



Joint Supply Chain Practice Group and Supplier Sharing Call

June 1st, 2026 – 2pm-3pm ET

Open Distribution for Supply Chain Materials

Copyright © 2026 North American Transmission Forum (“NATF”). All rights reserved. The NATF makes no and hereby disclaims all representations or warranties, either express or implied, relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use.

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

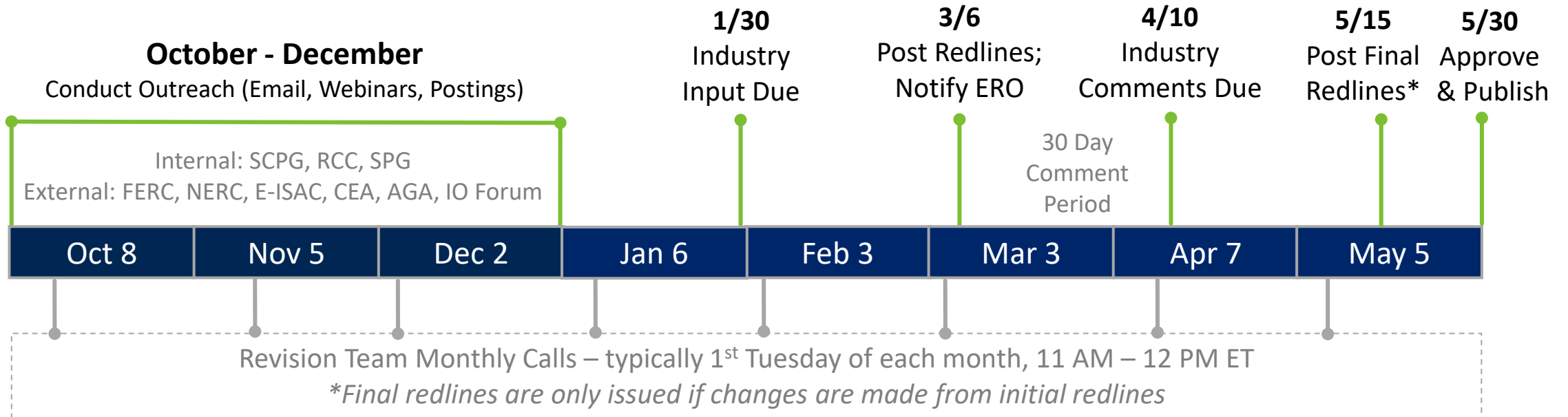
- Supply chain program updates
- NATF Supply Chain Risk Controls and Monitoring
- Panel on AI-discovered vulnerabilities

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						
Copyright © 2026 North American Transmission Forum, Inc.						
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							Version 7.0	Published 5/19/2026	
Open Distribution for Supply Chain Materials Copyright © 2026 North American Transmission Forum, Inc.							Date Submitted <i>mm/dd/yyyy</i>		
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 through this questionnaire encompasses 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 complying with applicable 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 business operations and efficiency within the industry.									
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

The screenshot shows the NATF website header with the logo, contact information (+1 (704) 945-1900, 6135 Park South Drive, Suite 598 Charlotte, NC 28210, info@natf.net), and a search bar. The navigation menu includes Home, About, Membership, Programs, Industry Initiatives, News, Documents, and Contact. The main content area features the heading 'The Industry Organizations Collaboration Effort' followed by three paragraphs of text. Below this, there are three columns of links: 'The Model' (with a '(Version History)' link), 'Upcoming Meetings and Activities' (with links for June and October calls, and an 'Expand all' link), and 'Announcements' (with a '(View All)' link and a date tag for 'May 26, 2026').

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

Questions?





