North American Transmission FORUM

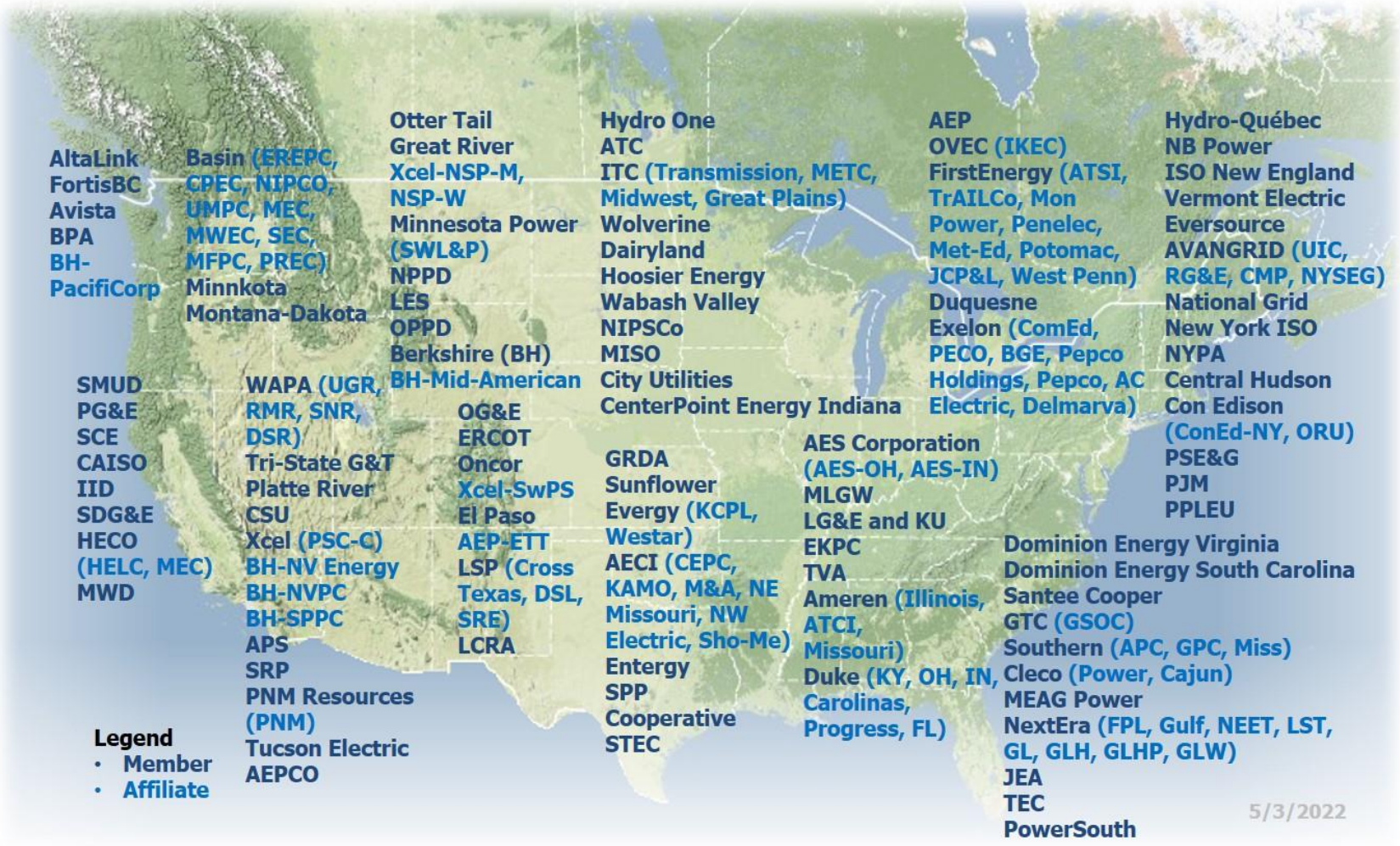
Community *Confidentiality* *Candor* *Commitment*

