North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Suppliers: Responding to Requests for Cyber Security Information

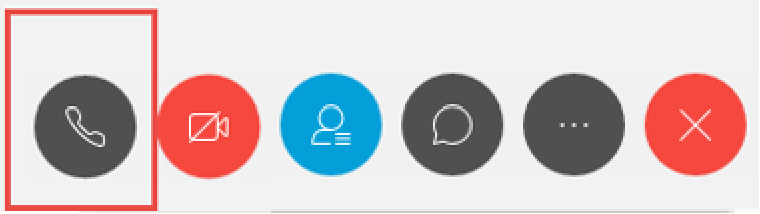
Brought to you by NATF and the Industry Organizations Team

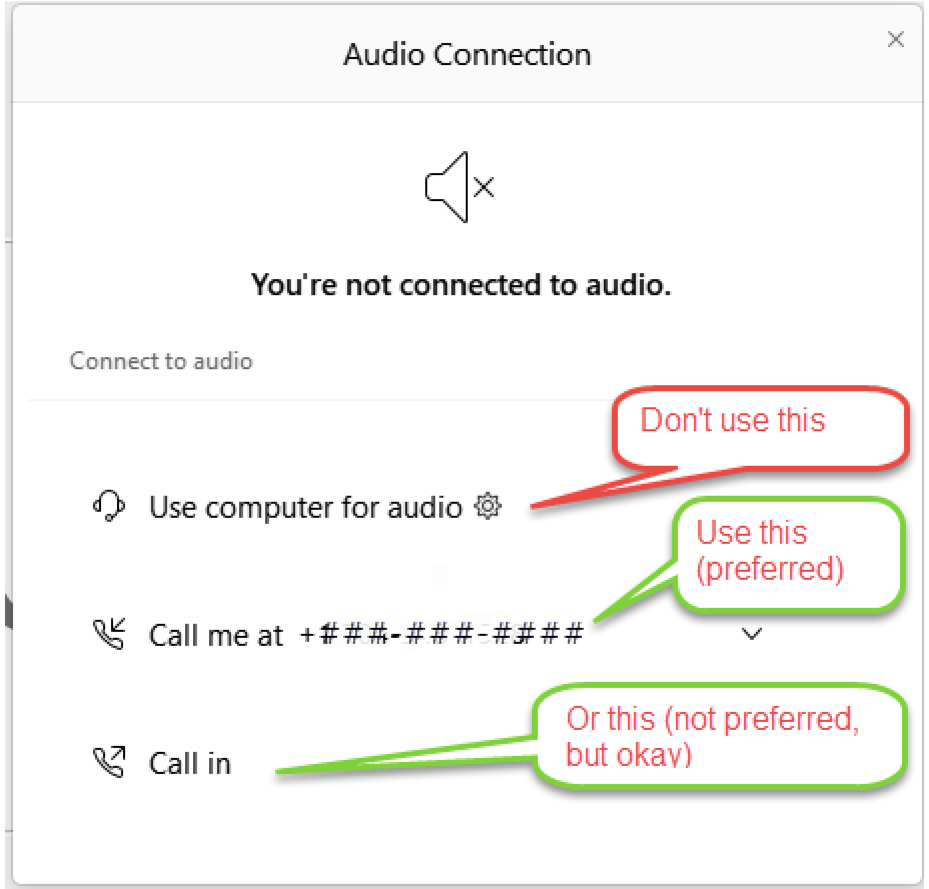
January 12, 2021

Open Distribution

Webex Audio Connection

- Select ☎ to connect to audio
  - Select the “Call me at…” option
  - Don’t select “Use computer for audio” unless you have a headset and are familiar with using a VOIP connection
  - Don’t select “Call in” unless “Call me at…” does not work





Audio Connection

You're not connected to audio.

Connect to audio

Use computer for audio

Call me at +###-###-####

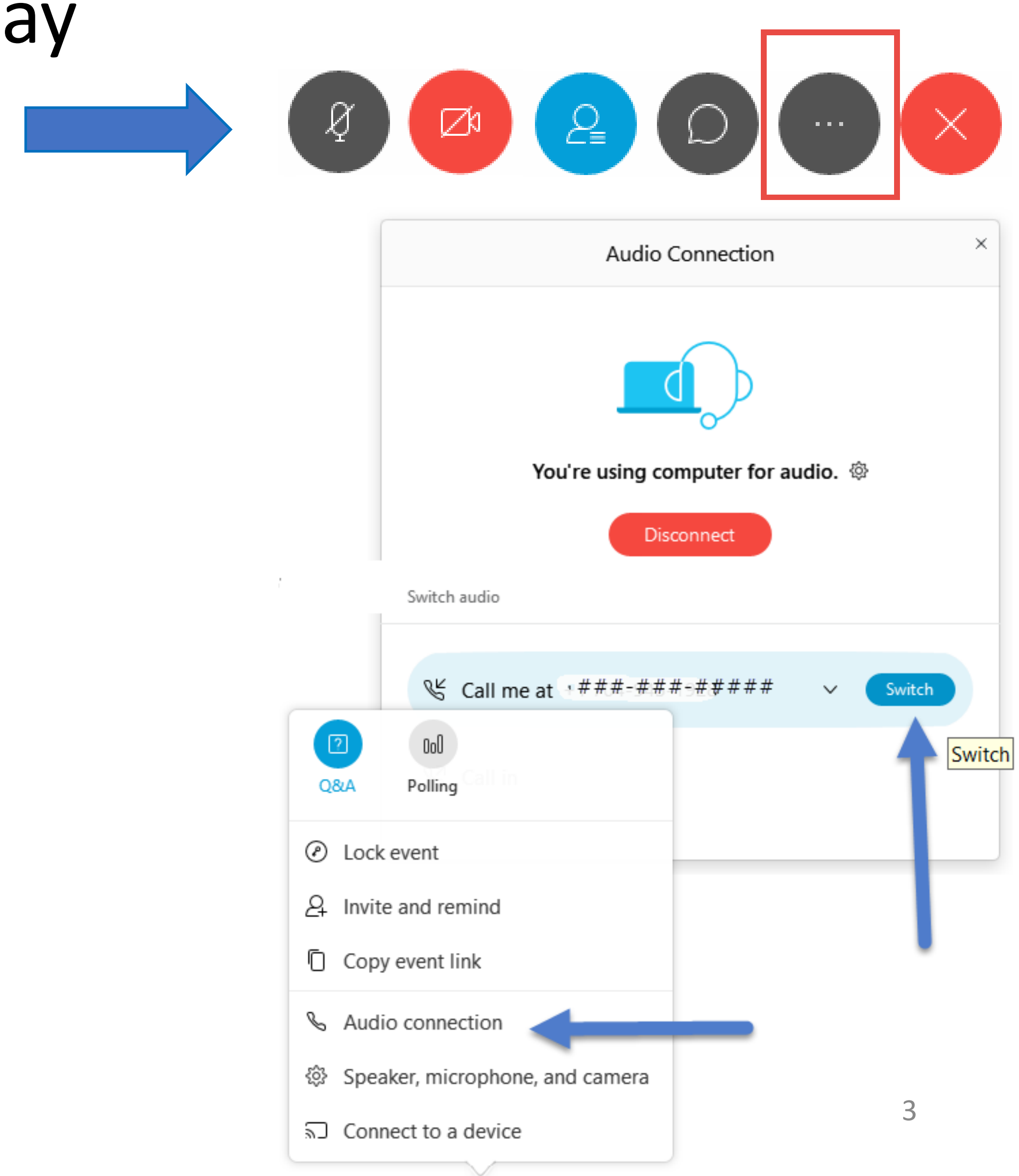
Call in

Don't use this

Use this (preferred)

Or this (not preferred, but okay)

- If you connect to audio the wrong way
  - Select the “More Options” menu
  - Select “Audio connection”
  - Select “Disconnect” or select “Switch” next to “Call me at…”



Audio Connection

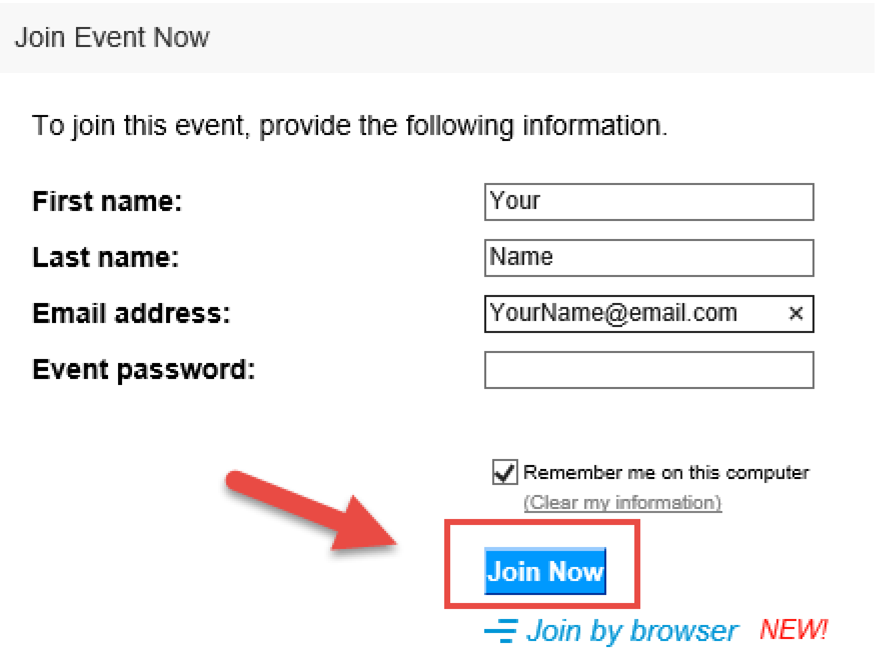
You're using computer for audio.

Switch audio

Call me at ###-###-#####

Raising Your Hand

If you joined using the desktop application (the Join Now button):



Join Event Now

To join this event, provide the following information.

