



*Community Confidentiality Candor Commitment*

# Optimizing Supplier-Purchaser Interaction for Supply Chain Risk Management

**Ken Keels**  
Director, Initiatives

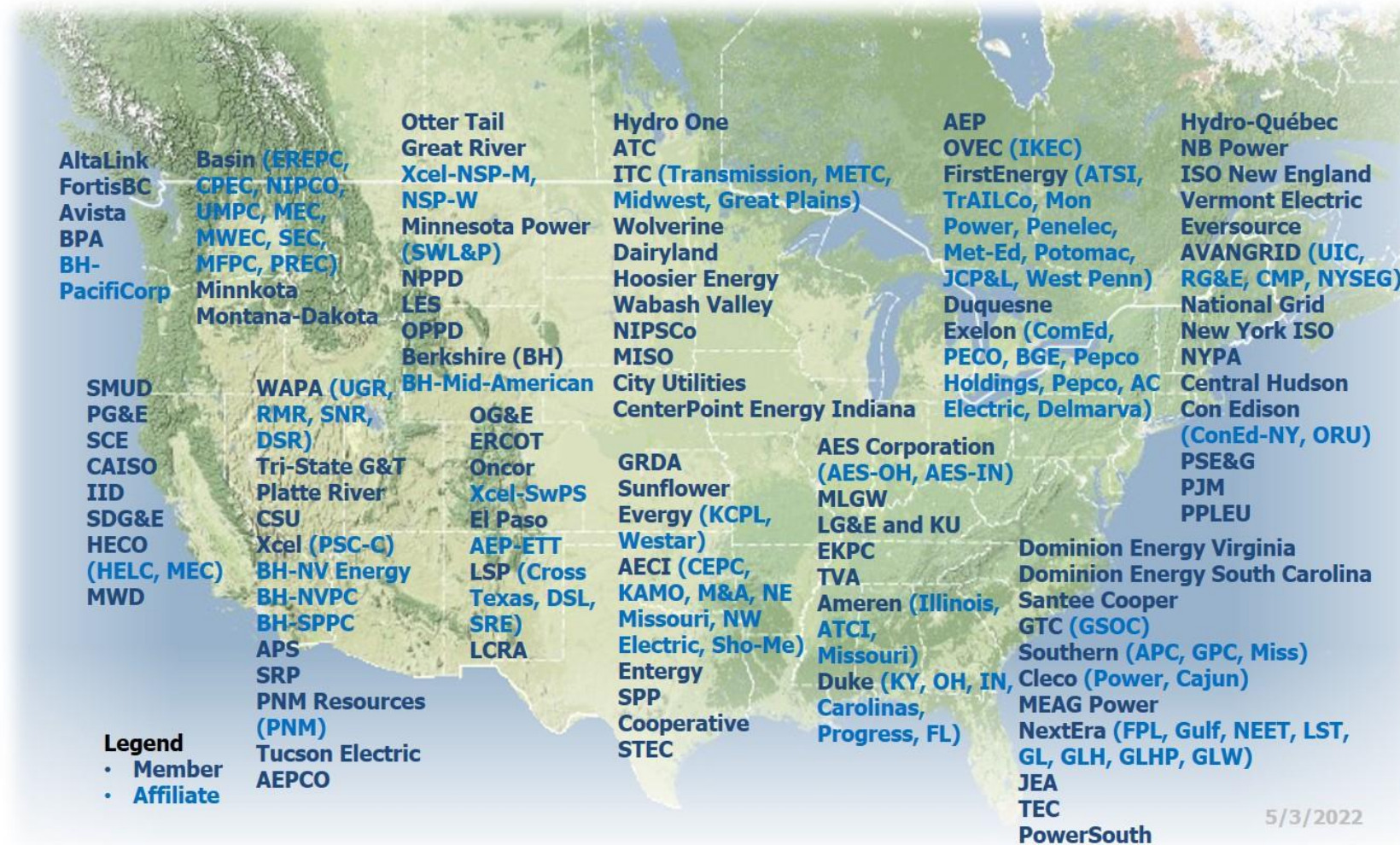
**David James Earley**  
Program Manager,  
Cybersecurity & Supply  
Chain

## **Open Distribution for Supply Chain Materials**

Copyright © 2022 North American Transmission Forum (“NATF”). All rights reserved.

The NATF permits the use of the content contained herein (“Content”), without modification; however, any such use must include this notice and reference the associated NATF document name & version number. The Content is provided on an “as is” basis. The NATF makes no and hereby disclaims all representations or warranties (express or implied) relating to the Content. The NATF shall not be liable for any damages arising directly or indirectly from the Content or use thereof. By using the Content, you hereby agree to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use.