Optimizing Supplier-Purchaser Interaction for Supply Chain Risk Management

Ken Keels
Director, Initiatives

David James Earley
Program Manager, Cybersecurity & Supply Chain

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

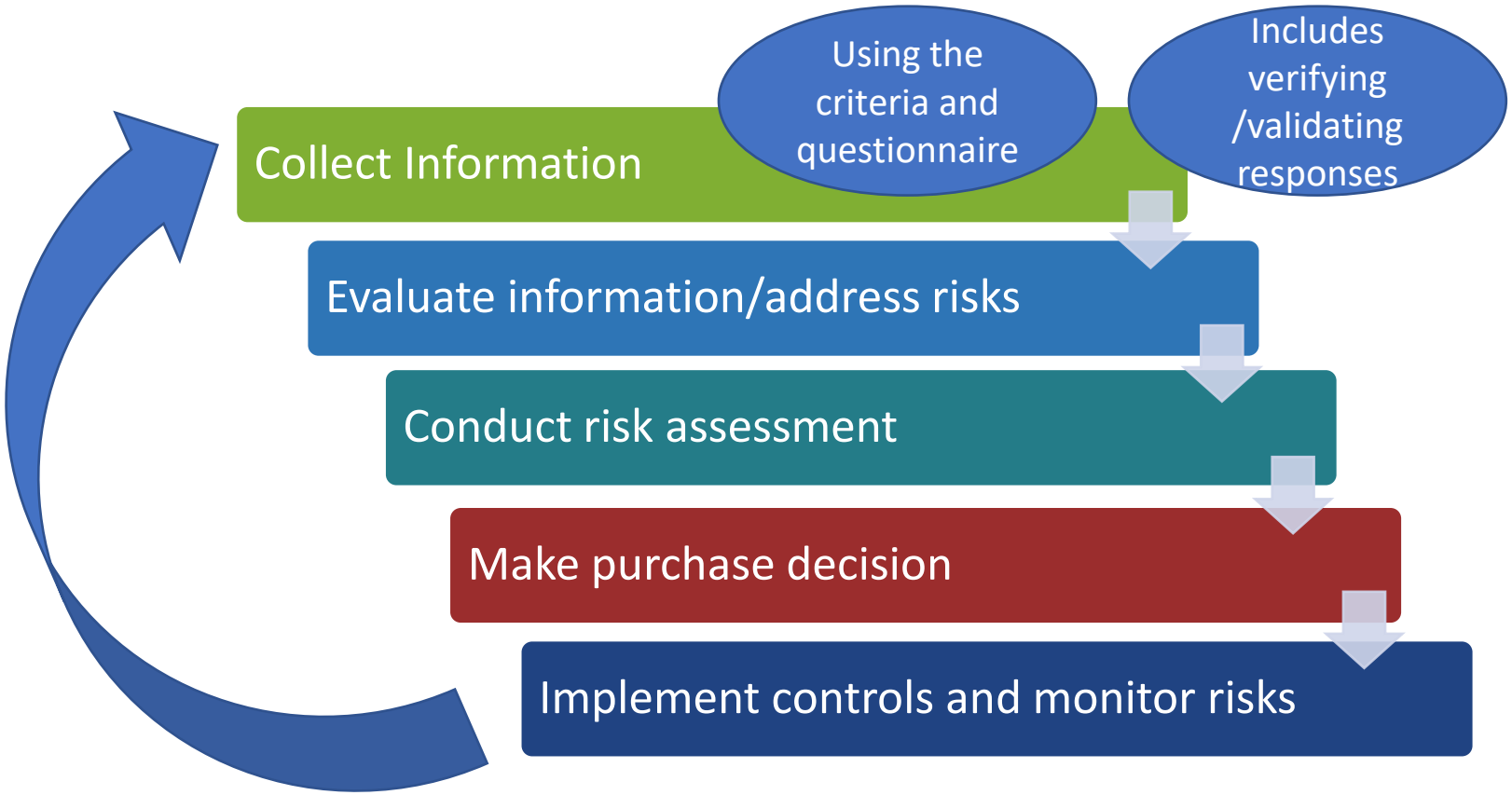
- NATF Supply Chain Security Assessment Criteria
- Energy Sector Supply Chain Risk Questionnaire
- NATF Criteria and Questionnaire Revision Process