First name: Your

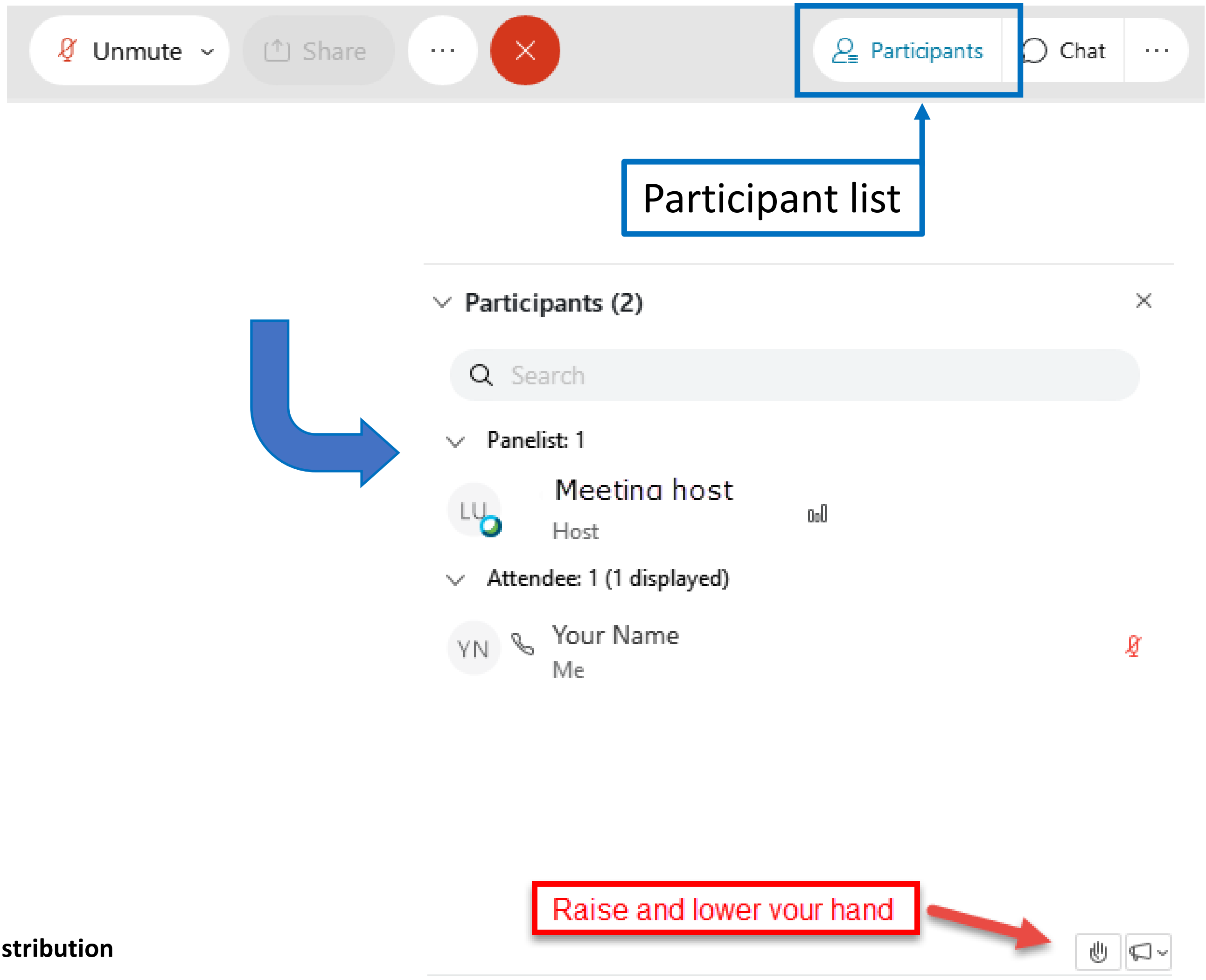
Last name: Name

Email address: YourName@email.com

Event password:

☑ Remember me on this computer

(Clear my information)



Participant list

Participants (2)

Search

Panelist: 1

LU Meeting host
Host

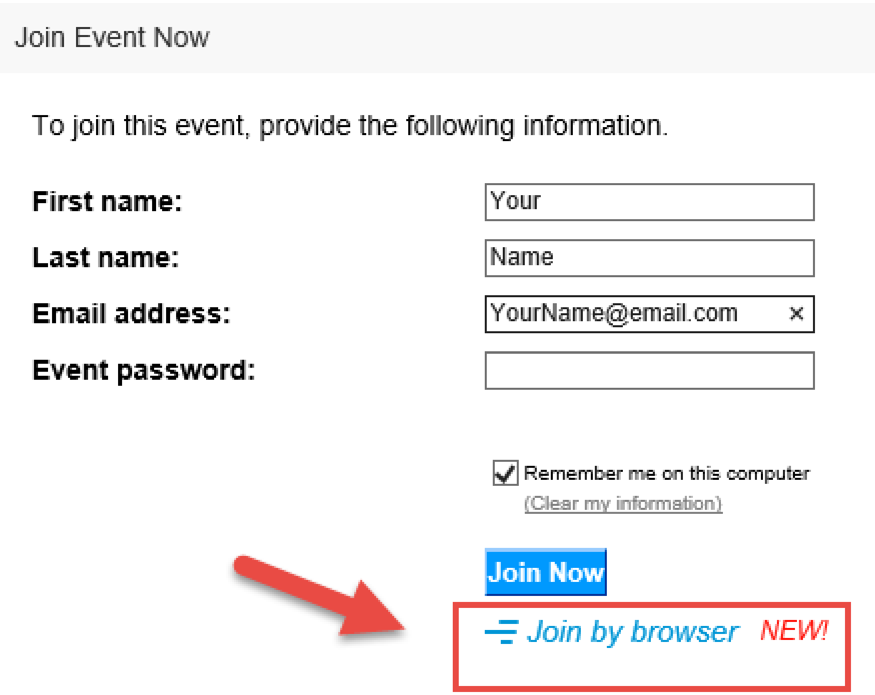
Attendee: 1 (1 displayed)

YN Your Name
Me

Raise and lower your hand

Raising Your Hand

If you joined by browser:



Join Event Now

To join this event, provide the following information.

First name: Your

Last name: Name

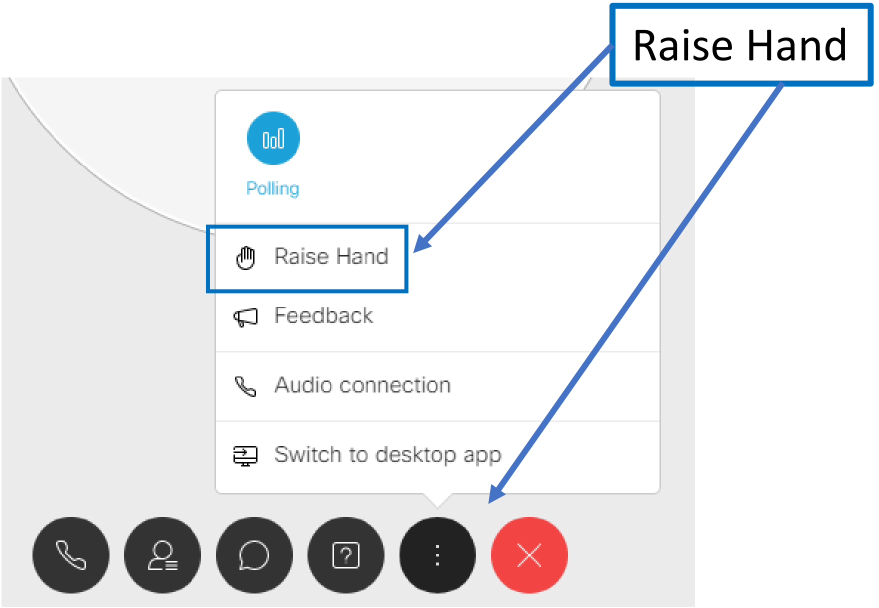
Email address: YourName@email.com ×

Event password:

☑ Remember me on this computer
(Clear my information)

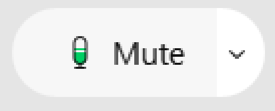
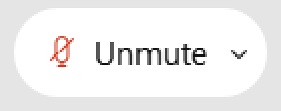
Join Now

Join by browser NEW!



Raise Hand

Audio for Discussion

- We will unmute lines for discussion
- During this time, you'll control your own mute
  - Select  to mute,  to unmute or locally mute on your phone

Agenda Overview

Valerie Agnew (NATF)

- Opening Remarks
- Background and Benefits
- The Industry Organizations Team and Model
- Overview of the Criteria and Questionnaire
- How suppliers can use the Criteria and Questionnaire
- The Revision Process
- Polls

