Report and Recommendations**, May 2019 (NERC)
- **Supply Chain Cyber Security Practices - Letter to Industry**, March 2019 (CIPC)

FAQ Table


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Search...
Account Log-In/Register | Contact Us
About NERC
Governance
Committees
Program Areas & Departments
Standards
Initiatives
Reports
Filings & Orders
Newsroom
One-Stop Shop (Compliance Monitoring & Enforcement Program)
Compliance Assurance
Compliance Guidance
Compliance Investigations
Compliance Analysis and Certification
Compliance Hotline
ERO Enterprise Program Alignment Process
Regional Audit Reports of Registered Entities
Risk-Based Compliance Monitoring and Enforcement Program (CMEP)
Organization Registration and Organization Certification
Organization Certification
CIP V5 Implementation Information
Enforcement and Mitigation
CMEP and Vegetation Reports
Reliability Standards Audit Worksheet (RSAWs)
Centralized Organization Registration ERO System (CORES) Technology Project
Compliance and Certification Committee (CCC)
Consolidated Hearing Process
Supply Chain Risk Mitigation Program FAQs
Home > Program Areas & Departments > Compliance & Enforcement > Supply Chain Risk Mitigation Program FAQs
Supply Chain Risk Mitigation Program FAQs
FAQs
Find an item
Category
Question
Answer
Ascending
Descending
Clear Filters from Category
Contracts
General / Applicability
Risk Mitigation
Software Source/Integrity
Third Party Assessment/Verification/Cert...
Vendor
Close
Organizational processes can (and should) be created to ensure software is validated at a higher (centralized) organizational units (e.g. using a central repository), rather than relying on numerous field operations groups. One suggestion is to include the verification and integrity verifications in the patch management process, if possible.
No, in general, ERO Enterprise audit teams do not accept attestations as primary evidence for performance-based Standards. Some vendors do not have the tools for end users to verify the software integrity obtained. If this were the case, the audit team likely would examine applicable mitigating measures taken for these exceptions. As CIP-010-3 R1 Part 1.6 states, "when the method to do so is available to the registered entity from the software source," the ERO Enterprise recommends registered entities consider how vendor capability may impact the development of potential internal or external mitigation controls in lieu of vendor support for Part 1.6. The ERO Enterprise also recognizes not all software sources have secure methods for verifying the integrity of the software, so suggests the registered entity document these exceptions in the SCRM plan. If there is an instance where a method is not available to verify the integrity and authenticity of software, it is recommended to document the exception and any mitigating measures internally to reduce the supply chain risk of introduction of malware or counterfeit software. While not required, it is a best practice to retain artifacts of the vendor's available methods or lack thereof for the verification of software integrity and authenticity of all software and patches. This will provide an internal audit trail for the registered entity's records to allow easy reference and may save research time in the event any of those methods should change in the future. For third parties performing the Part 1.6 controls, the audit team likely would expect the registered entity to demonstrate that it obtained the software update/install from the third party performing these services.
Only procurements for applicable BES Cyber Systems that occur on or after the effective date (October 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 October 1, 2020 and apply to all high and medium impact BES Cyber Systems, including existing applicable BES Cyber Systems.
Software Source/Integrity
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.
Software Source/Integrity
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.
Software Source/Integrity
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.

FAQ Table



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Search...
Account Log-In/Register | Contact Us

About NERC | Governance | Committees | Program Areas & Departments | Standards | Initiatives | Reports | Filings & Orders | Newsroom

- One-Stop Shop (Compliance Monitoring & Enforcement Program)
- Compliance Assurance
- Compliance Guidance
- Compliance Investigations
- Compliance Analysis and Certification
- Compliance Hotline
- ERO Enterprise Program Alignment Process
- Regional Audit Reports of Registered Entities
- Risk-Based Compliance Monitoring and Enforcement Program (CMEP)
- Organization Registration and Organization Certification
- Organization Certification
- CIP V5 Implementation Information
- Enforcement and Mitigation
- CMEP and Vegetation Reports
- Reliability Standards Audit Worksheet (RSAWs)
- Centralized Organization Registration ERO System (CORES) Technology Project
- Compliance and Certification Committee (CCC)
- Consolidated Hearing Process
- Supply Chain Risk Mitigation Program FAQs