NATF Supply Chain Risk Controls and Monitoring

David James Earley, NATF

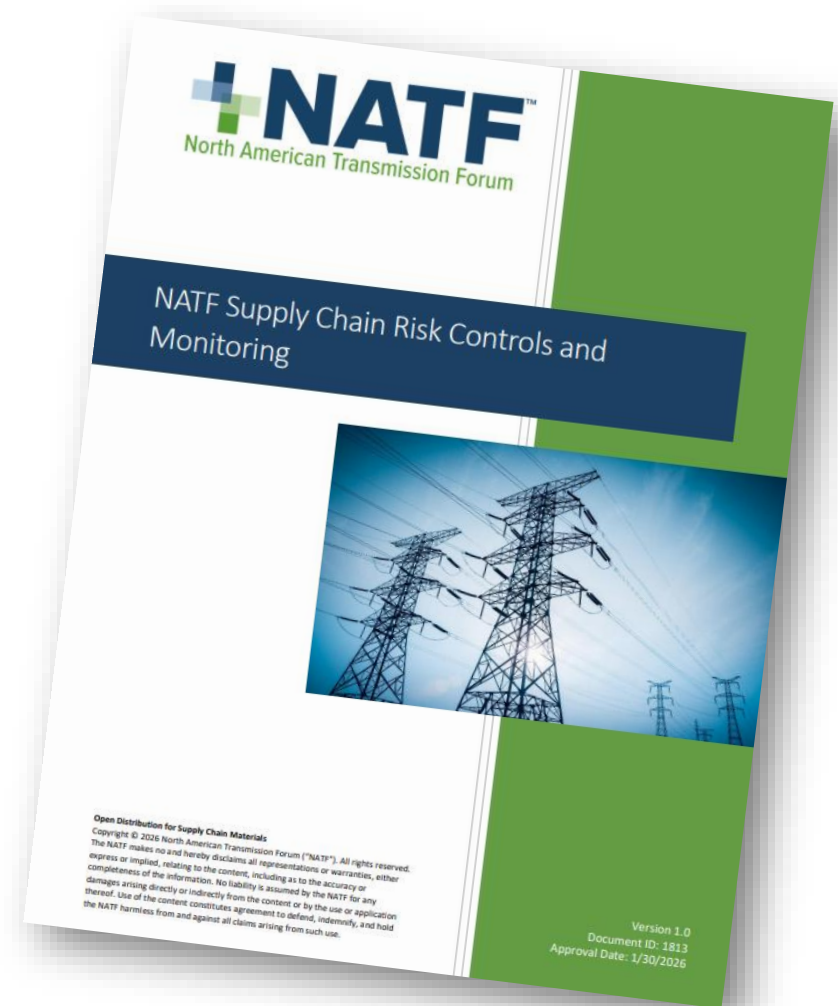
Jennifer Couch, Southern Company

Open Distribution for Supply Chain Materials

Copyright © 2026 North American Transmission Forum (“NATF”). All rights reserved. Presentations are provided with the presenters’ permission for distribution. The NATF makes no and hereby disclaims all representations or warranties, either express or implied, relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use. Further, no liability is assumed for infringement by any presentation materials, artwork, or photographs used in presentations not developed by NATF.