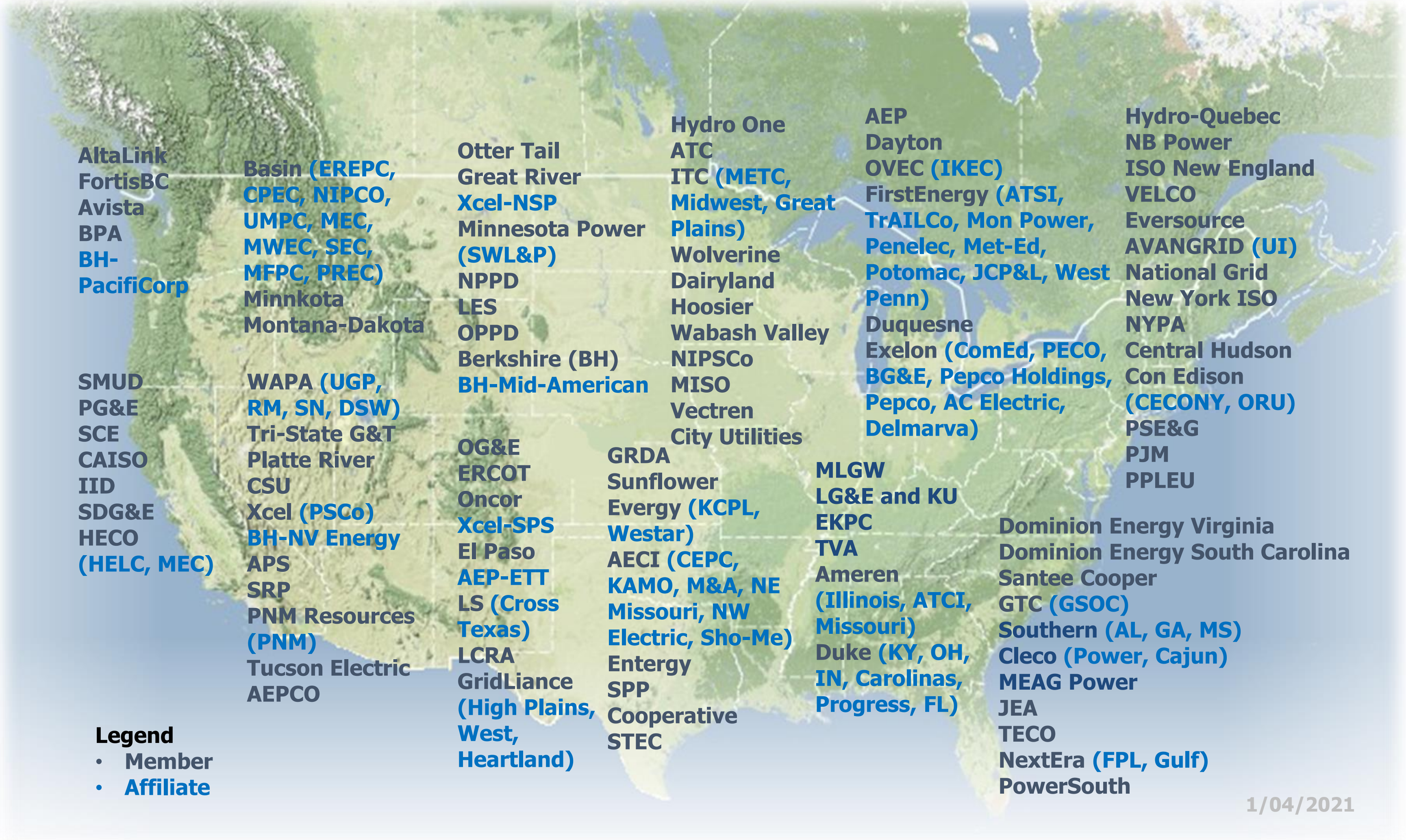
Opening Remarks

Tom Galloway, President and CEO
NATF

Tom Galloway

NATF President and CEO

NATF Members



AltaLink
FortisBC
Avista
BPA
BH-PacifiCorp

SMUD
PG&E
SCE
CAISO
IID
SDG&E
HECO
(HELC, MEC)

Basin (EREPC, CPEC, NIPCO, UMPC, MEC, MWEC, SEC, MFPC, PREC)
Minnkota
Montana-Dakota

WAPA (UGP, RM, SN, DSW)
Tri-State G&T
Platte River
CSU
Xcel (PSCo)
BH-NV Energy
APS
SRP
PNM Resources (PNM)
Tucson Electric
AEPCO

Otter Tail
Great River
Xcel-NSP
Minnesota Power (SWL&P)
NPPD
LES
OPPD
Berkshire (BH)
BH-Mid-American

OG&E
ERCOT
Oncor
Xcel-SPS
El Paso
AEP-ETT
LS (Cross Texas)
LCRA
GridLiance (High Plains, West, Heartland)

Hydro One
ATC
ITC (METC, Midwest, Great Plains)
Wolverine
Dairyland
Hoosier
Wabash Valley
NIPSCo
MISO
Vectren
City Utilities

GRDA
Sunflower
Evergy (KCPL, Westar)
AECI (CEPC, KAMO, M&A, NE Missouri, NW Electric, Sho-Me)
Entergy
SPP
Cooperative
STEC

AEP
Dayton
OVEC (IKEC)
FirstEnergy (ATSI, TrAILCo, Mon Power, Penelec, Met-Ed, Potomac, JCP&L, West Penn)
Duquesne
Exelon (ComEd, PECO, BG&E, Pepco Holdings, Pepco, AC Electric, Delmarva)

MLGW
LG&E and KU
EKPC
TVA
Ameren (Illinois, ATCI, Missouri)
Duke (KY, OH, IN, Carolinas, Progress, FL)

Hydro-Quebec
NB Power
ISO New England
VELCO
Eversource
AVANGRID (UI)
National Grid
New York ISO
NYPA
Central Hudson
Con Edison (CECONY, ORU)
PSE&G
PJM
PPLEU

Dominion Energy Virginia
Dominion Energy South Carolina
Santee Cooper
GTC (GSOC)
Southern (AL, GA, MS)
Cleco (Power, Cajun)
MEAG Power
JEA
TECO
NextEra (FPL, Gulf)
PowerSouth

Legend

- Member
- Affiliate

1/04/2021

94 members

78 affiliates

Member Types
IOUs
Federal/Provincial
Cooperatives
State/Municipal
ISOs/RTOs

Coverage (US/Canada)
~**85%** miles 100 kV+
~**90%** net peak demand

North American Transmission FORUM

Open Distribution

Betsy Soehren-Jones

Exelon

Tony Eddleman

NPPD

Laura Schepis

EEI

Mikhail Falkovich

ConEd

Today's Presenters

Background

Why suppliers are getting requests

Security Heightened by Regulatory Activity

Betsy Soehren-Jones (Exelon)

Entities are more aware of the risks that could be introduced via supply chain

These concerns are heightened by

- The Executive Order 13920 issued on May 1, 2020
  - Associated DOE RFI
  - Associated NERC Alert
- New NERC supply chain regulations that became enforceable on October 1, 2020
- SolarWinds Supply Chain Compromise identified in December 2020
- The DOE Prohibition Order issued on December 17, 2020
  - Associated NERC Alert
- The Executive Order addressing Applications or Software issued January 5, 2020

Collect Information

Government and Regulatory Actions

Betsy Soehren-Jones (Exelon)

Document	Date Released	Link
Executive Order 13920	1-May-20	https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/
DOE Executive Order Information		https://www.energy.gov/oe/bulkpowersystemexecutiveorder
DOE RFI - BPS Executive Order	8-Jul-20	https://www.federalregister.gov/documents/2020/07/08/2020-14668/securing-the-united-states-bulk-power-system
NERC Alert - Supply Chain Risk - III	8-Jul-20	https://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx
DOE Prohibition Order	17-Dec-20	https://www.energy.gov/sites/prod/files/2020/12/f81/BPS%20EO%20Prohibition%20Order%20Securing%20Critical%20Defense%20Facilities%2012.17.20%20-%20SIGNED.pdf
DOE Prohibition Order Information		https://www.energy.gov/articles/secretary-energy-signs-order-mitigate-security-risks-nations-electric-grid
NERC Alert - Supply Chain Risk	20-Dec-20	https://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx
FERC NOI - Equipment and Services	17-Sep-20	https://www.federalregister.gov/documents/2020/09/23/2020-20987/equipment-and-services-produced-or-provided-by-certain-entities-identified-as-risks-to-national
FERC White Paper - Cyber Security Incentives	18-Jun-20	https://www.ferc.gov/sites/default/files/2020-06/notice-cybersecurity.pdf
FERC NOI - CIP Enhancements	24-Jun-20	https://www.federalregister.gov/documents/2020/06/24/2020-13618/potential-enhancements-to-the-critical-infrastructure-protection-reliability-standards

Coming Together to Address Concerns Benefits Suppliers

Betsy Soehren-Jones (Exelon)

Inclusivity

- The Model is based on inclusivity of all suppliers
- Designed to help you and your customers identify risks
- You can work with your customers to mitigate those risks

Efficiency and Effectiveness

- When your customers are asking the same questions, you can be prepared with
  - Responses
  - Verification for your responses
- Making your customers satisfied and confident

Tony Eddleman (NPPD)

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

NATF and the Industry Organizations Team

Formed Fall 2019

Industry Organization Team Members

Tony Eddleman (NPPD)

Organizations, Forums and Working Groups

- AGA
- CEA
- EEI
- LPPC
- APPA
- TAPS
- NAGF
- NAESB
- ConEd Working Group
- NERC CCC/RSTC/SCWG
- NRECA

Suppliers

- Hitachi ABB Power Grids
- GE Grid Software Solutions
- OSI
- Siemens Industry, Inc.
- Schneider Electric
- Schweitzer Engineering

Third-Party Assessors

- Ernst & Young
- KPMG LLP
- PWC
- Deloitte

Organizations providing support products or services

- EPRI
- Fortress/A2V
- KY3P
- UL

Laura Schepis (EEI)

Electricity Subsector

ESCC

Electricity Subsector
Coordinating Council

Tony Eddleman (NPPD)

Objectives

Security

- Identifying and addressing cyber security risks introduced via supply chain

Industry Convergence

- Achieve industry convergence on the approach (Model) to facilitate addressing the following objectives