Home > Program Areas & Departments > Compliance & Enforcement > Supply Chain Risk Mitigation Program FAQs

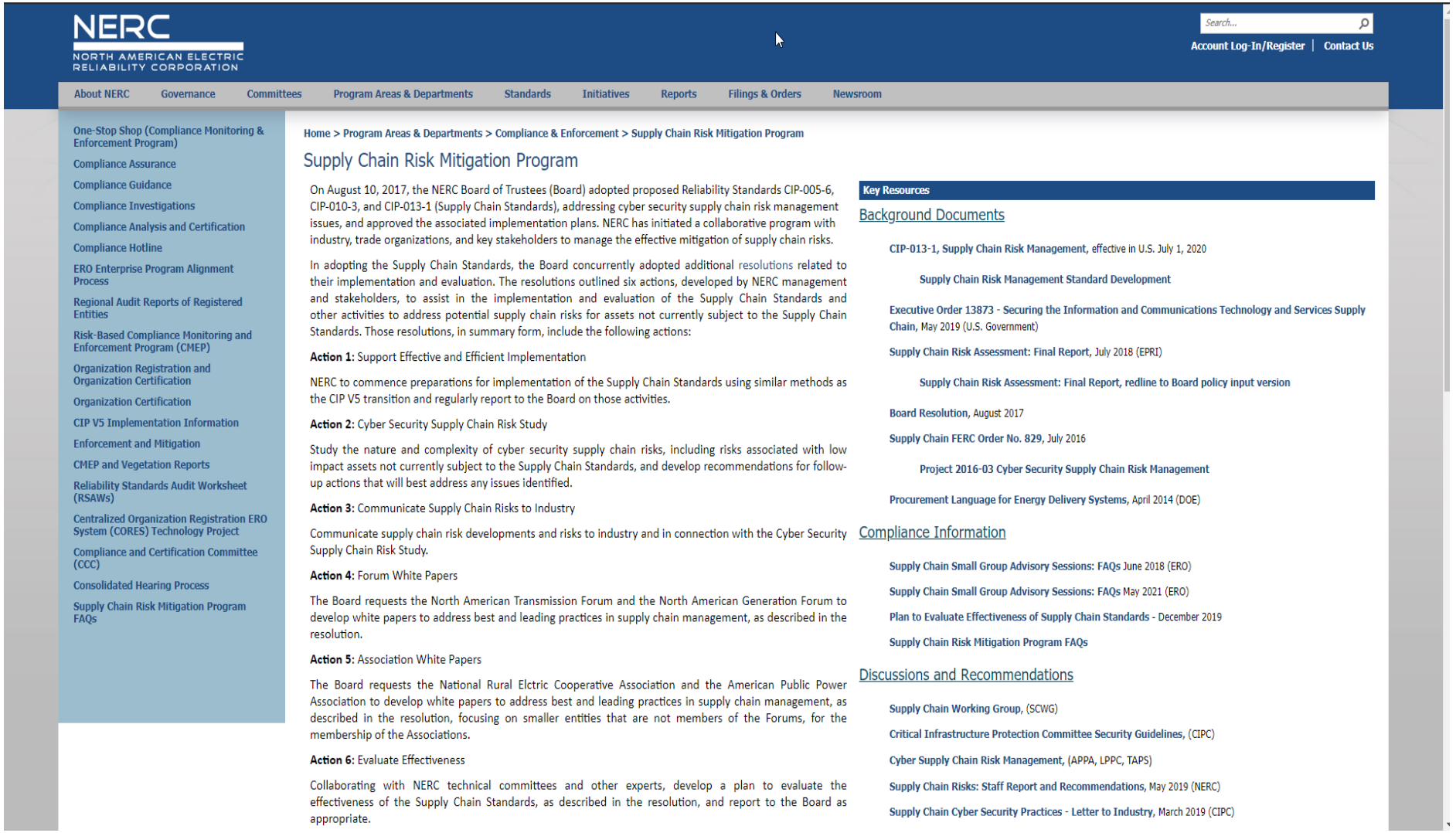
Supply Chain Risk Mitigation Program FAQs