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

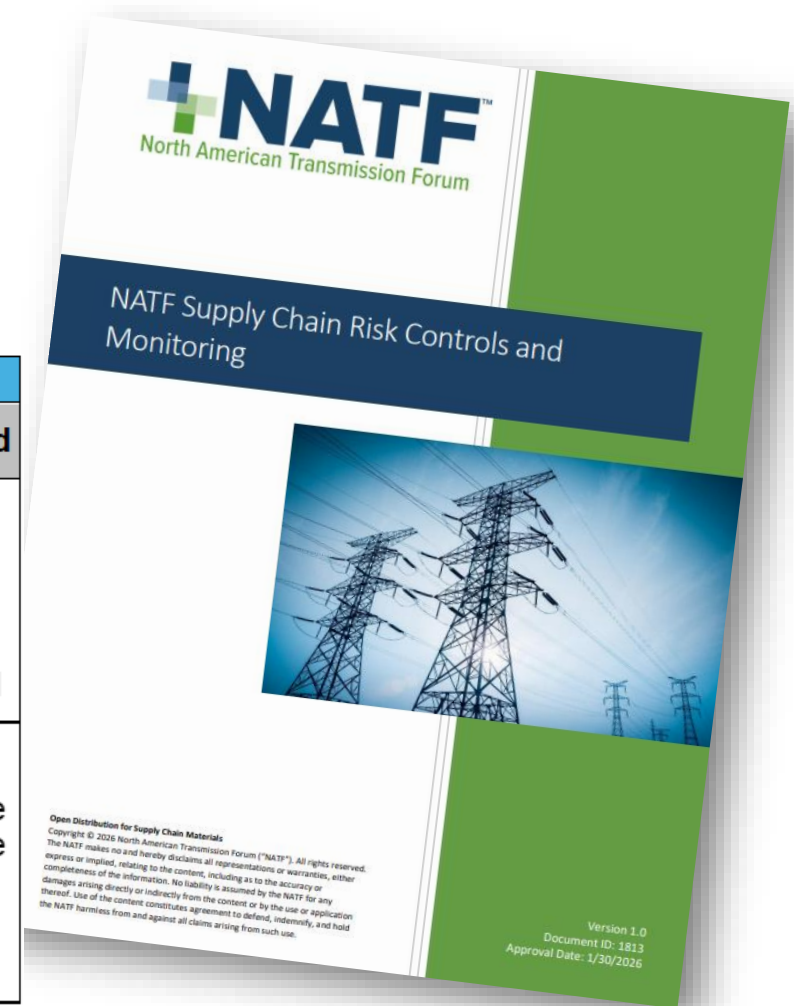


Supply Chain Risk Controls and Monitoring

- Key considerations:
 - Supplier risk tiering & reassessment

Example below:

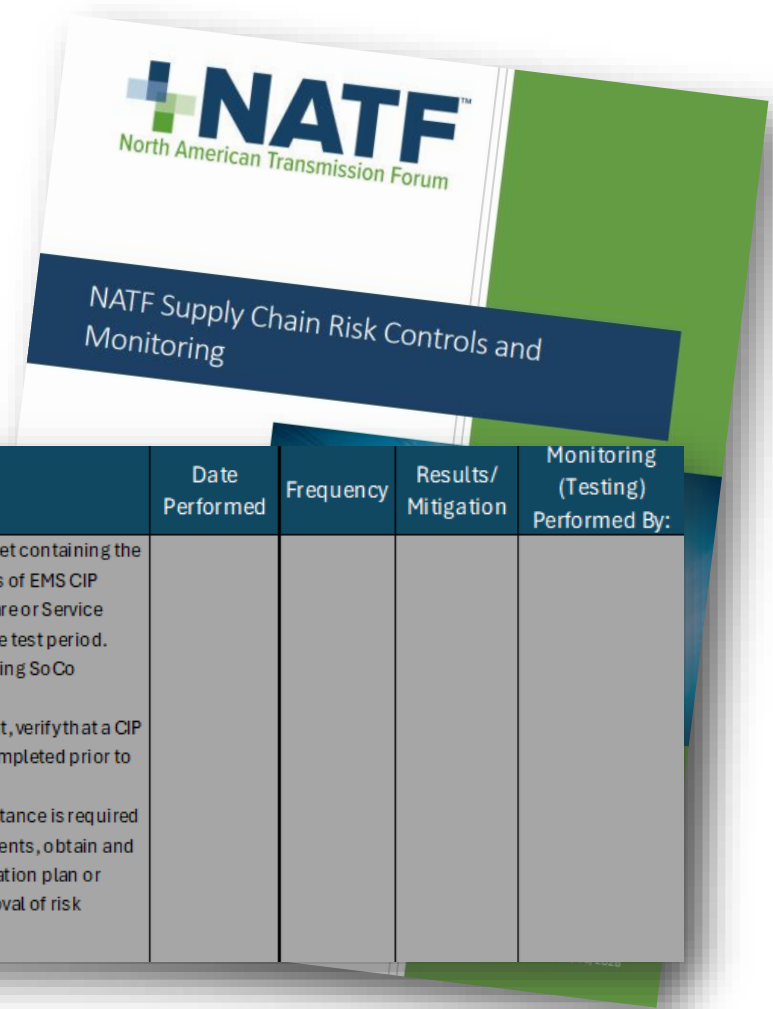
VRC 1	VRC 2	VRC 3
Vendor Risk Assessment (VRA)	Data Driven Vendor Assessment (DDVA)	No Assessment Required
<ul style="list-style-type: none"> • Highest Risk to the Company. • Perform a full CIP Vendor Risk Assessment 	<ul style="list-style-type: none"> • Medium Risk to the Company. • Perform at a minimum a Data Driven Vendor Assessment 	<ul style="list-style-type: none"> • Lowest Risk to the Company. • Consider conducting a Data Driven Vendor Assessment during RFI
<ul style="list-style-type: none"> • Business Questionnaire & VRA completed at least once every 12 calendar months. 	<ul style="list-style-type: none"> • Business Questionnaire completed at least once every 12 calendar months. • DDVA completed at least once every 24 calendar months. 	<ul style="list-style-type: none"> • 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:

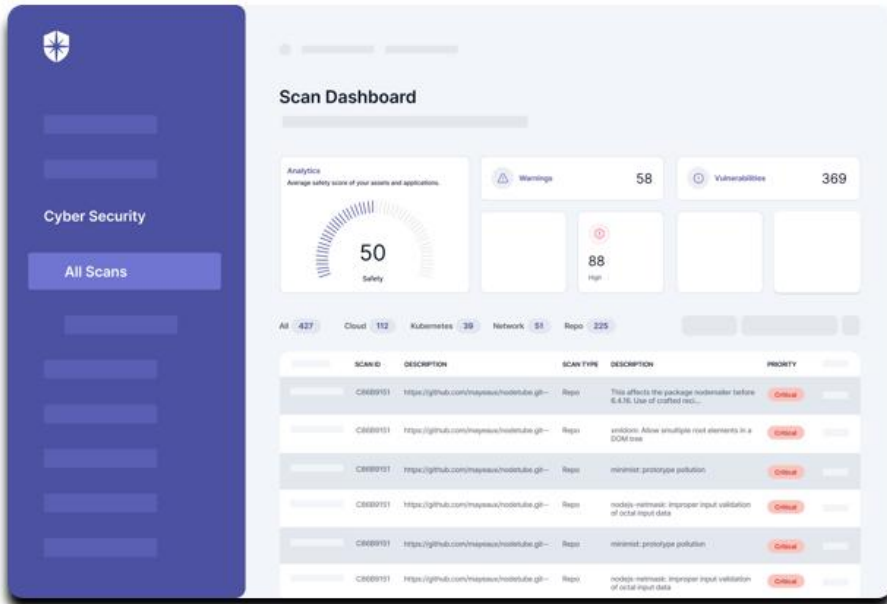


Control ID	Requirement	Control Objective	Control Activity	Control Owner	Test Steps	Date Performed	Frequency	Results/Mitigation	Monitoring (Testing) Performed By:
CIP.EMS.SC.C1	CIP-013-1 R2	Demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but 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.		<ol style="list-style-type: none"> 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

