Joint Supply Chain Practice Group and Supplier Sharing Call

June 1st, 2026 – 2pm-3pm ET

Guidelines for this meeting

- This is an open meeting
- Some participants of this meeting are not employees of NATF member companies
  - Do not share confidential information
  - Avoid conduct that unreasonably restrains competition
  - Adhere to your organization's standards of conduct
  - Do not share intellectual property unless authorized

Agenda

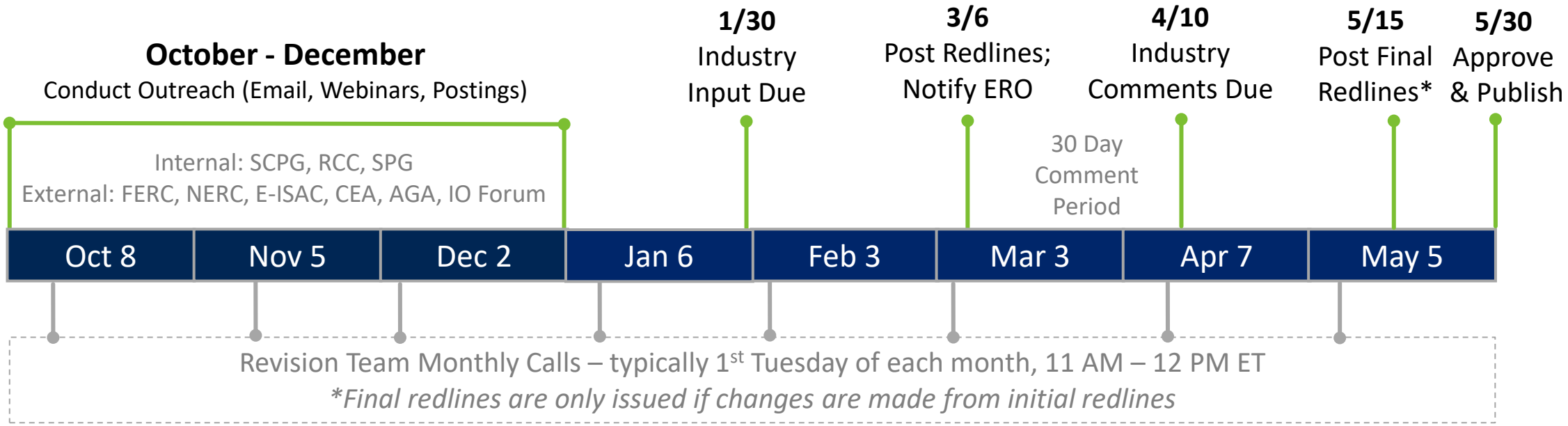
- Supply chain program updates
- NATF Supply Chain Risk Controls and Monitoring
- Panel on AI-discovered vulnerabilities