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

Intake of industry comments → **Consideration of comments** → **Modifications posted for comment** → **Comments resolved; modified Criteria or Questionnaire posted**

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

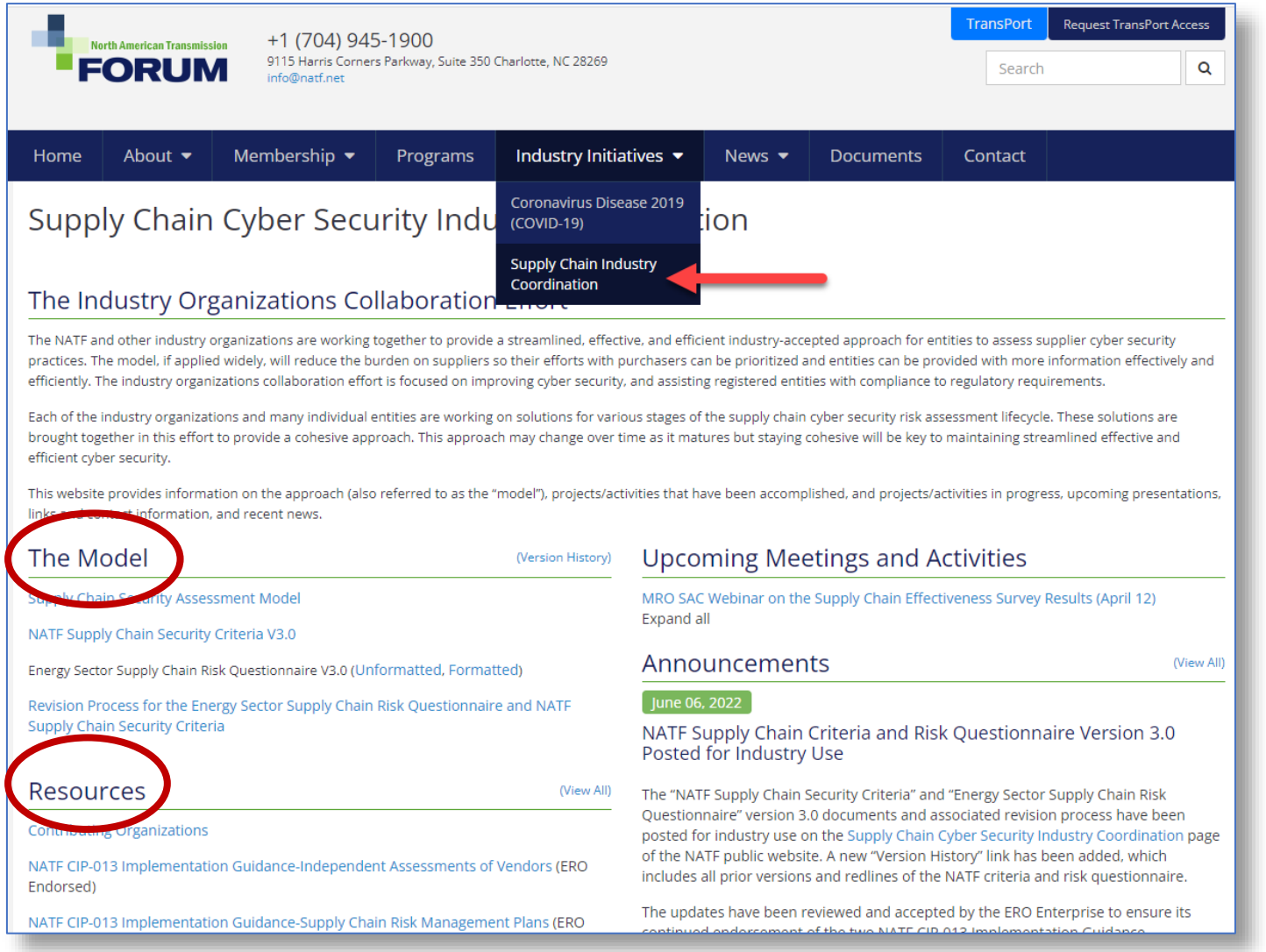
Describes how to use the NATF Supply Chain Security Assessment Model to develop a supply chain cyber security risk management plan(s)

- **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



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
- 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