# NATF Overview



**94 members**  
**89 affiliates**

**Member Types**

- IOUs
- Federal/Provincial
- Cooperatives
- State/Municipal
- ISOs/RTOs

**Coverage (US/Canada)**

~85% miles 100 kV+  
~90% net peak demand

# Objectives of NATF Supply Chain Initiatives

## Security

Identify and address security risks introduced via supply chain

## Industry Convergence

Achieve industry and supplier convergence on an approach (NATF Model) to facilitate assessment of suppliers' security posture

## Efficiency and Effectiveness

Convergence on common approaches to achieve reasonable assurance of suppliers' security practices

## Compliance

Implementation guidance to meet supply chain related CIP standards

# Don't Reinvent the Wheel!

## Conducted in open collaboration

- Industry
- Suppliers
- Third-party assessors
- Solution providers

## Leverage existing frameworks

- NIST
- IEC/ISO
- SOC

## Tailor to needs of electric industry

- Scalable as to size/organization type
- Usable by related industries/infrastructures

# NATF Resources Available to Industry

## NATF Supply Chain Security Assessment Model

- NATF Supply Chain Security Assessment Criteria
- Energy Sector Supply Chain Risk Questionnaire
- NATF Criteria and Questionnaire Revision Process

## NATF CIP-013 Implementation Guidance-Independent Assessments of Vendors (ERO Endorsed)

## NATF CIP-013 Implementation Guidance-Supply Chain Risk Management Plans (ERO Endorsed)

***Additional Resources from suppliers, third-party assessors, and solution providers are available on the NATF Public Website***



# Supply Chain Security Assessment Model



# NATF Supply Chain Security Criteria v3.0

63 criteria for supplier security practices within 6 risk areas:

- ✓ Asset control and management
- ✓ Asset change and configuration management
- ✓ Governance
- ✓ Incident response
- ✓ Information protection
- ✓ Vulnerability management

24 organizational information considerations

*Posted on <https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>*

# Energy Sector Supply Chain Risk Questionnaire

221 questions plus 19 general information questions in 12 categories:

- ✓ Company Overview
- ✓ Identity & Access Management
- ✓ Change & Configuration Management
- ✓ Mobile Devices & Application
- ✓ Cybersecurity Program Management
- ✓ Risk Management
- ✓ Cybersecurity Tools & Applications
- ✓ Supply Chain & External Dependencies Management
- ✓ Data Protection
- ✓ Vulnerability Management
- ✓ Event & Incident Response
- ✓ Workforce Management

Questions for 3 Areas:

- ✓ Supplier Corporate Systems
- ✓ Supplier Product
- ✓ Supplier Development System

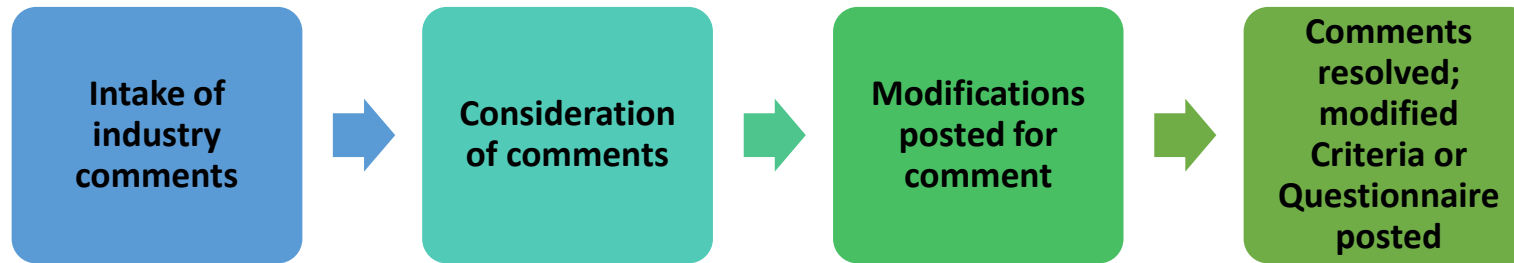
*Posted on <https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>*



# Revision Process for Criteria and Questionnaire

## Provides for an annual cycle for industry to modify or update the Criteria and Questionnaire

- Based on inputs from industry including utilities, suppliers, assessors, regulators, and other industry organizations



## NATF Board Approved Updated Versions on June 3, 2022

- Inclusion of ERO review in review process to maintain ERO Endorsement of the NATF CIP-013 Implementation Guidance documents
- Addition of three new criteria and two new questions
- Removal of four duplicative questions
- Minor changes include additional notes and terminology updates for clarity



Prior versions are also posted for tracking ease

# ERO Endorsed Implementation Guidance: Using Independent Assessments of Vendors

## Describes how to leverage the work of others

- R1: How to incorporate reliance on independent assessments into supply chain risk management plans
- R2: How to document use of independent assessments when implementing supply chain risk management plan