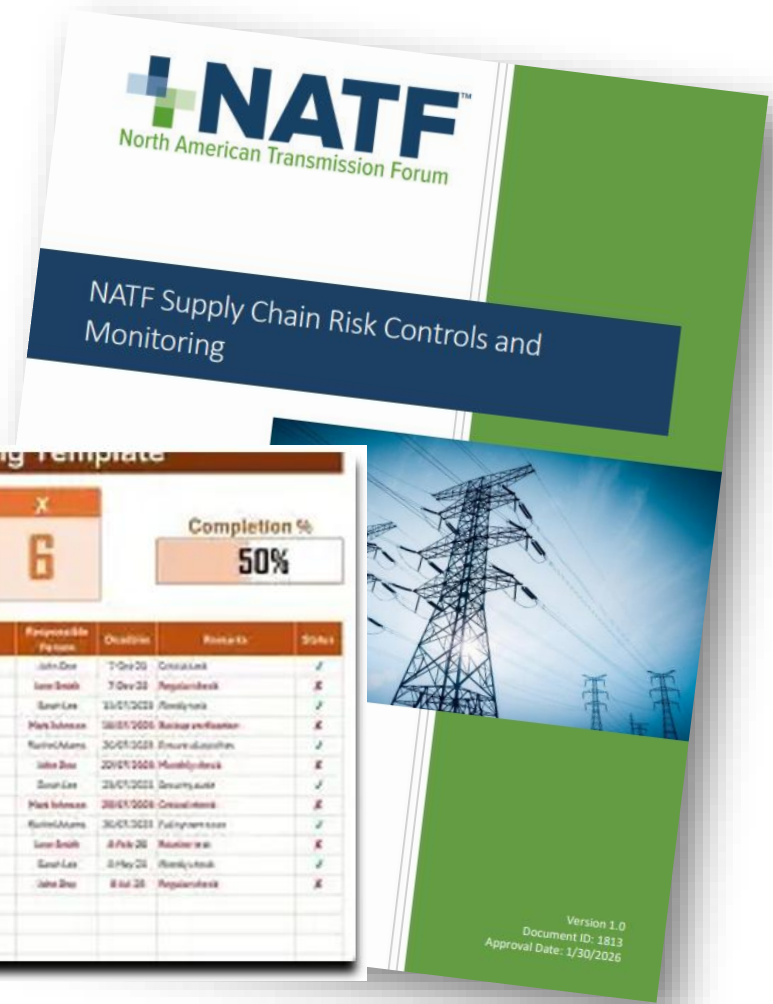
Examples below:



Cybersecurity Monitoring Template

Fail Count: 12 (Green: 6, Red: 6) Completion %: 50%

Checklist Item	Description	Responsible Person	Due Date	Priority	Status
System Updates	Ensure all systems are updated	John Doe	7 Dec 20	Critical	✓
Weekly Backup	Verify backup settings	Jane Smith	7 Dec 20	High	✗
Penetration Test	Run a full-scope scan	Sam Lee	23 Oct 2020	Medium	✓
Incident Response	Custom build integrity	Mary Johnson	28 Oct 2020	Backup verification	✗
Access Management	Apply least-privilege	Rachel Adams	30 Oct 2020	Ensure all assets	✓
Access Review	Review access control logs	John Doe	20 Oct 2020	Monthly review	✗
Encryption Test	Test encryption protocols	Sam Lee	23 Oct 2020	Security audit	✓
Security Scan	Scan for potential vulnerabilities	Mark Wilson	28 Oct 2020	Critical	✗
Incident Response	Conduct incident drills	Rachel Adams	30 Oct 2020	Full system scan	✓
Access Management Test	Test all services	Jane Smith	8 Nov 20	Review access	✗
Access Management	Review network traffic	Sam Lee	23 Nov 20	Monthly review	✓
Incident Response	Review ongoing risks	John Doe	8 Nov 20	Regularly check	✗

