



*Community Confidentiality Candor Commitment*

# NATF Supply Chain Criteria and Questionnaire Update

**Jamie Carnes**  
**Program Manager,**  
**Initiatives**

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

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

Copyright © 2023 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



**97 members**  
**90 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

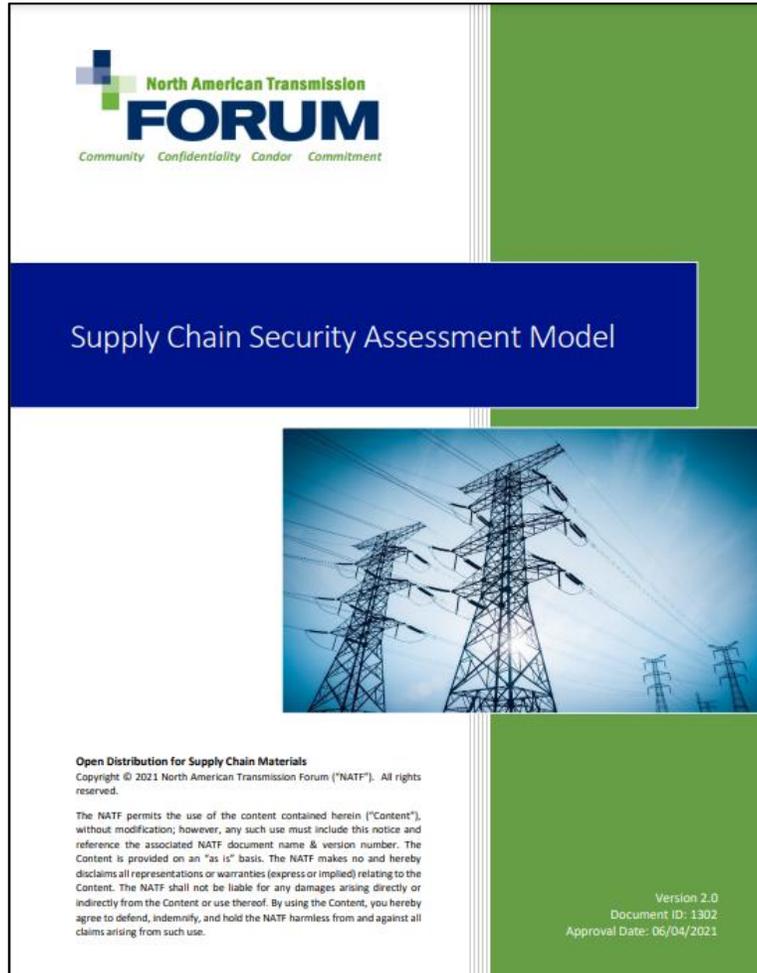
## Leverage existing frameworks

- NIST
- IEC/ISO
- SOC

## Tailor to needs of electric industry

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

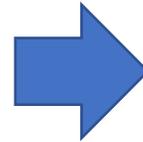
# NATF Supply Chain Security Assessment Model



# NATF Supply Chain Security Assessment Model

Collect Information

Includes  
verifying/validating  
responses



## Tools available

NATF Supply Chain Security Criteria

Energy Sector Supply Chain Risk Questionnaire

*NATF Criteria and Questionnaire Revision Process*

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

# NATF Supply Chain Security Criteria

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

# NATF Supply Chain Security Criteria V3.0

*Provides a basis for measuring a supplier's security posture/practices (i.e., a "best practices" list)*