Supply chain program updates

David James Earley, NATF

Criteria and Questionnaire revision update

2026 Annual Revision Process (v7) Timeline



2026 Criteria and Questionnaire updates

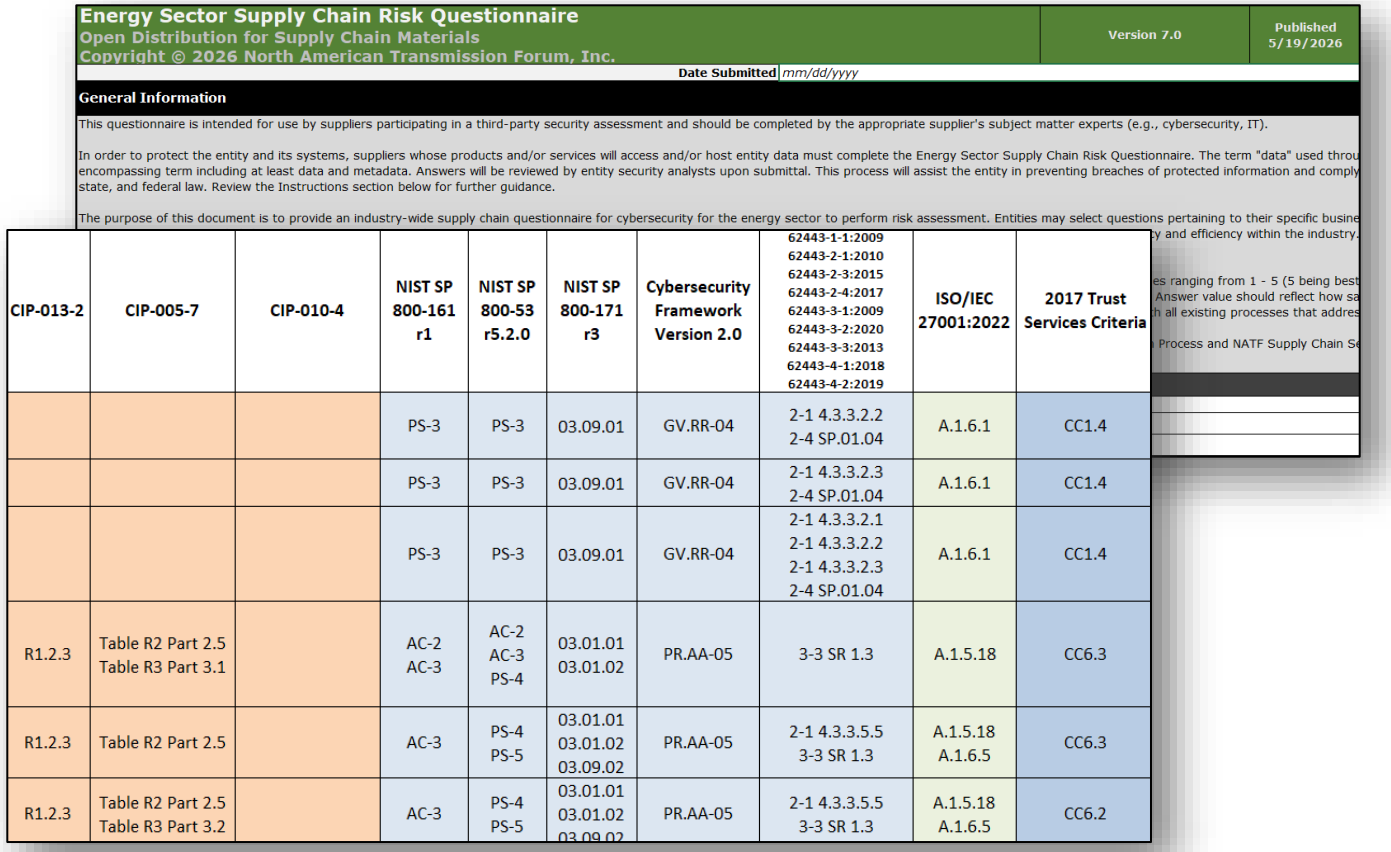
- Criteria
  - Addition of *Supplier Response* column
  - 1 added, 1 removed, 2 merged criteria
  - 5 edits for clarity and completeness
  - Updated references and mapping updates for NIST SP 800-171r3 & NIST SP 800-53r5.2.0

Open Distribution for Supply Chain Materials

Criteria Number	Risk Area	NATF Supply Chain Security Criteria	Supplier Response	Answer	Weight	Score
				Total Score		0
1	Access Control and Mgmt	Supplier establishes and maintains an identity and access management program that ensures secure product manufacturing/development				0
1.1	Access Control and Mgmt	Supplier's organization, including the computing application system, implements phishing-resistant multi-factor authentication (e.g., Authenticator app, One-Time-Password (OTP) codes, passkeys)				0
2	Access Control and Mgmt	Supplier establishes and maintains a program that ensures storage security of hardware, software, data, or other physical evidence at supplier's site (e.g. chain of custody)				0

2026 Criteria and Questionnaire updates

- Questionnaire
  - 18 edits for clarity and improved coverage
  - Revised guidance text
  - 1 added, 3 removed, 2 merged questions
  - Updated references and mapping updates for NIST SP 800-171r3 & NIST SP 800-53r5.2.0



Energy Sector Supply Chain Risk Questionnaire
Open Distribution for Supply Chain Materials
Copyright © 2026 North American Transmission Forum, Inc.
Version 7.0 | Published 5/19/2026

Date Submitted mm/dd/yyyy

General Information

This questionnaire is intended for use by suppliers participating in a third-party security assessment and should be completed by the appropriate supplier's subject matter experts (e.g., cybersecurity, IT).