FAQs

terms

Category	Question	Answer
Contracts	What if a registered entity has a master agreement effective before the effective date of CIP-013-1 (October 1, 2020) which does not include terms associated with CIP-013-1 R1 Part 1.2 and its sub-parts, and purchase products or services after October 1,	... 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 October 1, 2020 would be applicable, under the R1 SCRM plan and R2 implementation.
General / Applicability	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."
General / Applicability	Is a registered entity a vendor if they are providing products such as hardware or software (BES CyberSystems)? 	... Yes, in 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 or Reliability Coordinator 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." The definition does not exclude registered entities as vendors if they are providing products such as hardware or software.
Software Source/Integrity	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.
Third Party Assessment/Verification/Certification	Is it possible to have certifications stored in a central repository for the industry, as a whole, to utilize? Including to the ERO. By having access to the repository, the ERO would be able to stay abreast of security concerns as well. There have been s	... The utilization third-party assessments or certifications within an entity's supply chain risk management program can be implemented. It is the responsibility of the entity to demonstrate the effectiveness of the third-party assessments or certifications within the overall supply change risk management strategy being implemented, regardless of source and accessibility by the ERO. While having this information provides other intrinsic benefits for awareness, entities are expected to show how the certification works within their program. The ERO Enterprise does not provide guidance or endorsement for industry in terms of where and how certifications are obtained.
Vendor	The drafting team stopped short of defining the term "vendor," but it could be interpreted in a number of different ways; besides suppliers, it	... Although the term "vendor" is not defined in the NERC Glossary of Terms, the drafting team did provide guidance in the CIP-013-1 Guidelines and Technical Basis section. As discussed therein, the standard drafting team (SDT) intended the term vendor

FAQ Table



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Search...
Account Log-In/Register | Contact Us

About NERC | Governance | Committees | Program Areas & Departments | Standards | Initiatives | Reports | Filings & Orders | Newsroom

- One-Stop Shop (Compliance Monitoring & Enforcement Program)
- Compliance Assurance
- Compliance Guidance
- Compliance Investigations
- Compliance Analysis and Certification
- Compliance Hotline
- ERO Enterprise Program Alignment Process
- Regional Audit Reports of Registered Entities
- Risk-Based Compliance Monitoring and Enforcement Program (CMEP)
- Organization Registration and Organization Certification
- Organization Certification
- CIP V5 Implementation Information
- Enforcement and Mitigation
- CMEP and Vegetation Reports
- Reliability Standards Audit Worksheet (RSAWs)
- Centralized Organization Registration ERO System (CORES) Technology Project
- Compliance and Certification Committee (CCC)
- Consolidated Hearing Process
- Supply Chain Risk Mitigation Program FAQs

Home > Program Areas & Departments > Compliance & Enforcement > Supply Chain Risk Mitigation Program

Supply Chain Risk Mitigation Program

On August 10, 2017, the NERC Board of Trustees (Board) adopted proposed Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 (Supply Chain Standards), addressing cyber security supply chain risk management issues, and approved the associated implementation plans. NERC has initiated a collaborative program with industry, trade organizations, and key stakeholders to manage the effective mitigation of supply chain risks.

In adopting the Supply Chain Standards, the Board concurrently adopted additional resolutions related to their implementation and evaluation. The resolutions outlined six actions, developed by NERC management and stakeholders, to assist in the implementation and evaluation of the Supply Chain Standards and other activities to address potential supply chain risks for assets not currently subject to the Supply Chain Standards. Those resolutions, in summary form, include the following actions:

Action 1: Support Effective and Efficient Implementation

NERC to commence preparations for implementation of the Supply Chain Standards using similar methods as the CIP V5 transition and regularly report to the Board on those activities.

Action 2: Cyber Security Supply Chain Risk Study

Study the nature and complexity of cyber security supply chain risks, including risks associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address any issues identified.

Action 3: Communicate Supply Chain Risks to Industry

Communicate supply chain risk developments and risks to industry and in connection with the Cyber Security Supply Chain Risk Study.

Action 4: Forum White Papers

The Board requests the North American Transmission Forum and the North American Generation Forum to develop white papers to address best and leading practices in supply chain management, as described in the resolution.

Action 5: Association White Papers

The Board requests the National Rural Elctric Cooperative Association and the American Public Power Association to develop white papers to address best and leading practices in supply chain management, as described in the resolution, focusing on smaller entities that are not members of the Forums, for the membership of the Associations.