Open Distribution				Mapping to Existing Frameworks												
Criteria Identification Number	Risk Area	NATF Supply Chain Security Criteria	Required by NERC Reliability Standards?		NIST						CIS Controls v7.1	IEC 62443	ISO 27001			
			Good security practices; exceeds NERC CIP Standards' requirements	CIP-013 requirement or supports other standards	Governance and all criteria NIST SP 800-161, 800-53	Access NIST SP 1800-2	Asset Chg Config - NIST SP 1800-5	Info Protection - NIST SP 800-171	Incident Response - NIST SP 800-184, 800-150, 800-61	Vulnerability Mgmt - NIST SP 800-64, 800-160, 800-82, 800-115, 800-125	Cybersecurity Framework Version 1.1			List other versions of ISO 27001.xxxx, 27001 if applicable		
1	Access Control and Mgmt	Supplier establishes and maintains an identity and access management program that ensures sustainable, secure product manufacturing/development		R1.2.3 R1.2.6	PR.AC-1-5 Rev. 4 AC-1-6 IA Family AC-16-20 CM-7 PE-2-6 PE-9 SC-7							PR.AC-1 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.PT-3	CSC 14: Controlled Access Based on the Need to Know  CSC 16: Account Monitoring and Control	2.4 SP.03.01 2.4 SP.03.07 2.4 SP.03.08	A.9.1.1 A.9.4.1	
2	Access Control and Mgmt	Supplier establishes and maintains a program that ensures storage security at supplier's site (e.g. chain of custody)	x		PR.AC-4 Rev. 4 AC-16 MP-4							PR.AC-1 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.PT-3	CSC 14: Controlled Access Based on the Need to Know  CSC 16: Account Monitoring and Control	2.4 SP.03.10	A.15.1.2	
3	Access Control and Mgmt	Supplier's personnel vetting process allows supplier to share background check criteria and results with entity for confirmation of process or verification of sampled employees	x	Supports CIP-004 R3.4												7.1.1
		Supplier has a process that requires supplier to have background checks (e.g. personnel risk assessments) conducted for all of its employees and contractors. Please provide a list of any exempted employees or contractors.	x	Supports CIP-004 R3	PR.AC-1 Rev. 4 PS-3											7.1.1
		Supplier's process requires to conduct background checks at not require at least every 7 years, supplier's process requires			PR.AC-4 Rev. 4											

Maps criteria to multiple security frameworks (e.g., ISO, IEC, NIST...)

Developed by NATF-led team of industry SMEs; Updated with input from industry, suppliers, third-party assessors, ERO, and FERC

# Energy Sector Supply Chain Risk Questionnaire

## 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

221 questions plus 19 general information questions

# Energy Sector Supply Chain Risk Questionnaire v3.0

Energy Sector Supply Chain Risk Questionnaire - Formatted						Version 3.0	Published 06/06/2022	
Open Distribution for Supply Chain Materials Copyright © 2022 North American Transmission Forum, Inc.								
Cybersecurity Program Management		Supplier Corporate Systems	Supplier Product	Product Development Systems	Additional Information	Guidance	NATF Criteria	Primary or Supporting for NATF Criteria
CSPM-01	Do you have a business continuity plan (BCP) to support ongoing operations of your systems and scope of equipment and/or services provided to the utility?						21	Primary (21) Supports (44)
CSPM-02	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?							Supports (21)
CSPM-03	Has your BCP been tested in the last year?							
CSPM-04	Does your organization have a data privacy policy that applies to your computing systems?							Supports (38)
CSPM-05	Have overall system and/or application architecture diagrams, including a full description of the data communications architecture, been developed and documented for the product(s) and/or service(s) being purchased?							Supports (56)
CSPM-06	Do you have a media handling process (that is documented and currently implemented) including end-of-life, repurposing, and data sanitization procedures?							Primary (40) Supports (2)
	on (e.g., data,							Primary (46)
	Do you have							Primary (24)
	nd							
	n.							
	onment,							