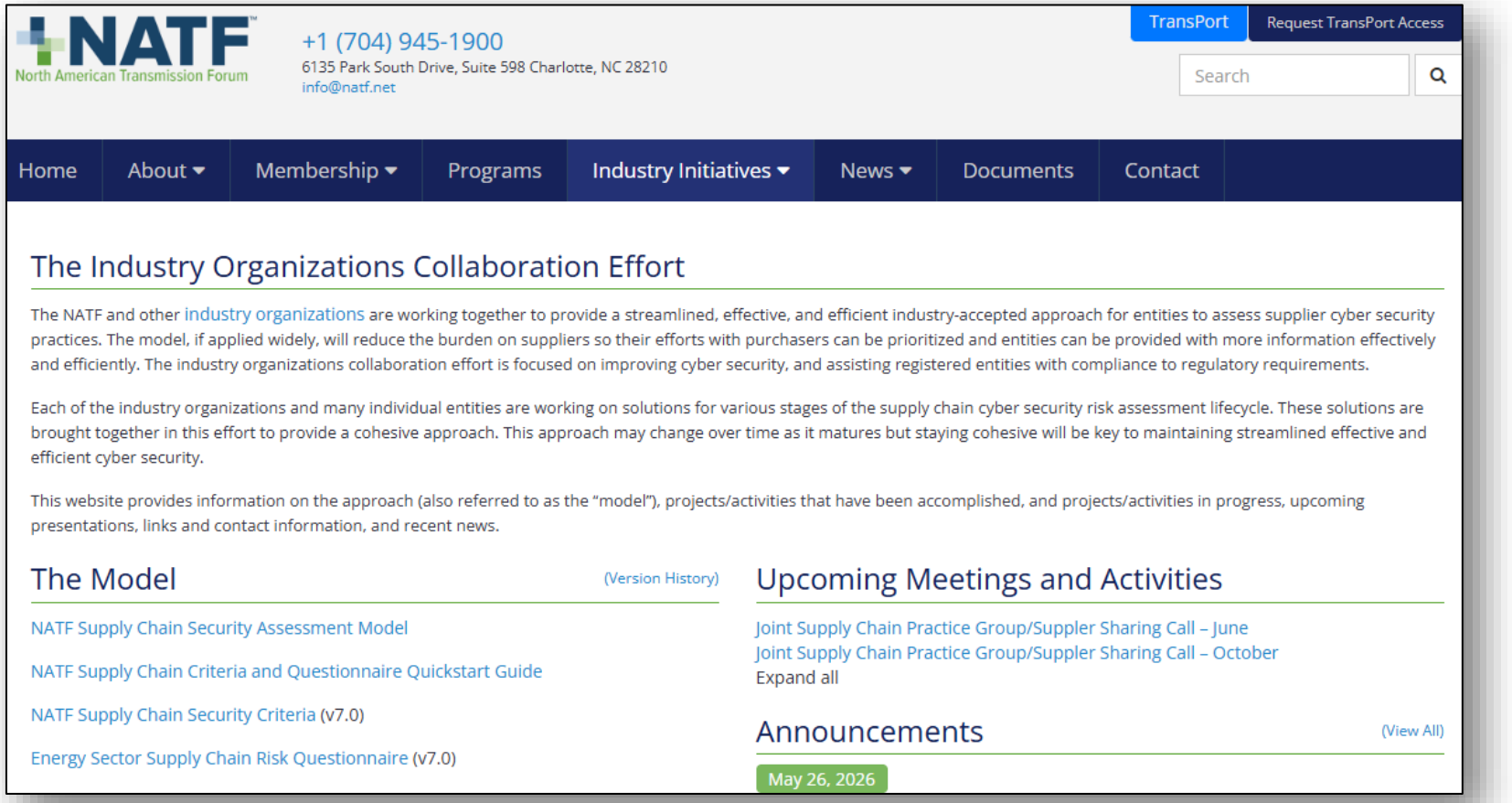
In order to protect the entity and its systems, suppliers whose products and/or services will access and/or host entity data must complete the Energy Sector Supply Chain Risk Questionnaire. The term "data" used throu
encompassing term including at least data and metadata. Answers will be reviewed by entity security analysts upon submittal. This process will assist the entity in preventing breaches of protected information and comply
state, and federal law. Review the Instructions section below for further guidance.