**Incorporates, by reference, NATF criteria, questionnaire, and associated revision process**



*Providing assurance of alignment between security and compliance*

# ERO Endorsed Implementation Guidance: Supply Chain Risk Management Plans

Describes how to use the NATF Supply Chain Security Assessment Model to develop a supply chain cyber security risk management plan(s)

- Focus is on security
- Addresses the six risk areas identified in Requirement R1, Part 1.2

Incorporates, by reference, NATF model, criteria, questionnaire, and associated revision process

*Providing assurance of alignment between security and compliance*



# Where to find resources: the NATF Public Website

North American Transmission FORUM +1 (704) 945-1900  
9115 Harris Corners Parkway, Suite 350 Charlotte, NC 28269  
info@natf.net

TransPort Request TransPort Access

Search

Home About Membership Programs Industry Initiatives News Documents Contact

Supply Chain Cyber Security Industry Coordination

Coronavirus Disease 2019 (COVID-19)  
Supply Chain Industry Coordination

The Industry Organizations Collaboration Effort

The NATF and other industry organizations are working together to provide a streamlined, effective, and efficient industry-accepted approach for entities to assess supplier cyber security practices. The model, if applied widely, will reduce the burden on suppliers so their efforts with purchasers can be prioritized and entities can be provided with more information effectively and efficiently. The industry organizations collaboration effort is focused on improving cyber security, and assisting registered entities with compliance to regulatory requirements.

Each of the industry organizations and many individual entities are working on solutions for various stages of the supply chain cyber security risk assessment lifecycle. These solutions are brought together in this effort to provide a cohesive approach. This approach may change over time as it matures but staying cohesive will be key to maintaining streamlined effective and efficient cyber security.

This website provides information on the approach (also referred to as the "model"), projects/activities that have been accomplished, and projects/activities in progress, upcoming presentations, links to related information, and recent news.

**The Model** (Version History)

- Supply Chain Security Assessment Model
- NATF Supply Chain Security Criteria V3.0
- Energy Sector Supply Chain Risk Questionnaire V3.0 (Unformatted, Formatted)
- Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Supply Chain Security Criteria

**Resources** (View All)

- Contributing Organizations
- NATF CIP-013 Implementation Guidance-Independent Assessments of Vendors (ERO Endorsed)
- NATF CIP-013 Implementation Guidance-Supply Chain Risk Management Plans (ERO Endorsed)

**Upcoming Meetings and Activities**

- MRO SAC Webinar on the Supply Chain Effectiveness Survey Results (April 12)  
Expand all

**Announcements** (View All)

June 06, 2022

NATF Supply Chain Criteria and Risk Questionnaire Version 3.0 Posted for Industry Use

The "NATF Supply Chain Security Criteria" and "Energy Sector Supply Chain Risk Questionnaire" version 3.0 documents and associated revision process have been posted for industry use on the Supply Chain Cyber Security Industry Coordination page of the NATF public website. A new "Version History" link has been added, which includes all prior versions and redlines of the NATF criteria and risk questionnaire.

The updates have been reviewed and accepted by the ERO Enterprise to ensure its continued endorsement of the two NATF CIP-013 Implementation Guidance

*Available at:*

<https://www.natf.net/industry-initiatives/supply-chain-industry-coordination>

# Panel Discussion

Facilitator: Valerie Agnew, NATF

## **Mikhail Falkovich**

Chief Information Security Officer  
Consolidated Edison, Inc.

## **Tony Hall**

Manager, CIP and Federal  
Regulatory Compliance  
LG&E and KU Energy

## **Jennifer M. Couch**

Manager, Transmission EMS  
Compliance  
Southern Company

## **Michael Pyle**

Director, Product Cyber Security  
Schneider Electric

## **Frank Harrill**

Vice President of Security  
Schweitzer Engineering Laboratories

## **Chris Fitzhugh**

Industrial Control Systems Security  
Consultant, North America  
Siemens Energy

# Discussion Question

***How does the use of the criteria and questionnaire enhance security and enable efficiencies?***

# Discussion Question

***How can industry and suppliers work together to converge on the use of the criteria and questionnaire?***

# Discussion Question

***How can third-party assessments and certifications optimize approaches to understanding and managing supply chain risks?***



# Panel Discussion



# Key Takeaways

- NATF continues to work towards bringing industry and suppliers together
- ERO-endorsed implementation guidance:
  - NATF.net > Industry Initiatives > Supply Chain Industry Coordination
- How to provide feedback to Criteria and Questionnaire:
  - Send message to [supplychain@natf.net](mailto:supplychain@natf.net)
- Leverage third-party assessments & certifications

# Continuing the Conversation for Suppliers

## NATF Supplier Sharing Calls

- A forum for suppliers to help suppliers
- Applicable to suppliers of all sizes and security maturity
- Inaugural call to be held on **October 26, 2022 1:00pm-2:30pm EDT**
- To request an invite, send a message to [supplychain@natf.net](mailto:supplychain@natf.net)