key supporting questions are identified

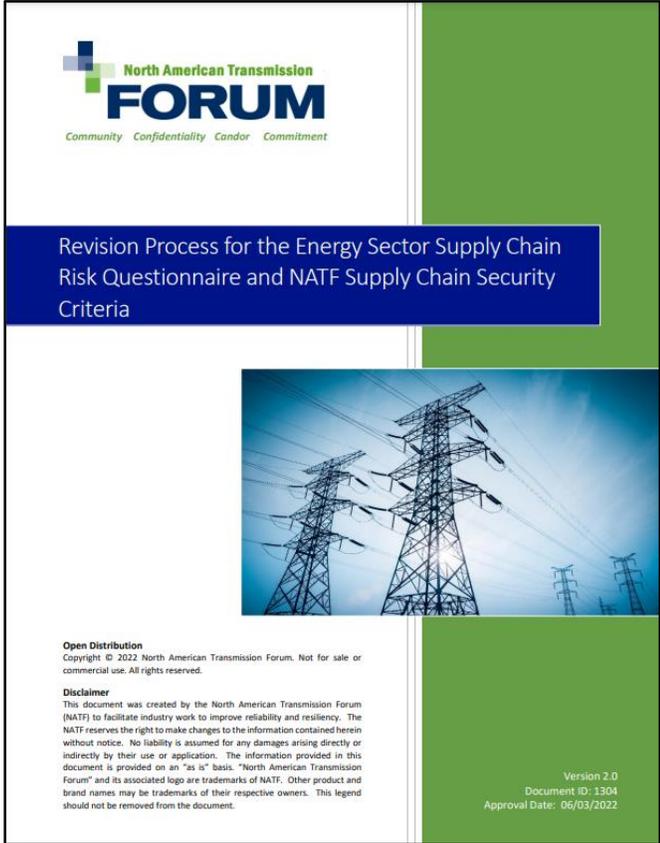
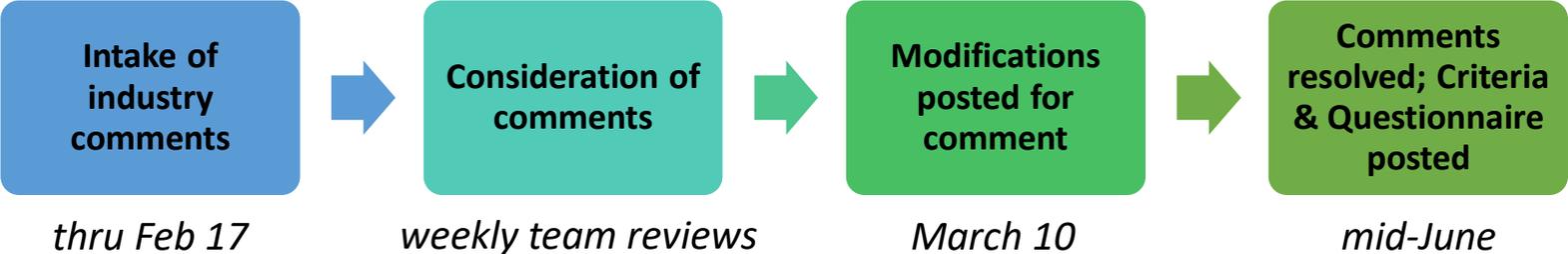
Developed by NATF-led team of industry SMEs;  
Updated with input from industry, suppliers, third-party assessors, ERO, and FERC

Provides a consistent set of questions that support the NATF Criteria and help obtain more-granular information on a supplier's security risk performance

# 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
- Prior versions are also posted for tracking ease



# Questionnaire Scorable Option

DEMO

# 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

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, and contact 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, Scorable Option)
- 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

Expand all

Announcements (View All)

December 22, 2022

Scorable Version of NATF Supply Chain Risk Questionnaire Now Available

Based on industry feedback, the NATF has developed a scorable version of the *Energy Sector Supply Chain Risk Questionnaire* to provide an optional format for entities to help assess supply chain risk. This optional format provides all the same questions as the existing questionnaire but adds the ability for entities to provide their own per-question score and weight to a completed questionnaire. This flexible approach allows entities to adjust weights to reflect their unique needs or priorities while allowing for the consistent evaluation of multiple responses. No prescribed thresholds or requirements are made by the NATF, and all scores are provided by the entities themselves.

## 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)
- NATF Industry Collaboration: Using Solution Providers for Third-Party Risk Management

Click "View All" above to access additional documents, presentations, supply-chain sites, and support products and services.

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

# Key Takeaways

- NATF continues to work towards bringing industry and suppliers together
- Review the NATF Model, Criteria, and Questionnaire at:
  - <https://www.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)

# Questions