The purpose of this document is to provide an industry-wide supply chain questionnaire for cybersecurity for the energy sector to perform risk assessment. Entities may select questions pertaining to their specific busine
y and efficiency within the industry.

es ranging from 1 - 5 (5 being best
Answer value should reflect how sa
h all existing processes that addres
Process and NATF Supply Chain Se

CIP-013-2	CIP-005-7	CIP-010-4	NIST SP 800-161 r1	NIST SP 800-53 r5.2.0	NIST SP 800-171 r3	Cybersecurity Framework Version 2.0	62443-1-1:2009 62443-2-1:2010 62443-2-3:2015 62443-2-4:2017 62443-3-1:2009 62443-3-2:2020 62443-3-3:2013 62443-4-1:2018 62443-4-2:2019	ISO/IEC 27001:2022	2017 Trust Services Criteria
			PS-3	PS-3	03.09.01	GV.RR-04	2-1 4.3.3.2.2 2-4 SP.01.04	A.1.6.1	CC1.4
			PS-3	PS-3	03.09.01	GV.RR-04	2-1 4.3.3.2.3 2-4 SP.01.04	A.1.6.1	CC1.4
			PS-3	PS-3	03.09.01	GV.RR-04	2-1 4.3.3.2.1 2-1 4.3.3.2.2 2-1 4.3.3.2.3 2-4 SP.01.04	A.1.6.1	CC1.4
R1.2.3	Table R2 Part 2.5 Table R3 Part 3.1		AC-2 AC-3	AC-2 AC-3 PS-4	03.01.01 03.01.02	PR.AA-05	3-3 SR 1.3	A.1.5.18	CC6.3
R1.2.3	Table R2 Part 2.5		AC-3	PS-4 PS-5	03.01.01 03.01.02 03.09.02	PR.AA-05	2-1 4.3.3.5.5 3-3 SR 1.3	A.1.5.18 A.1.6.5	CC6.3
R1.2.3	Table R2 Part 2.5 Table R3 Part 3.2		AC-3	PS-4 PS-5	03.01.01 03.01.02 03.09.02	PR.AA-05	2-1 4.3.3.5.5 3-3 SR 1.3	A.1.5.18 A.1.6.5	CC6.2

2026 Criteria and Questionnaire updates



Available for free on NATF's [Supply Chain Industry Coordination]() website

Questions?

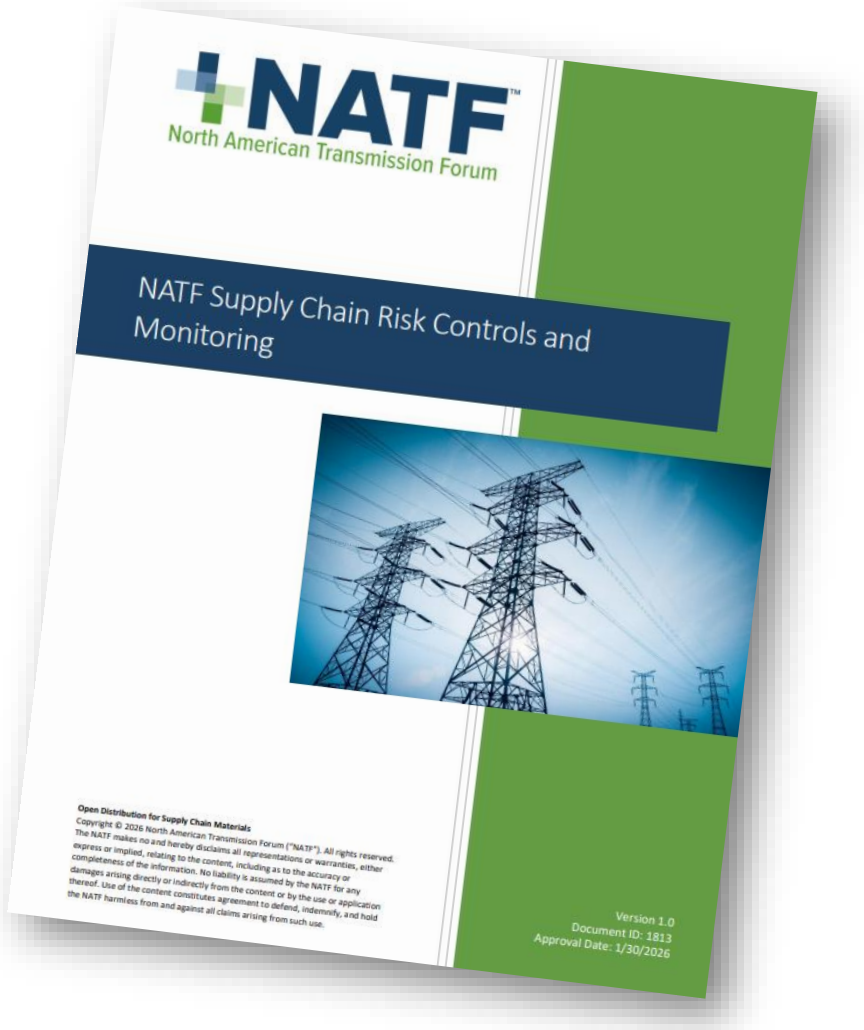
NATF Supply Chain Risk Controls and Monitoring

David James Earley, NATF
Jennifer Couch, Southern Company

David E.