Action 6: Evaluate Effectiveness

Collaborating with NERC technical committees and other experts, develop a plan to evaluate the effectiveness of the Supply Chain Standards, as described in the resolution, and report to the Board as appropriate.

Key Resources

Background Documents

CIP-013-1, Supply Chain Risk Management, effective in U.S. July 1, 2020

Supply Chain Risk Management Standard Development

Executive Order 13873 - Securing the Information and Communications Technology and Services Supply Chain, May 2019 (U.S. Government)

Supply Chain Risk Assessment: Final Report, July 2018 (EPRI)

Supply Chain Risk Assessment: Final Report, redline to Board policy input version

Board Resolution, August 2017

Supply Chain FERC Order No. 829, July 2016

Project 2016-03 Cyber Security Supply Chain Risk Management

Procurement Language for Energy Delivery Systems, April 2014 (DOE)

Compliance Information

Supply Chain Small Group Advisory Sessions: FAQs June 2018 (ERO)

Supply Chain Small Group Advisory Sessions: FAQs May 2021 (ERO)

Plan to Evaluate Effectiveness of Supply Chain Standards - December 2019

Supply Chain Risk Mitigation Program FAQs

Discussions and Recommendations

Supply Chain Working Group, (SCWG)

Critical Infrastructure Protection Committee Security Guidelines, (CIPC)

Cyber Supply Chain Risk Management, (APPA, LPPC, TAPS)

Supply Chain Risks: Staff Report and Recommendations, May 2019 (NERC)

Supply Chain Cyber Security Practices - Letter to Industry, March 2019 (CIPC)

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Supply Chain Compliance

Closing Comments

Jennifer Flandermeyer Director, Federal Regulatory Affairs, Evergy

RELIABILITY | RESILIENCE | SECURITY




Closing Comments

- CCC SCTF continued work through 2021 on outstanding Supply Chain Q&A
  - Created an inbox to capture questions
    - Processed collaboratively with ERO Enterprise and CCC SCTF members
    - Can submit anonymously through CCC Members
- Regional Entities as key Point of Contact for questions
- FAQs
- Other resources - NERC SCWG, Guidelines, Webinars, NATF Industry Organizations, EEI Contract language, Newsletters, and Small Group Advisory Sessions

  (Note: not exhaustive list)

Supply Chain Inbox

sctf@nerc.com

Questions and Answers

Appendices

Supply Chain Announcement

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Announcement

Supply Chain Inbox

Click here for: Supply Chain Inbox

The NERC Compliance and Certification Committee's Supply Chain Task Force (SCTF) has established an email address for submission of industry's questions or requests regarding Supply Chain compliance. In addition, industry may request additional clarification in this very dynamic area of the business. While the email address will be temporary, the CCC SCTF will ensure collaboration with the ERO Enterprise and NERC SCWG to provide clarification when possible and gather additional inputs for the Frequently Asked Questions. If you have a question, please submit it via email to **Supply Chain Inbox**.

For more information or assistance, please contact **Tiffany Whaley** (via email) or at 404-290-2388.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

RELIABILITY | RESILIENCE | SECURITY

Bios

Jennifer Flandermeyer
Director, Federal Affairs, Evergy

As Director, Federal Affairs, Ms. Flandermeyer is focused on federal regulatory activities related to reliability, resilience and security. While the regulatory actions are primarily with FERC and NERC, because the advocacy role is dedicated to reliability, security and resilience, the role continues to broaden as Evergy engages other departments and agencies of the federal government tasked with critical infrastructure protection.

In 1999, she joined Evergy bringing with her several years of finance and accounting experience coupled with knowledge of the energy industry. Since joining the company, she has held positions in Internal Audit and Strategic Business Planning and Financial Operations in Delivery (T&D) Operations. In 2009, she accepted the opportunity to lead the company's FERC and NERC compliance team responsible for the company-wide regulatory compliance function establishing a new program for the company. The program was eventually expanded to include additional regulatory bodies and functions. In 2015, she was promoted to her current role to focus on strategy and policy advocacy for federal affairs.