Efficiency and Effectiveness

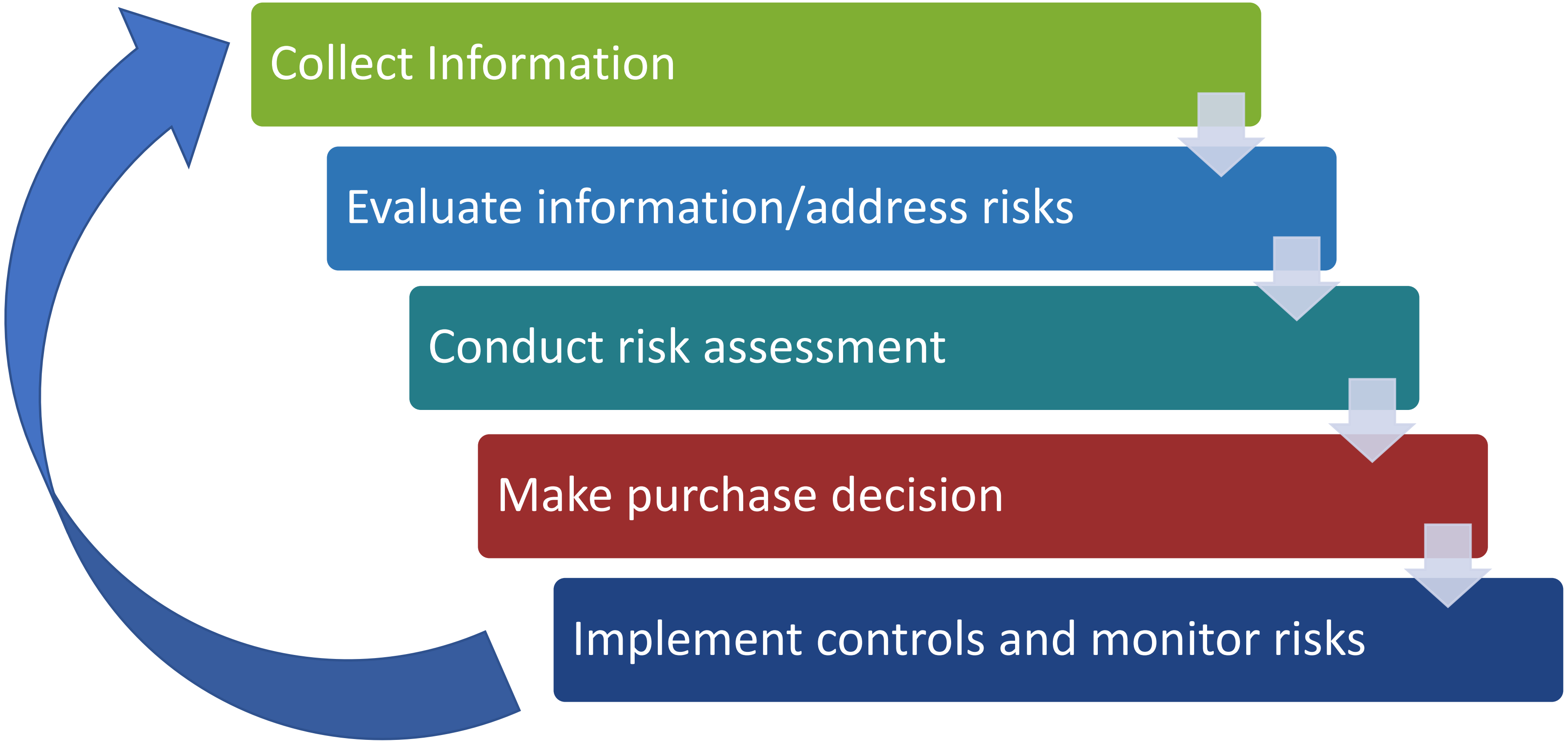
- Convergence on common approaches to achieve reasonable assurance of suppliers' security practices

Compliance

- Implementation guidance to meet supply chain related CIP standards (CIP-013-1; CIP-005-6 R2.4; CIP-010-3 R1.6)

Tony Eddleman (NPPD)

Supplier Assessment Model Process Overview



Collect Information

Evaluate information/address risks

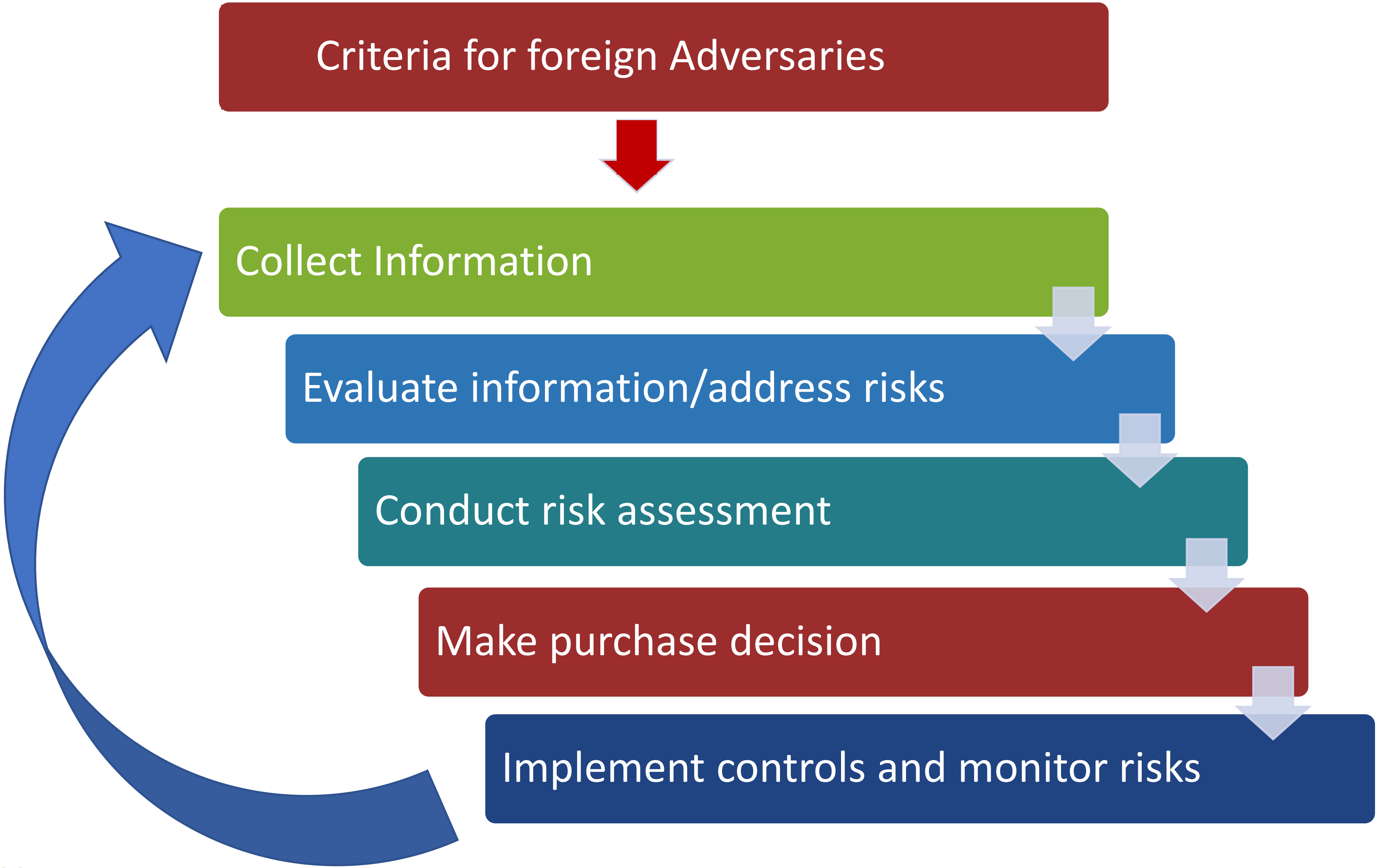
Conduct risk assessment

Make purchase decision

Implement controls and monitor risks

Possible Assessment Process with EO Criteria

Tony Eddleman (NPPD)



Criteria for foreign Adversaries

Collect Information

Evaluate information/address risks

Conduct risk assessment

Make purchase decision

Implement controls and monitor risks

Customers Collecting Information

Tony Eddleman (NPPD)

Collect it from Suppliers themselves

- NATF Cyber Security Criteria for Suppliers
- Energy Sector Supply Chain Questionnaire
- Supplement with
  - Historical knowledge
  - Open-source research

Use a solution-provider service

Also need to verify or obtain assurance of accuracy

Collect Information

Methods Customers May Use to Obtain Assurance of Accuracy

Tony Eddleman (NPPD)

Third-party Assessments

- *Obtain a qualified assessors' third-party assessment, certification and/or independent audit that addresses NATF Criteria and Questionnaire*

Obtain a validation/verification from a solution provider

- *Solution-provider risk assessments*
- *Shared assessments*

Conduct their own validation/verification

- *Obtain evidence from supplier to conduct your own validation/verification*

Collect Information

Available Today

Tony Eddleman (NPPD)

NATF Criteria

- 60 Criteria for suppliers’ supply chain cyber security practices
- 24 Organization Information considerations