Supply Chain Risk Controls and Monitoring

- Recently published supply chain guidance
- Discusses supplier controls, control documentation, and supplier monitoring practices
- Relates to **Step 5**: *Implement controls and monitor risks* of NATF Supply Chain Security model
- Available on NATF's public Supply Chain Industry Coordination website

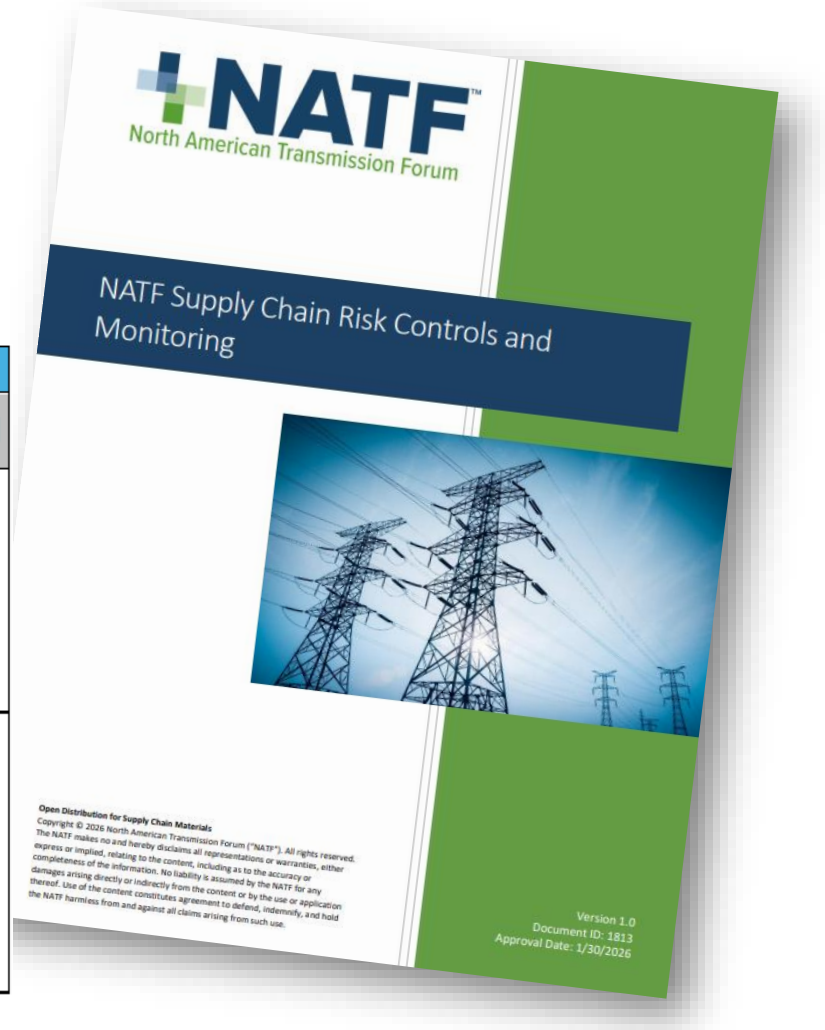


Supply Chain Risk Controls and Monitoring

- Key considerations:
  - Supplier risk tiering & reassessment

Example below:

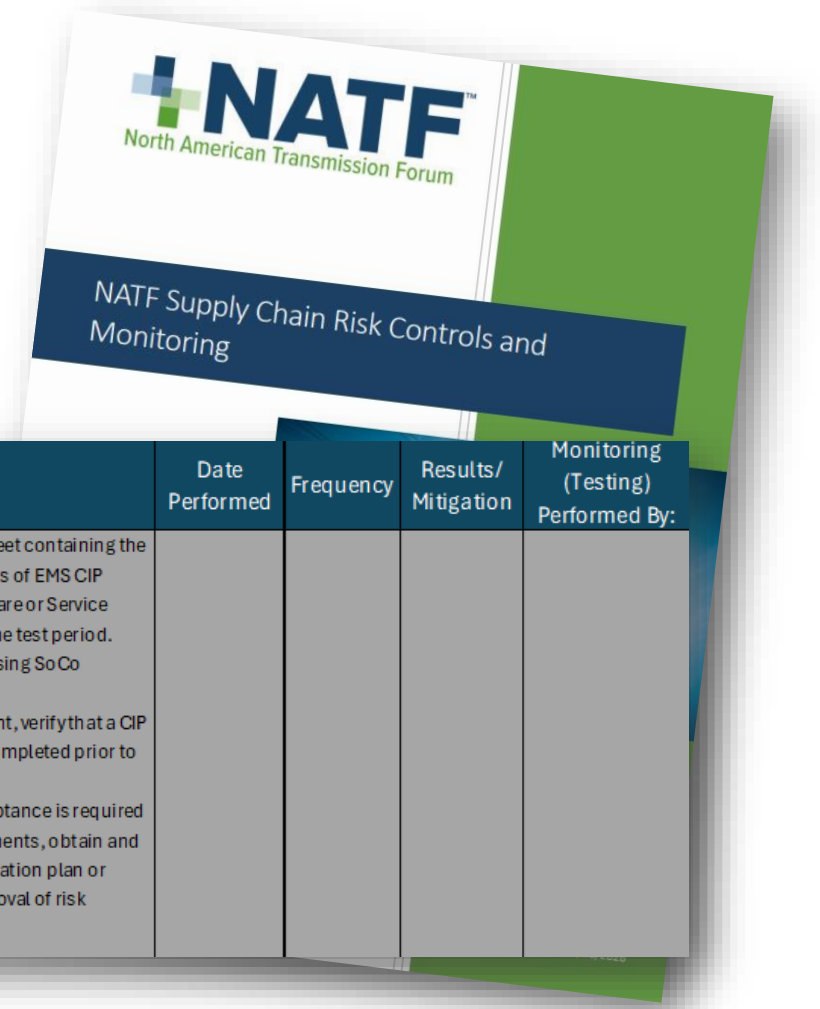
VRC 1	VRC 2	VRC 3
Vendor Risk Assessment (VRA)	**Data Driven Vendor Assessment (DDVA)**	**No Assessment Required**
• Highest Risk to the Company. • Perform a full CIP Vendor Risk Assessment	• Medium Risk to the Company. • Perform at a minimum a Data Driven Vendor Assessment	• Lowest Risk to the Company. • Consider conducting a Data Driven Vendor Assessment during RFI
• Business Questionnaire & VRA completed at least once every 12 calendar months.	• Business Questionnaire completed at least once every 12 calendar months. • DDVA completed at least once every 24 calendar months.	• Business Questionnaire completed at least once every 12 calendar months.



Supply Chain Risk Controls and Monitoring

- Key considerations:
  - Identify, assign, and implement controls

Example below:

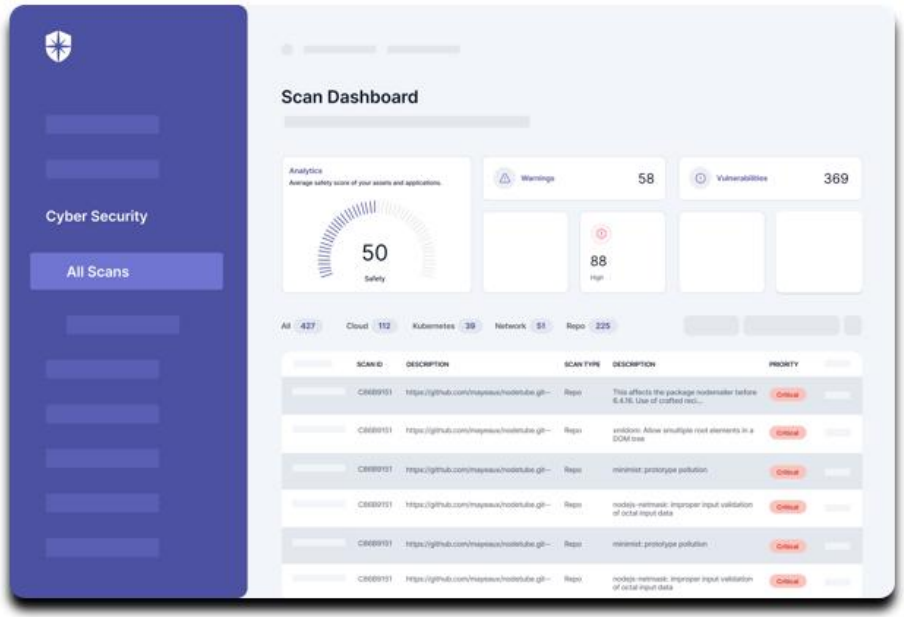


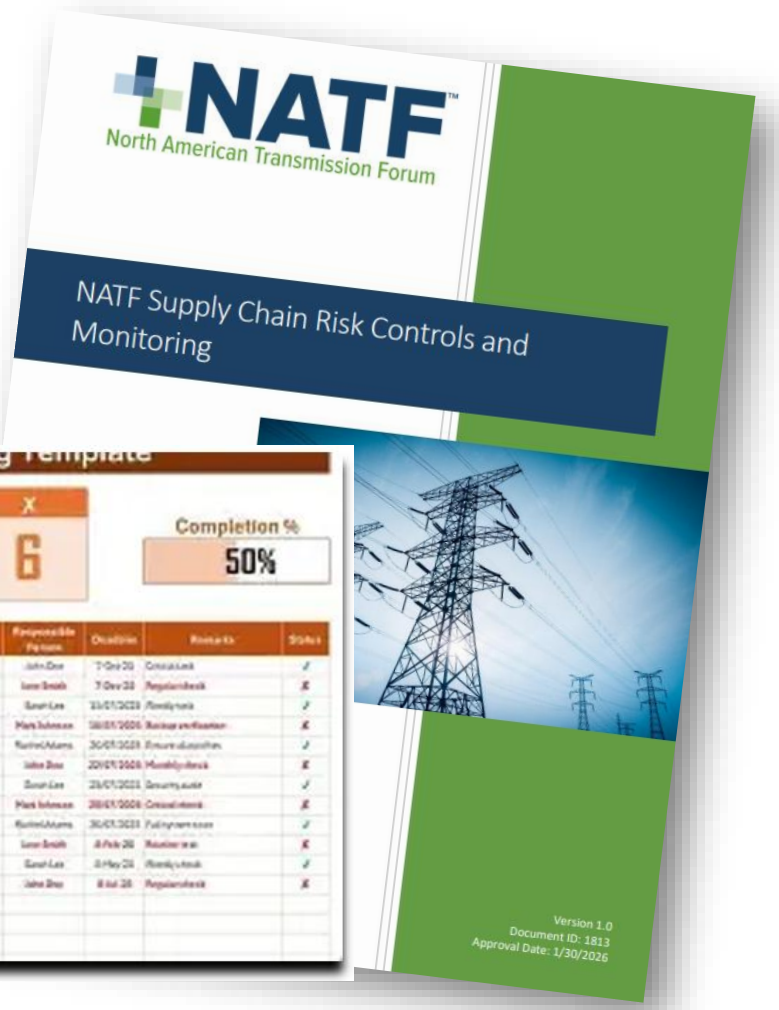
Control ID	Requirement	Control Objective	Control Activity	Control Owner	Test Steps	Date Performed	Frequency	Results/ Mitigation	Monitoring (Testing) Performed By:
CIP.EMS.SC.C1	CIP-013-1 R2	Demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.	A CIP Vendor Risk Assessment and, as applicable, a risk mitigation plan and/or risk acceptance decision is performed and documented for procurements of EMS CIP Vendor in-scope systems, software and services.		1. Obtain the tracking spreadsheet containing the population of new procurements of EMS CIP Vendor In-Scope System, Software or Service related to Cyber Assets during the test period. 2. Select a sample from step 1 using SoCo Sampling Guidance. 3. For each sampled procurement, verify that a CIP Vendor Risk Assessment was completed prior to procurement finalization. 4. If Risk mitigation and/or acceptance is required for any of the sampled procurements, obtain and inspect a documented risk mitigation plan or documented management approval of risk acceptance as applicable.				