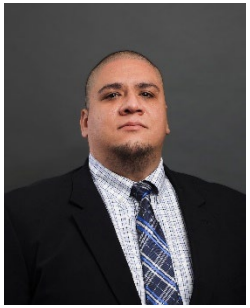
Ms. Flandermeyer holds a Bachelor of Science degree in Accountancy from William Jewell College, a master's degree in Business Administration from Rockhurst University and certifications in Risk Management as well as Compliance and Ethics. Ms. Flandermeyer serves as a Director for the Midwest Reliability Organization. She serves in several roles on NERC Committees, including the Chair of the NERC Compliance and Certification Committee and one of the two members of the NERC Member Representatives Committee representing Investor-Owned Utilities. Ms. Flandermeyer is active in the industry serving in leadership roles for several organizations including Southwest Power Pool's Reliability Compliance Advisory Group and the North American Transmission Forum Risk, Controls and Compliance Practices Group. Ms. Flandermeyer previously served as the President for Rose Brooks Center's Board of Directors, an organization dedicated to breaking the cycle of domestic violence, in addition to many other community activities.

Bios

Leigh Mulholland
Chief Compliance Officer, Capital Power

Leigh Mulholland joined Capital Power in 2007 and was appointed Chief Compliance Officer in September 2015, where she oversees and manages the compliance function within Capital Power, including developing the annual compliance program and maintaining current knowledge of regulations and laws applicable to the electricity sector in the jurisdictions we operate. Prior to her current position, Leigh was Vice President, Corporate Strategy & Planning and was responsible for Capital Power's Corporate Long-Term Plan, the Annual Business Planning process, the Alberta Coal Commercial Services & Real-Time Operations (Settlements) Teams as well as some Business Development activity. Leigh also served as Senior Manager, Valuations, where she was responsible for leading the financial analytics on acquisition, divestiture and business development activity. Leigh is a Certified Compliance & Ethics Professional (CCEP), a Chartered Global Management Accountant (CGMA) and a Certified Public Accountant (CPA-Illinois). She is a member of NERC's Compliance and Certification Committee and currently serves as Vice-Chair of the ERO Monitoring Subcommittee.

Bios



Kenath Carver
Manager, CIP Compliance Monitoring (Texas RE)

Kenath Carver is the Manager of CIP Compliance Monitoring at Texas RE and has been with the company since 2012. He has over 15 years of Information Technology experience and prior to joining Texas RE, Kenath worked as an IT Business Solutions Analyst and Senior IT Security Administrator. Mr. Carver holds numerous industry-leading certifications, including CompTIA Network+, Security +, CySA+; GIAC CIP, and ISC^2 SSCP.

Bios

Shon Austin
Principal Technical Auditor CIP Monitoring

Mr. Austin currently works in the CIP department and is responsible for monitoring, measuring and reporting the compliance to ERO Reliability Standards for the Registered Entities in the ReliabilityFirst footprint. These functions are accomplished through database management, real-time monitoring techniques, and on-site visits. He has an extensive knowledge of industrial and technical cyber security information.

Mr. Austin has 21+ years progressive experience in the Electrical Energy Industry, with 18+ years professional experience in Information Security, and 14+ years specialized experience in NERC/FERC Compliance & Enforcement.
Previously, Mr. Austin served as a Lead Compliance Specialist Southwest Power Pool (SPP) Regional Entity (RE) and a senior level Application Developer/System Engineer for the SPP Regional Transmission Organization.

Mr. Austin previously served as the:
- President of the Central Arkansas Chapter of ISACA
- Energy Sector Chief for the Arkansas InfraGard Members Alliance

Mr. Austin served in the United States Army Reserves at the rank of E5 (Sergeant) as a 91B20 (Medical Specialist).

Mr. Austin has a Masters of Business Administration and a Bachelor of Science degree in Computer Science and a minor in Mathematics. He is a certified NERC Lead Auditor and has completed NERC CIP training. He represented the Regional Entities in the development of the NERC CIP training pilot and has obtained the following certifications: Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information System Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), Physical Security Professional (PSP), Microsoft Certified Solution Developer (MCSD.NET), Microsoft Certified Application Developer (MCAD),Microsoft Certified Database Administrator (MCDBA), Microsoft Certified Professionals (MCP), Microsoft Certified Systems Administrator (MCSA), and Oracle Certified Associate (OCA)

Lonnie J Ratliff
Senior Manager, Cyber and Physical Security Assurance, NERC

Summary Statement: Lonnie is a Senior Manager, Cyber and Physical Security Assurance in the NERC Compliance Assurance group. In this position, Lonnie is responsible for providing oversight, guidance, and coordination in managing programs and processes to monitor, review, and evaluate program effectiveness of Electric Reliability Organization (ERO) Enterprise implementation of risk-based compliance monitoring and adherence to the NERC Rules of Procedure, Compliance Monitoring and Enforcement Program, and approved delegation agreements.