Energy Sector Supply Chain Risk Questionnaire

- 223 cyber security questions
- 20 general information questions

Supplier Assessment Model

- Model for assessing suppliers’ cyber security practices

EEI Procurement Language

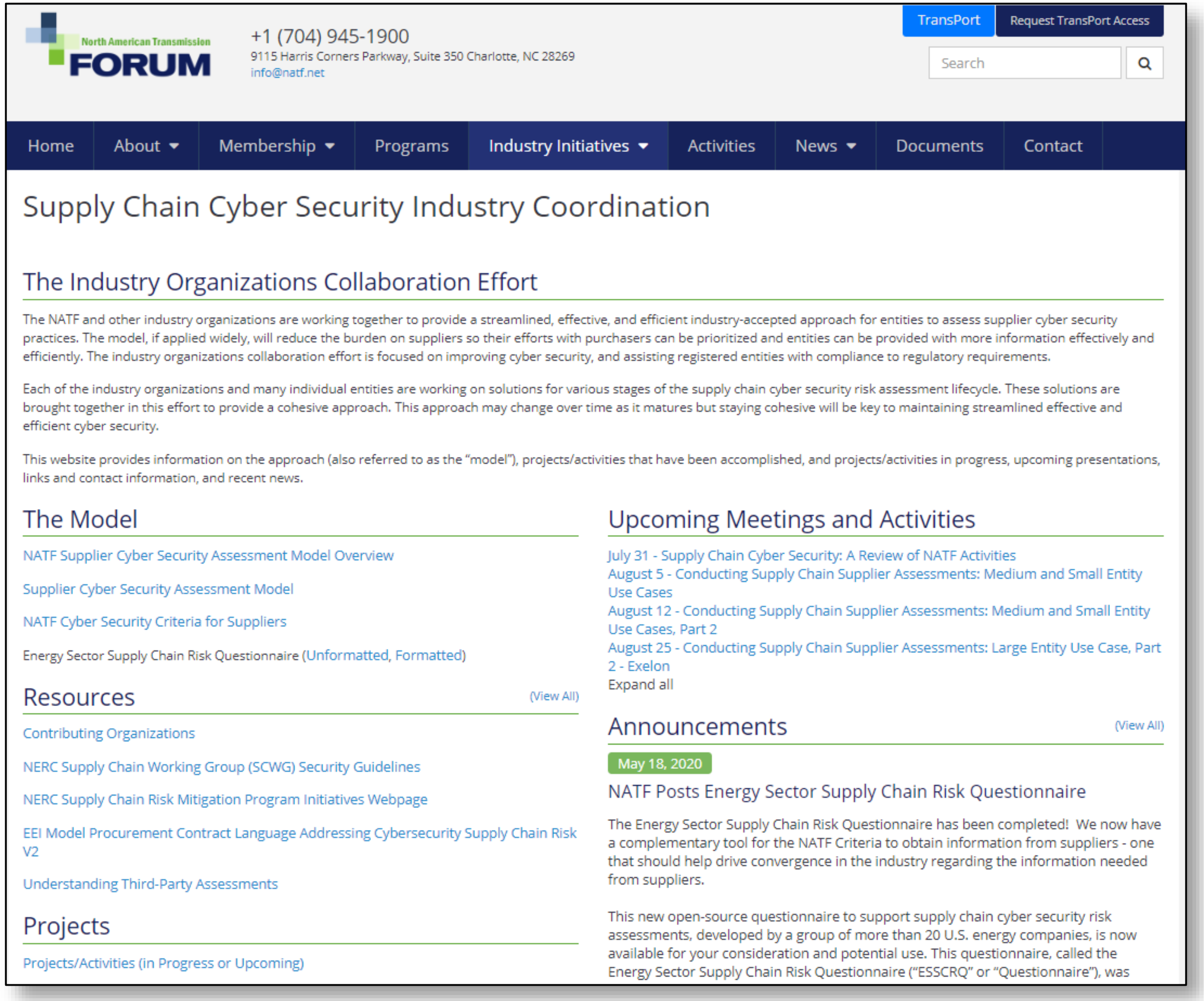
- Sample contract language to mitigate risk and provide assurances of supplier performance

Other

- Presentations
- Additional Resources

NATF-hosted Industry Organizations Web Page

Tony Eddleman (NPPD)



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

Supply Chain Cyber Security 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

NATF Supplier Cyber Security Assessment Model Overview

Supplier Cyber Security Assessment Model

NATF Cyber Security Criteria for Suppliers

Energy Sector Supply Chain Risk Questionnaire (Unformatted, Formatted)

Resources

(View All)

Contributing Organizations

NERC Supply Chain Working Group (SCWG) Security Guidelines

NERC Supply Chain Risk Mitigation Program Initiatives Webpage

EEI Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk V2

Understanding Third-Party Assessments

Projects

Projects/Activities (in Progress or Upcoming)

Upcoming Meetings and Activities

July 31 - Supply Chain Cyber Security: A Review of NATF Activities
August 5 - Conducting Supply Chain Supplier Assessments: Medium and Small Entity Use Cases
August 12 - Conducting Supply Chain Supplier Assessments: Medium and Small Entity Use Cases, Part 2
August 25 - Conducting Supply Chain Supplier Assessments: Large Entity Use Case, Part 2 - Exelon
Expand all

Announcements

(View All)

May 18, 2020

NATF Posts Energy Sector Supply Chain Risk Questionnaire

The Energy Sector Supply Chain Risk Questionnaire has been completed! We now have a complementary tool for the NATF Criteria to obtain information from suppliers - one that should help drive convergence in the industry regarding the information needed from suppliers.

This new open-source questionnaire to support supply chain cyber security risk assessments, developed by a group of more than 20 U.S. energy companies, is now available for your consideration and potential use. This questionnaire, called the Energy Sector Supply Chain Risk Questionnaire ("ESSCRQ" or "Questionnaire"), was

Tony Eddleman (NPPD)

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Overview of the NATF Criteria and Questionnaire

What you can expect to see

North American Transmission
FORUM

Tony Eddleman (NPPD)

The NATF Criteria

Available on the NATF Public Website:

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

Criteria for Evaluations: The NATF Criteria

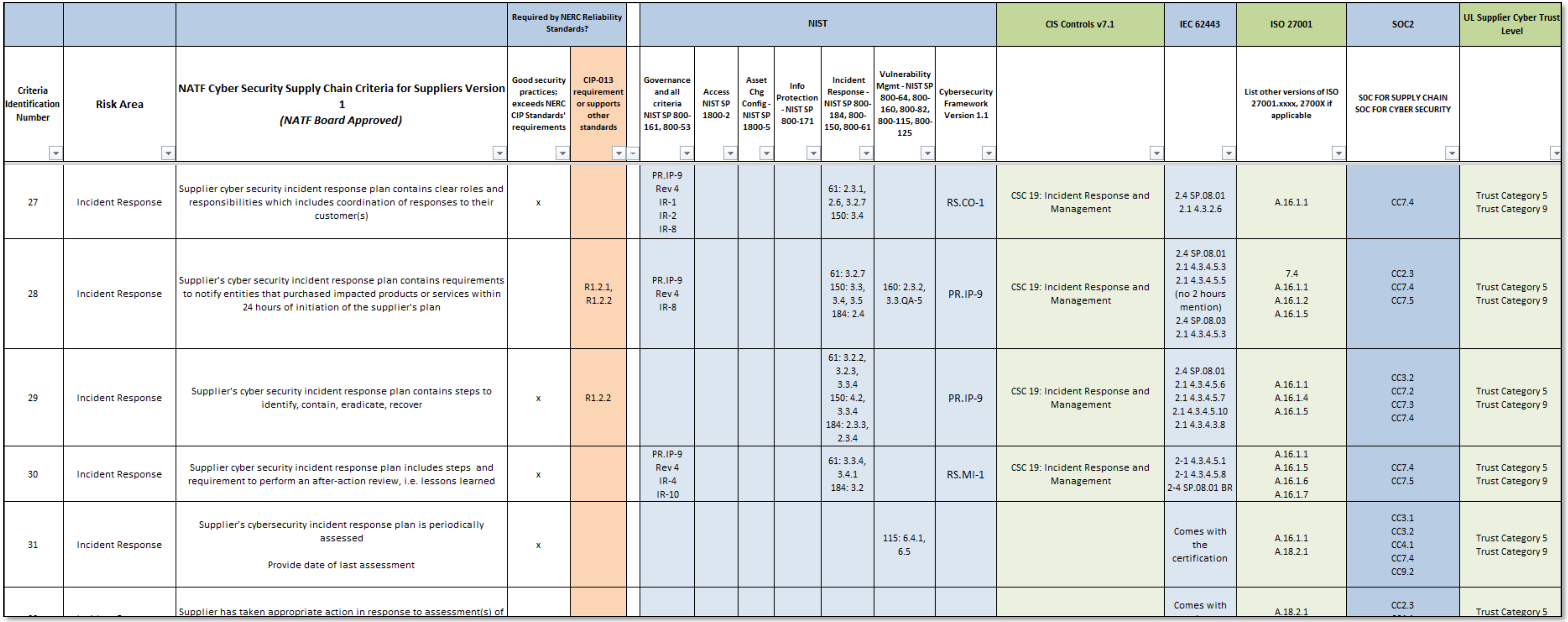
Tony Eddleman (NPPD)

What is the criteria or security framework?

- Posted on the NATF Public Website
- 60 criteria for supplier supply chain cyber security practices within 6 Risk Areas:
    - Asset Control and Mgmt
    - Asset, Change and Configuration Mgmt
    - Governance
    - Incident Response
    - Information Protection
    - Vulnerability Mgmt
- 24 organizational information considerations
- Maps to existing frameworks

Tony Eddleman (NPPD)