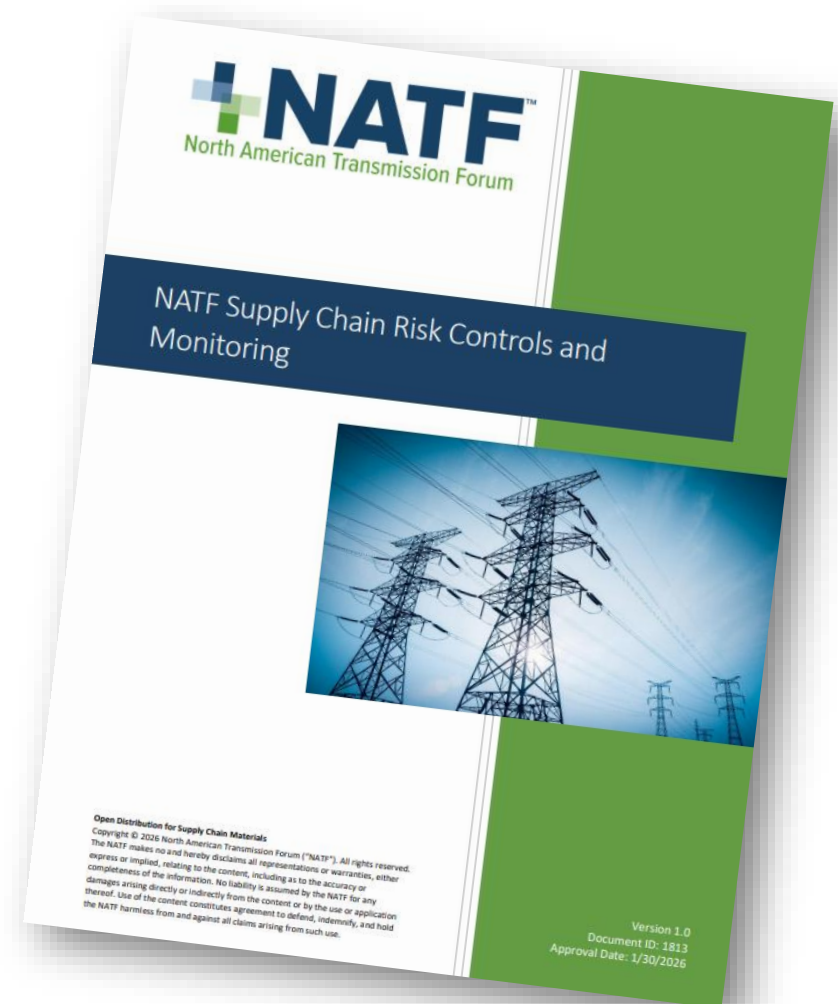


Supply Chain Risk Controls and Monitoring

- Key considerations:
 - Documenting risk determinations

Example below:

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



Questions?



AI-discovered vulnerabilities

Panel discussion

Open Distribution for Supply Chain Materials

Copyright © 2026 North American Transmission Forum (“NATF”). All rights reserved. Presentations are provided with the presenters’ permission for distribution. The NATF makes no and hereby disclaims all representations or warranties, either express or implied, relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use. Further, no liability is assumed for infringement by any presentation materials, artwork, or photographs used in presentations not developed by NATF.

AI Discovered Vulnerabilities



Frank Harrill
Schweitzer
Engineering
Laboratories



Mike Pyle
Schneider Electric



Chris Fitzhugh
Siemens Energy

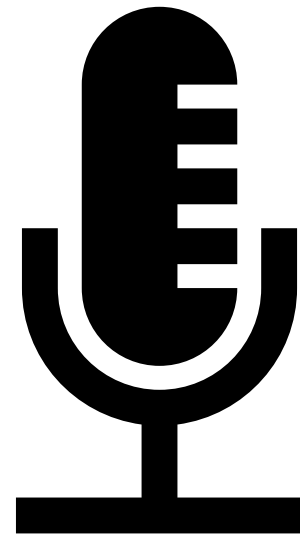


AI Discovered Vulnerabilities

How is artificial intelligence powering vulnerability research and exploitation?

AI Discovered Vulnerabilities

How do you prepare and prioritize?



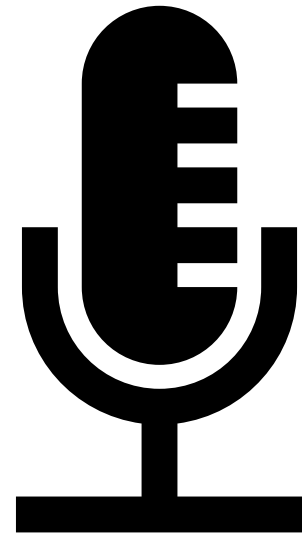
AI Discovered Vulnerabilities

What changes may be needed for patching and mitigation approaches?



AI Discovered Vulnerabilities

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



AI Discovered Vulnerabilities

What does responsible disclosure look like?



AI Discovered Vulnerabilities

Looking ahead, what are your biggest areas of concern?



AI Discovered Vulnerabilities

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



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](#)