Detail Statement: In July 2017, Lonnie joined NERC's Grid Assurance group. Prior to joining NERC, Lonnie was the Manager, Entity Assessment and Mitigation (EAM) at SERC Reliability Corporation. Lonnie led a team that was responsible for assessing non-compliance scope and risk posed to the Bulk Power System. In addition, his team was responsible for conducting registered entity Inherent Risk Assessments and ensuring appropriate mitigation activities were applied for each non-compliance.

As the Manager, EAM, Lonnie was also responsible for developing, implementing, and maintaining the SERC regional Self-Logging Program.
Lonnie is a seasoned IT professional with over twelve years of Critical Infrastructure Protection (CIP) experience. He specializes in operating system and network security, penetration testing, and vulnerability risk assessments. He is proficient with a wide variety of system and network security solutions, including routers, switches, system and network firewalls, server and network intrusion detection systems.

Prior to SERC Reliability Corporation, Lonnie served as a consultant for Network and Security Technologies, Inc., (N&ST) for nine years performing numerous penetration tests and technical security assessments for major clients in the financial, education and electric power sectors. In addition, Lonnie performed high-profile projects related to compliance with the NERC CIP Cyber Security Standards for several large Bulk Electric System participants, as well as the U.S. Department of Energy.

Lonnie is a Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), and has held certifications from Sun, Cisco, and Netscreen.

Bios

Brian Allen
CIP Assurance Advisor , NERC

Summary Statement: Brian serves as a CIP Assurance Advisor in the NERC Grid Assurance group. In this position, Brian works with the Assurance Team to provide oversight, guidance, and coordination in managing programs and processes to monitor, review, and evaluate program effectiveness of the Electric Reliability Organization (ERO) Enterprise implementation of risk-based compliance monitoring and adherence to the NERC Rules of Procedure, Compliance Monitoring and Enforcement Program, and approved delegation agreements.

Detail Statement: Brian joined the NERC CIP Assurance team in January 2019. Prior to NERC, Brian served as a Cyber Security Specialist at Georgia Systems Operation Corporation. In this role, Brian worked within Security Operations focusing on governance, risk, and compliance of the CIP Program.

1 Legal Notice: NERC staff biographies are for use by NERC and Regional Entities in implementing the NERC Rules of Procedure, including the NERC Compliance Monitoring and Enforcement Program set forth in Appendix 4C (referred to herein collectively as "NERC Rules of Procedure"). Regional Entities shall provide applicable NERC staff biographies to Registered Entities as required by the NERC Rules of Procedure. The NERC staff biographies are the property of NERC and may not be modified by anyone other than NERC, nor may they be used for

Bios

Ellen Watkins
NERC Compliance Director, Sunflower Electric Power Corporation

Ms. Watkins joined Sunflower in 2006 and transitioned from Human Resources into NERC Compliance in 2013. In 2016, she was promoted to her current role as the NERC Compliance Director.

Ms. Watkins earned a bachelor's degree in Organizational Management and Development and a master's degree in Business Administration, both from Friends University. She also earned a Graduate Certificate in Human Resource Management from Fort Hays State University.

As a member of the NERC Compliance and Certification Committee (CCC), Ms. Watkins also serves on the CCC ERO Monitoring Subcommittee (EROMS) as well as the Chair for the CCC Supply Chain Task Force (SCTF). Additionally, Ms. Watkins is active in industry and serves several roles for various organizations including the Southwest Power Pool's (SPP) Reliability Compliance Advisory Group (RCAG), North American Transmission Forum (NATF) Risk, Controls, and Compliance (RCC) Core Team, numerous NATF RCC projects teams, as well as serving as the lead for the RCC Emerging Issues Project Team.