NATF Criteria Spreadsheet: Criteria



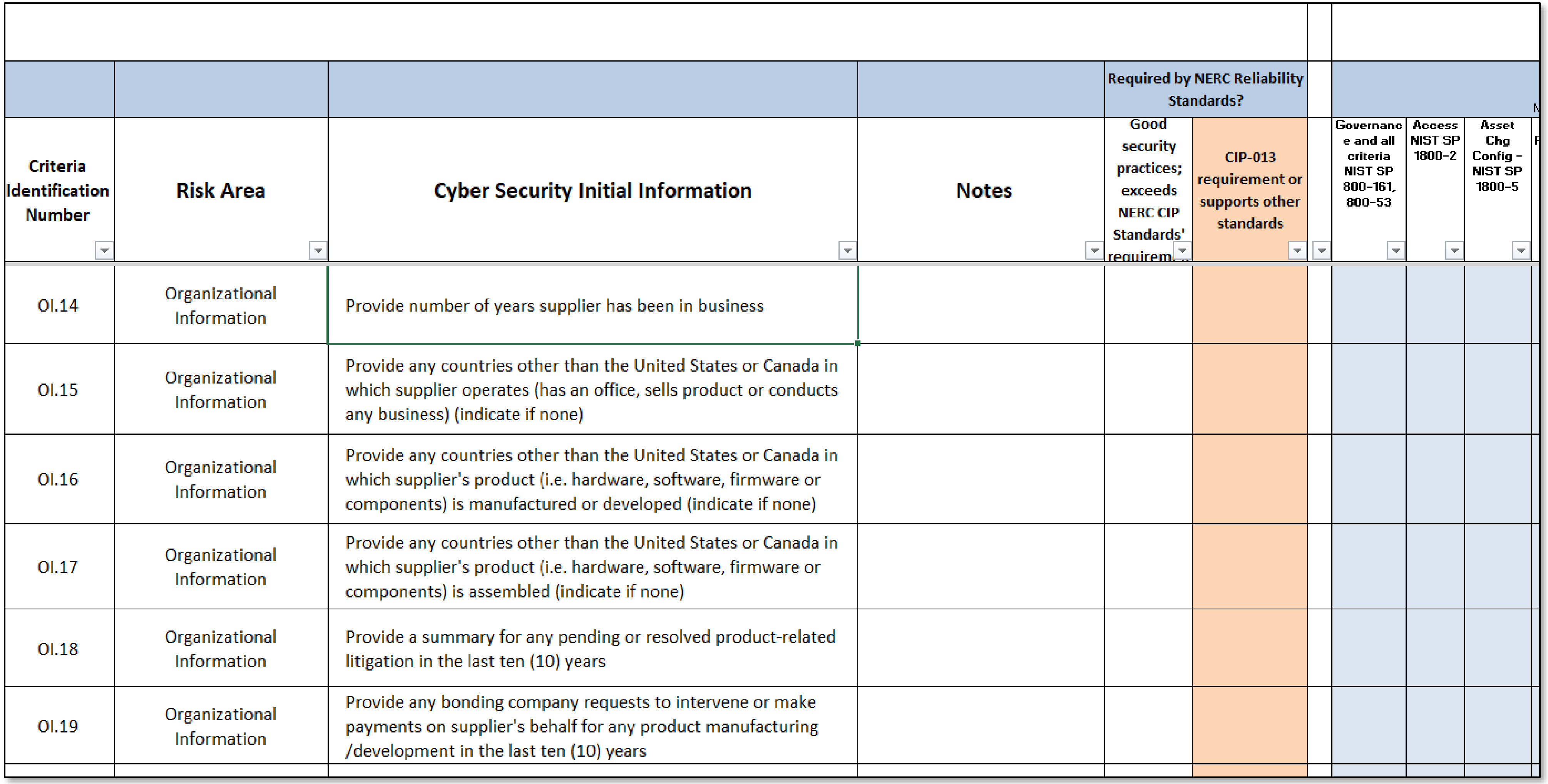
			Required by NERC Reliability Standards?			NIST							CIS Controls v7.1	IEC 62443	ISO 27001	SOC2	UL Supplier Cyber Trust Level
Criteria Identification Number	Risk Area	NATF Cyber Security Supply Chain Criteria for Suppliers Version 1 *(NATF Board Approved)*	Good security practices; exceeds NERC CIP Standards' 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, 2700X if applicable	SOC FOR SUPPLY CHAIN SOC FOR CYBER SECURITY	
27	Incident Response	Supplier cyber security incident response plan contains clear roles and responsibilities which includes coordination of responses to their customer(s)	x			PR.IP-9 Rev 4 IR-1 IR-2 IR-8				61: 2.3.1, 2.6, 3.2.7 150: 3.4		RS.CO-1	CSC 19: Incident Response and Management	2.4 SP.08.01 2.1 4.3.2.6	A.16.1.1	CC7.4	Trust Category 5 Trust Category 9
28	Incident Response	Supplier's cyber security incident response plan contains requirements to notify entities that purchased impacted products or services within 24 hours of initiation of the supplier's plan		R1.2.1, R1.2.2		PR.IP-9 Rev 4 IR-8				61: 3.2.7 150: 3.3, 3.4, 3.5 184: 2.4	160: 2.3.2, 3.3.QA-5	PR.IP-9	CSC 19: Incident Response and Management	2.4 SP.08.01 2.1 4.3.4.5.3 2.1 4.3.4.5.5 (no 2 hours mention) 2.4 SP.08.03 2.1 4.3.4.5.3	7.4 A.16.1.1 A.16.1.2 A.16.1.5	CC2.3 CC7.4 CC7.5	Trust Category 5 Trust Category 9
29	Incident Response	Supplier's cyber security incident response plan contains steps to identify, contain, eradicate, recover	x	R1.2.2						61: 3.2.2, 3.2.3, 3.3.4 150: 4.2, 3.3.4 184: 2.3.3, 2.3.4		PR.IP-9	CSC 19: Incident Response and Management	2.4 SP.08.01 2.1 4.3.4.5.6 2.1 4.3.4.5.7 2.1 4.3.4.5.10 2.1 4.3.4.3.8	A.16.1.1 A.16.1.4 A.16.1.5	CC3.2 CC7.2 CC7.3 CC7.4	Trust Category 5 Trust Category 9
30	Incident Response	Supplier cyber security incident response plan includes steps and requirement to perform an after-action review, i.e. lessons learned	x			PR.IP-9 Rev 4 IR-4 IR-10				61: 3.3.4, 3.4.1 184: 3.2		RS.MI-1	CSC 19: Incident Response and Management	2-1 4.3.4.5.1 2-1 4.3.4.5.8 2-4 SP.08.01 BR	A.16.1.1 A.16.1.5 A.16.1.6 A.16.1.7	CC7.4 CC7.5	Trust Category 5 Trust Category 9
31	Incident Response	Supplier's cybersecurity incident response plan is periodically assessed Provide date of last assessment	x								115: 6.4.1, 6.5			Comes with the certification	A.16.1.1 A.18.2.1	CC3.1 CC3.2 CC4.1 CC7.4 CC9.2	Trust Category 5 Trust Category 9
		Supplier has taken appropriate action in response to assessment(s) of												Comes with	A.18.2.1	CC2.3	Trust Category 5

North American Transmission FORUM

Open Distribution

NATF Criteria Spreadsheet: Organizational Information

Tony Eddleman (NPPD)



				Required by NERC Reliability Standards?						N
Criteria Identification Number	Risk Area	Cyber Security Initial Information	Notes	Good security practices; exceeds NERC CIP Standards' requirem...	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	F
OI.14	Organizational Information	Provide number of years supplier has been in business								
OI.15	Organizational Information	Provide any countries other than the United States or Canada in which supplier operates (has an office, sells product or conducts any business) (indicate if none)								
OI.16	Organizational Information	Provide any countries other than the United States or Canada in which supplier's product (i.e. hardware, software, firmware or components) is manufactured or developed (indicate if none)								
OI.17	Organizational Information	Provide any countries other than the United States or Canada in which supplier's product (i.e. hardware, software, firmware or components) is assembled (indicate if none)								
OI.18	Organizational Information	Provide a summary for any pending or resolved product-related litigation in the last ten (10) years								
OI.19	Organizational Information	Provide any bonding company requests to intervene or make payments on supplier's behalf for any product manufacturing /development in the last ten (10) years								

North American Transmission FORUM

Open Distribution

North American Transmission
FORUM

Mikhail Falkovich (ConEd)

The Energy Sector
Supply Chain Risk Questionnaire
“The Questionnaire”

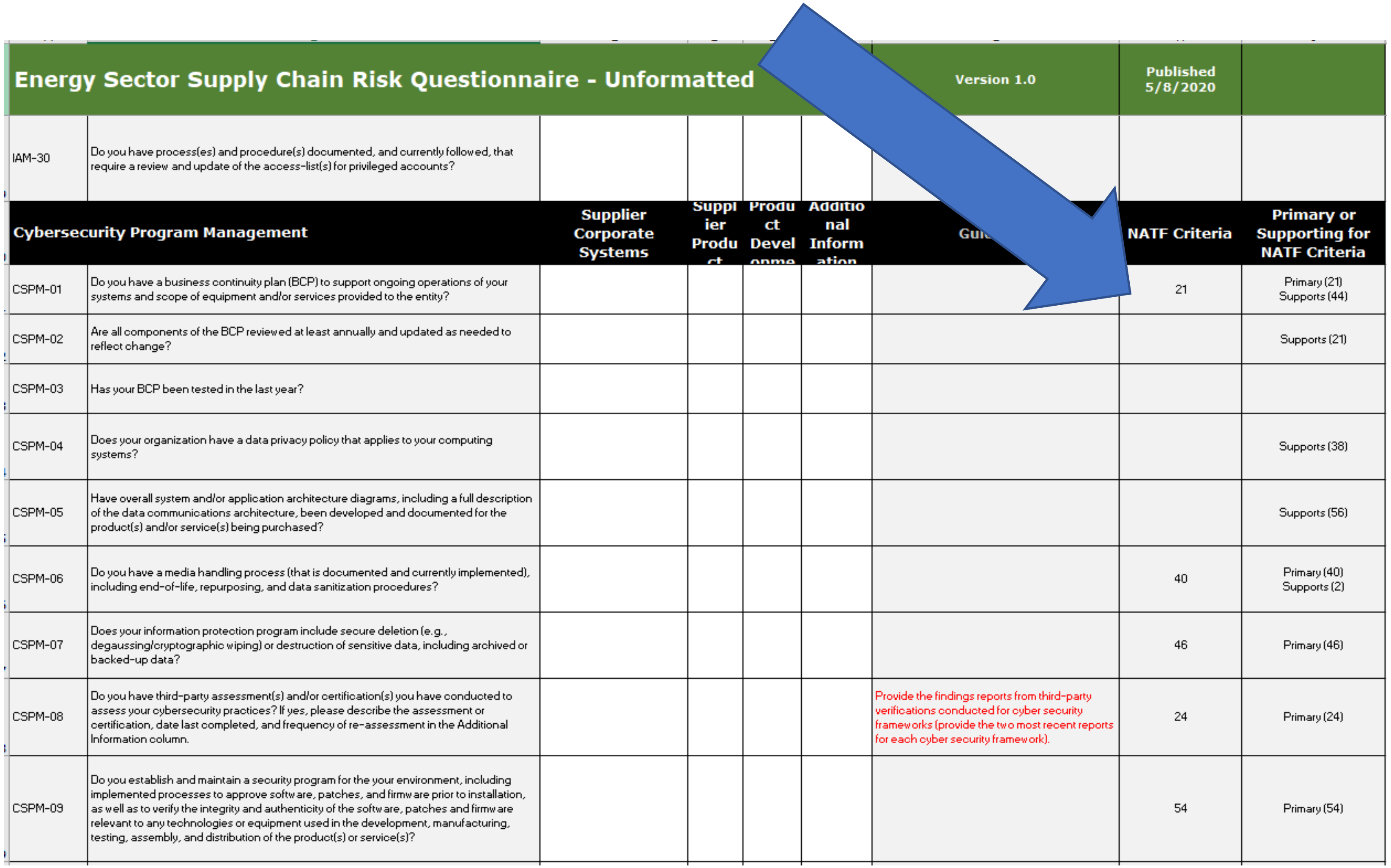
Available on the NATF Public Website:

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

Questionnaire Mapping

Mikhail Falkovich (ConEd)

- To the NATF Criteria
  - All questions provide support information for the NATF Criteria; the key supporting questions are identified
- To existing frameworks/ standards



Energy Sector Supply Chain Risk Questionnaire - Unformatted						Version 1.0	Published 5/8/2020	
IAM-30	Do you have process(es) and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?							
Cybersecurity Program Management		Supplier Corporate Systems	Supplier Product	Product Developme	Additional Information	Gui	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 entity?						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?						40	Primary (40) Supports (2)
CSPM-07	Does your information protection program include secure deletion (e.g., degaussing/cryptographic wiping) or destruction of sensitive data, including archived or backed-up data?						46	Primary (46)
CSPM-08	Do you have third-party assessment(s) and/or certification(s) you have conducted to assess your cybersecurity practices? If yes, please describe the assessment or certification, date last completed, and frequency of re-assessment in the Additional Information column.					Provide the findings reports from third-party verifications conducted for cyber security frameworks (provide the two most recent reports for each cyber security framework).	24	Primary (24)
CSPM-09	Do you establish and maintain a security program for the your environment, including implemented processes to approve software, patches, and firmware prior to installation, as well as to verify the integrity and authenticity of the software, patches and firmware relevant to any technologies or equipment used in the development, manufacturing, testing, assembly, and distribution of the product(s) or service(s)?						54	Primary (54)

Questionnaire Overview

Mikhail Falkovich (ConEd)

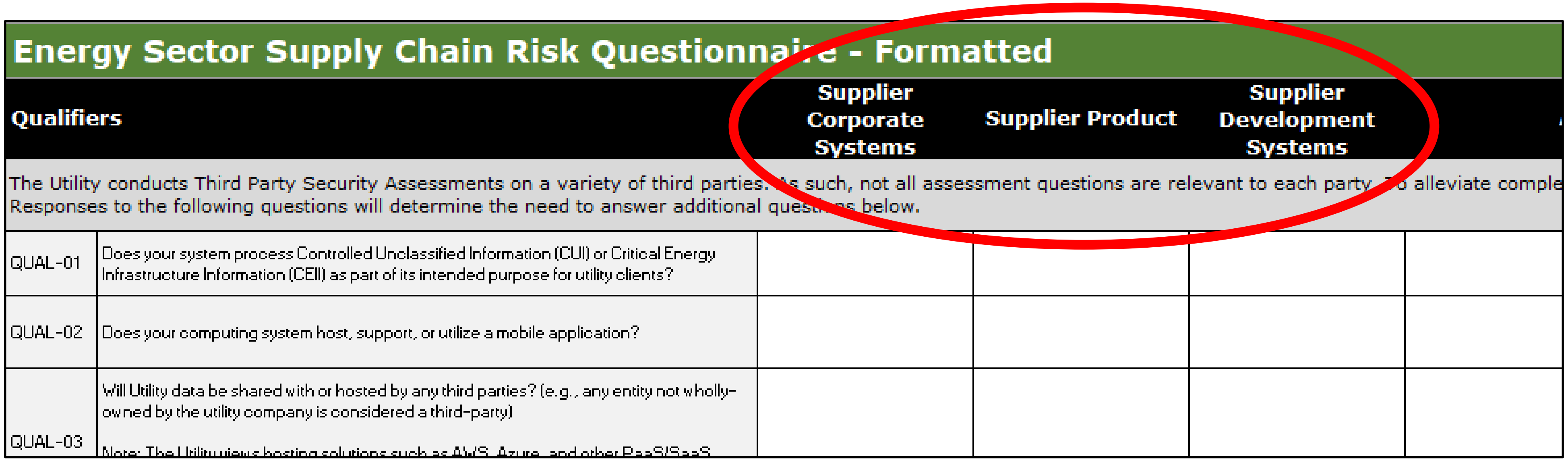
- Posted on the NATF Public Website
- Formatted and Unformatted versions
- 223 Questions plus 20 General Information questions
- Twelve categories:

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

Questions for three areas

Mikhail Falkovich (ConEd)

- Supplier Corporate Systems
- Supplier Product
- Supplier Development Systems



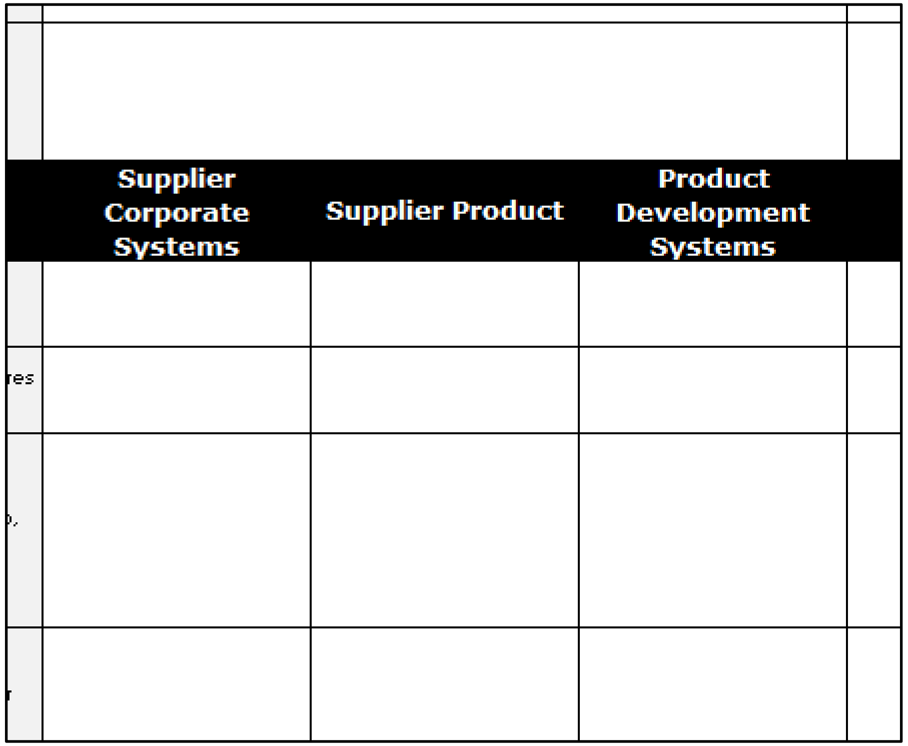
Energy Sector Supply Chain Risk Questionnaire - Formatted

Qualifiers		Supplier Corporate Systems	Supplier Product	Supplier Development Systems	
The Utility conducts Third Party Security Assessments on a variety of third parties. As such, not all assessment questions are relevant to each party. To alleviate comple Responses to the following questions will determine the need to answer additional questions below.					
QUAL-01	Does your system process Controlled Unclassified Information (CUI) or Critical Energy Infrastructure Information (CEII) as part of its intended purpose for utility clients?				
QUAL-02	Does your computing system host, support, or utilize a mobile application?				
QUAL-03	Will Utility data be shared with or hosted by any third parties? (e.g., any entity not wholly-owned by the utility company is considered a third-party) Note: The Utility views hosting solutions such as AWS, Azure, and other PaaS/SaaS				

Completing the Questionnaire

Mikhail Falkovich (ConEd)

- Complete questions for Supplier Corporate Systems (yes/no/free form)
- Determine whether responses to Corporate Systems applies to Product
  - If yes, indicate yes, no or “same as CS”
  - If not, respond to Product questions
- Determine whether responses to either Corporate Systems or Product applies to the Product Development system
  - If yes, indicate yes, no or “same as CS, or same as P” for free-form questions
  - If not, respond to Product Development System questions



Supplier Corporate Systems	Supplier Product	Product Development Systems

Betsy Soehren-Jones (Exelon)

Use of the NATF Criteria and Questionnaire

Betsy Soehren-Jones (Exelon)

Supplier's Use

- ***Have responses prepared for the NATF Criteria and Questionnaire***
- ***Determine what verification you will provide***
  - A third-party verification
  - Evidence to support responses
  - Suggest the use of a solution provider
- ***If you don't have responses prepared***
  - Ask if the customer would start with responses to the NATF Criteria
  - See what are the most critical responses customer needs
  - Ask if the customer is using a gate system, so you could provide some responses now and some at a later point in time

Collect Information

Betsy Soehren-Jones (Exelon)

Customers’ needs may vary

- Customers may not need responses to all the questions; it depends upon how each company is conducting risk assessments
- We are working with companies to encourage them to tell you:
  - ***All*** – if they need responses to all criteria and/or questions
  - ***All, but in stages*** – they will need responses to all the criteria and questions, but they will be requesting them in stages (i.e., they may be using a “gate” system)
  - ***Some*** - If they don’t need responses to all, they should add a column for indicating the criteria and/or questions they want responses to, or use the formatted questionnaire filters
    - This will help you recognize that they are using the Criteria and the Questionnaire, so you can use your developed responses
    - They may ask, or you can determine, whether it is more efficient to just provide all the responses
  - ***Additional or modified*** - If they want additional or modified information, those criteria or questions should be provided in an addendum. We are asking entities ***not to modify the Criteria or questions in the Questionnaire***

North American Transmission

FORUM

Community *Confidentiality* *Candor* *Commitment*

Mikhail Falkovich (ConEd)

The Revision Process for the NATF Criteria and Questionnaire

Mikhail Falkovich (ConEd)