Supply Chain Risk Controls and Monitoring

- Key considerations:
  - First and third-party monitoring

Examples below:



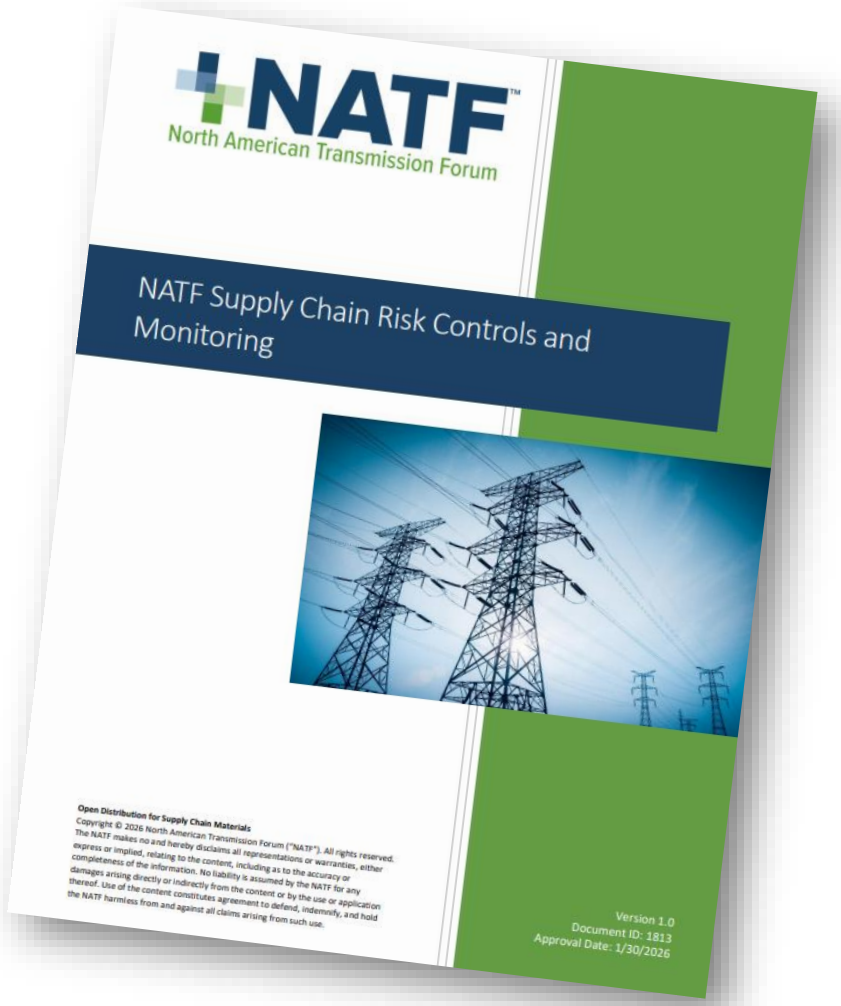


Supply Chain Risk Controls and Monitoring

- Key considerations:
  - Documenting risk determinations

Example below:

Malware Detection and Protection – ability to configure host-based malware prevention and detection capabilities or whitelisting solutions that are tested and validated. **Provide summary of Risks considered in performing the Business Security Risk Assessment:** **Risk Assessment/Identified Unique Risks which will not be the contractual responsibility of the Vendor and require Mitigation or Acceptance:**	**Is this Business Security Risk Area Applicable?** Yes: ☐ No: ☐ **Any Business Security Risk Identified?** Yes: ☐ No: ☐	**Any Unique Risks Identified?** Yes: ☐ No: ☐	**Post Contract Risk Mitigation Required?** Yes: ☐ No: ☐ **Post Contract Risk Acceptance Required?** Yes: ☐ No: ☐



Questions?

AI-discovered vulnerabilities

Panel discussion

David E.

AI Discovered Vulnerabilities

Frank Harrill

Schweitzer Engineering Laboratories

Mike Pyle

Schneider Electric

Chris Fitzhugh

Siemens Energy

AI Discovered Vulnerabilities

How is artificial intelligence powering vulnerability research and exploitation?

Mike P.
Frank H.
Chris F.

AI Discovered Vulnerabilities

How do you prepare and prioritize?

Mike P.
Frank H.
Chris F.

AI Discovered Vulnerabilities

What changes may be needed for patching and mitigation approaches?

Mike P.
Frank H.
Chris F.

AI Discovered Vulnerabilities

How can you incorporate AI tools into your own vulnerability management and testing pipeline?

Mike P.
Frank H.
Chris F.

AI Discovered Vulnerabilities

What does responsible disclosure look like?

Mike P.
Frank H.
Chris F.

AI Discovered Vulnerabilities

Looking ahead, what are your biggest areas of concern?

Mike P.
Frank H.
Chris F.

AI Discovered Vulnerabilities

What are you doing differently to stay abreast of this changing environment?

Mike P.
Frank H.
Chris F.

Questions?

Thank you for attending!

NATF Contact Information

NATF Supply Chain

supplychain@natf.net

Let us know your thoughts on today's meeting:

Post-meeting survey