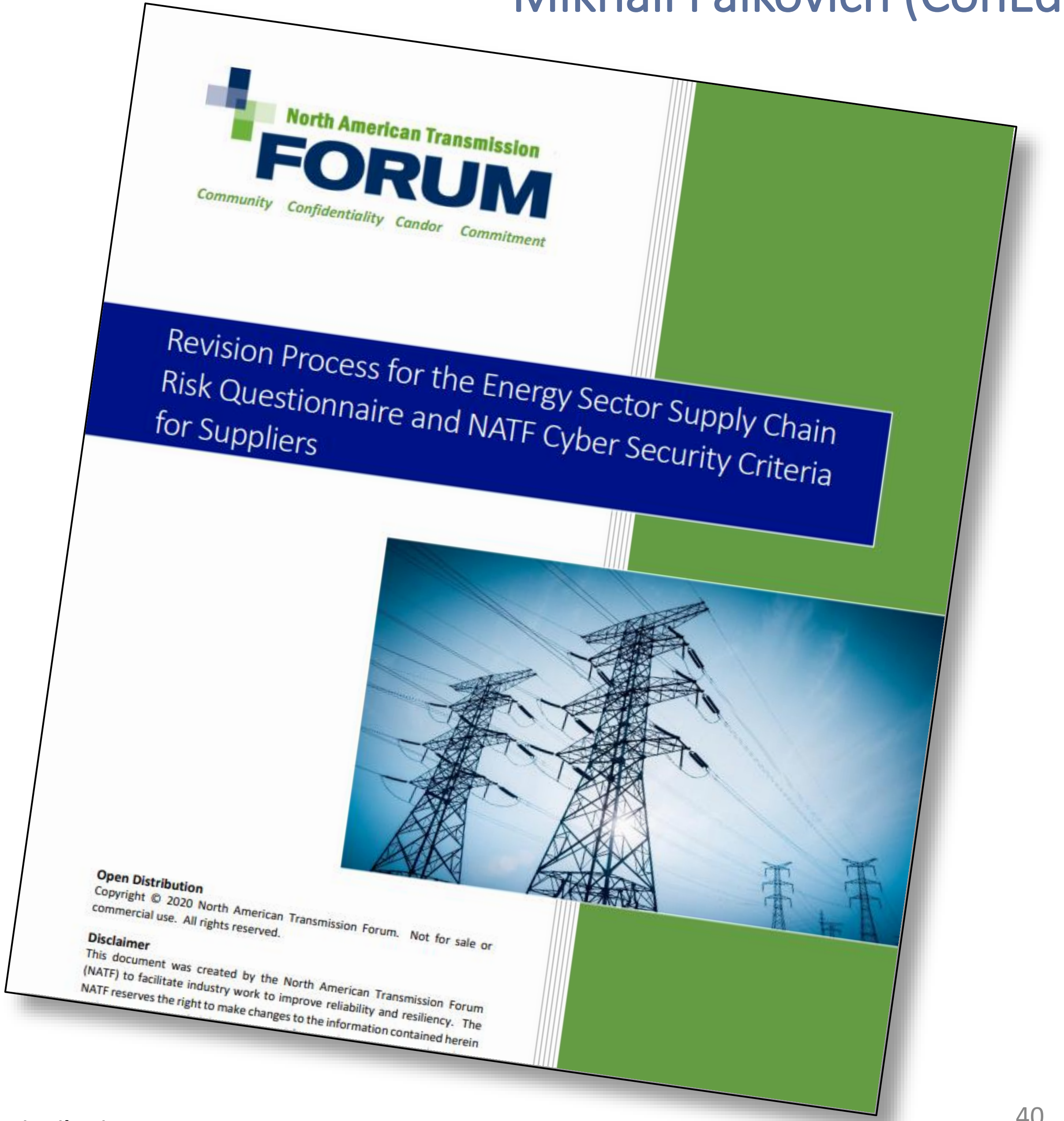
Industry Convergence

- Aligning industry on the information
  - that is being asked of suppliers and
  - is used when conducting risk assessments
- Suppliers can participate in the review process
- **Provide feedback to:**
  - supplychain@natf.net

Collect Information

The Revision Process

- Approved by the NATF Board
- Industry-wide process; NATF resources to maintain



North American Transmission FORUM

Community Confidentiality Candor Commitment

Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Cyber Security Criteria for Suppliers

Open Distribution

Copyright © 2020 North American Transmission Forum. Not for sale or commercial use. All rights reserved.

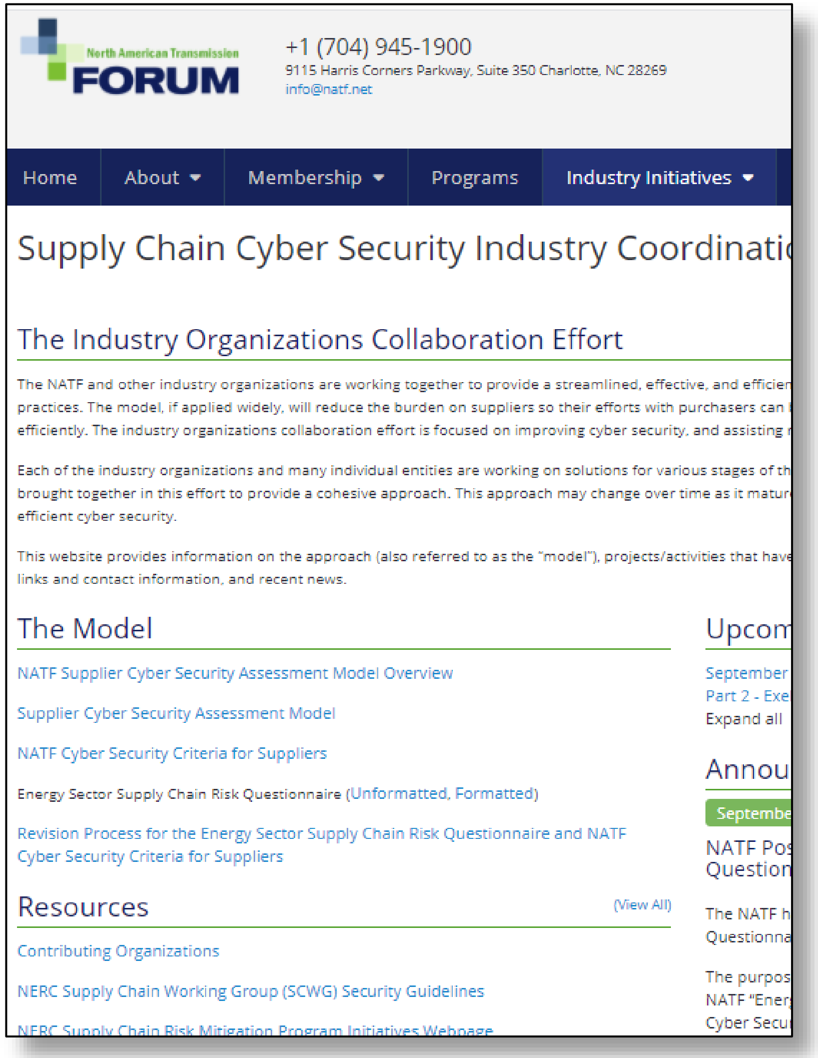
Disclaimer

This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve reliability and resiliency. The NATF reserves the right to make changes to the information contained herein

Mikhail Falkovich (ConEd)

The Revision Process

- Is posted on the NATF public website/Industry Coordination page https://www.natf.net/industry-initiatives/supply-chain-industry-coordination



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

Supply Chain Cyber Security Industry Coordinati

The Industry Organizations Collaboration Effort

The NATF and other industry organizations are working together to provide a streamlined, effective, and efficien
practices. The model, if applied widely, will reduce the burden on suppliers so their efforts with purchasers can
efficiently. The industry organizations collaboration effort is focused on improving cyber security, and assisting

Each of the industry organizations and many individual entities are working on solutions for various stages of th
brought together in this effort to provide a cohesive approach. This approach may change over time as it matur
efficient cyber security.

This website provides information on the approach (also referred to as the "model"), projects/activities that have
links and contact information, and recent news.

The Model

NATF Supplier Cyber Security Assessment Model Overview

Supplier Cyber Security Assessment Model

NATF Cyber Security Criteria for Suppliers

Energy Sector Supply Chain Risk Questionnaire (Unformatted, Formatted)

Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Cyber Security Criteria for Suppliers

Resources (View All)

Contributing Organizations

NERC Supply Chain Working Group (SCWG) Security Guidelines

NERC Supply Chain Risk Mitigation Program Initiatives Webpage

Upcom

September
Part 2 - Exe
Expand all

Annou

Septembe

NATF Pos
Question

The NATF h
Questionna

The purpos
NATF "Ener
Cyber Secu

The Revision Process

Mikhail Falkovich (ConEd)

The Criteria and Questionnaire will be updated annually

- January/February – Review team reviews inputs
- March – A redlined version is posted for 30 days for industry comments
- April/May - Review team reviews and addresses comments
- May
  - Revised Criteria and Questionnaire are posted on the NATF public Industry Coordination webpage
  - The Review Team provides communication to industry

Mikhail Falkovich (ConEd)

NATF Contact Information

supplychain@natf.net

kkeels@natf.net

vagnew@natf.net

Was today helpful?

Valerie Agnew (NATF)

Was this introduction to the NATF Criteria and Questionnaire helpful?

A. Yes

B. No

C. I need more information

Would you be interested in another webinar to interact with the suppliers that have been involved?

Valerie Agnew (NATF)

Would you be interested in a future webinar to hear from and interact with the suppliers on the Industry Organizations' Team?

A. Yes
B. No
C. Maybe

Would you be interested in another webinar to interact with the solution providers that have been involved?

Valerie Agnew (NATF)

Would you be interested in a future webinar to hear from and interact with the solution providers on the Industry Organizations' Team?

A. Yes
B. No
C. Maybe

Thank you for attending!

Valerie Agnew (NATF)

North American Transmission FORUM