North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

NATF Criteria and ESSCR Questionnaire: Overview, Use, and Revision Process

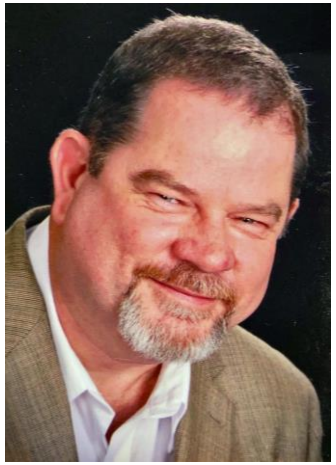
October 2, 2020

Open Distribution

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

Agenda Overview

- Background
- Overview of the Criteria and Questionnaire
- How to use the Criteria and Questionnaire
- The Revision Process
- Questions/Discussion



Chuck Abell

Ameren

Jack Cashin

APPA

Dina Mangialino

ConEd

Mikhail Falkovich

ConEd

Betsy Soehren-Jones

Exelon

Tony Eddleman

NPPD

Today’s Presenters - Industry

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Sam Chanoski

Hitachi-ABB

Rob Koziy

OSI

Tobias Whitney

Fortress A2V

Today’s Supplier and Solution Provider Presenters

Tony Eddleman (NPPD)

Purpose of Today's Webinar and Background

Tony Eddleman (NPPD)

Encourage Industry Convergence

Tony Eddleman (NPPD)

Benefits of Industry Convergence

- Obtain the information you need and use
- Suppliers providing responses
  - Suppliers are gathering information for all of the questions in the questionnaire
  - Readily available for you

Collect Information

Industry Organization Team Members

Tony Eddleman (NPPD)

Organizations, Forums and Working Groups

- AGA
- CEA
- EEI
- LPPC
- APPA
- TAPS
- NAGF
- NAESB
- ConEd Working Group
- SCWG/CIPC
- 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

Val Agnew (NATF)

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

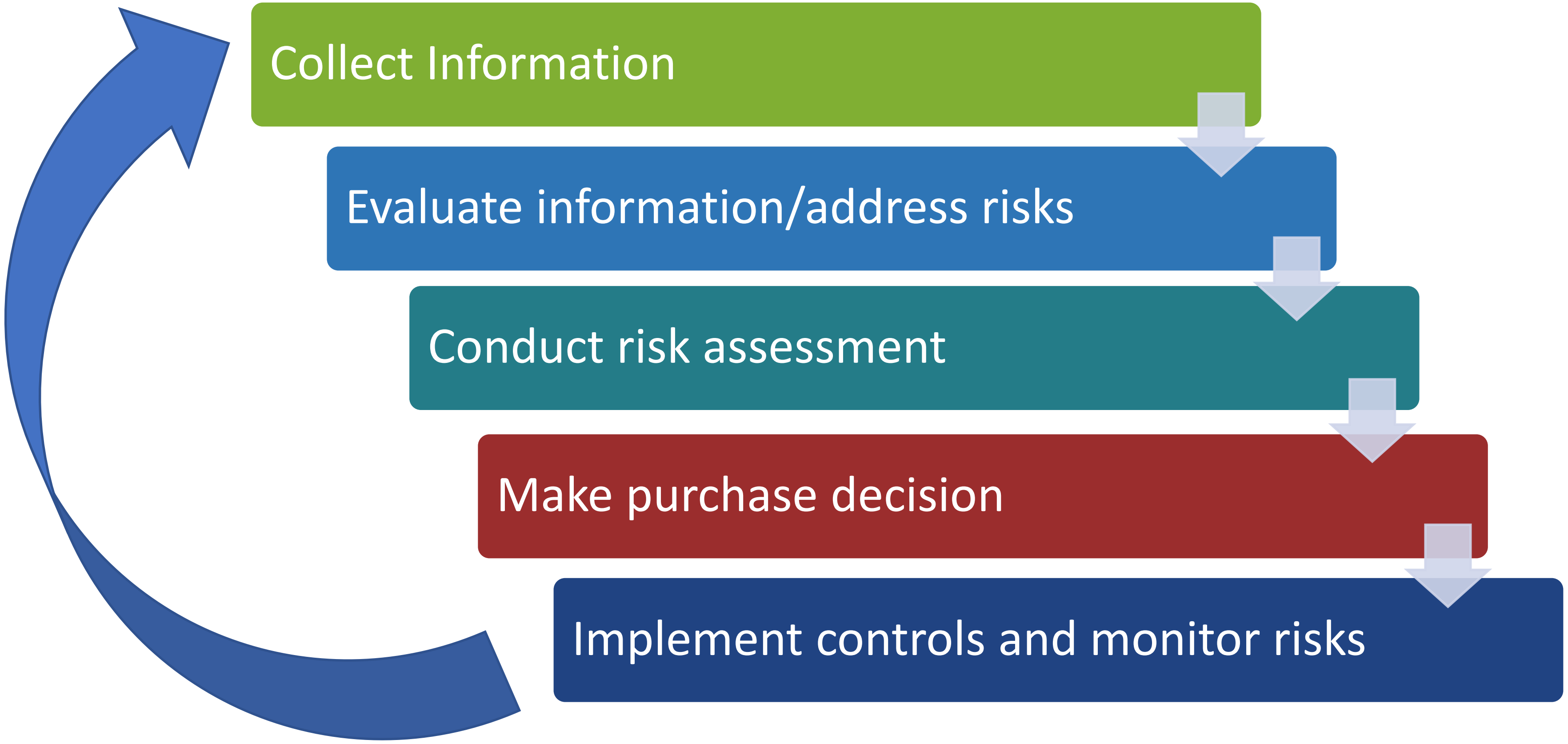
- Convergence on common approaches to achieve reasonable assurance of suppliers' security practices

Compliance

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

Val Agnew (NATF)

Supplier Assessment Model Process Overview



Collect Information

Evaluate information/address risks

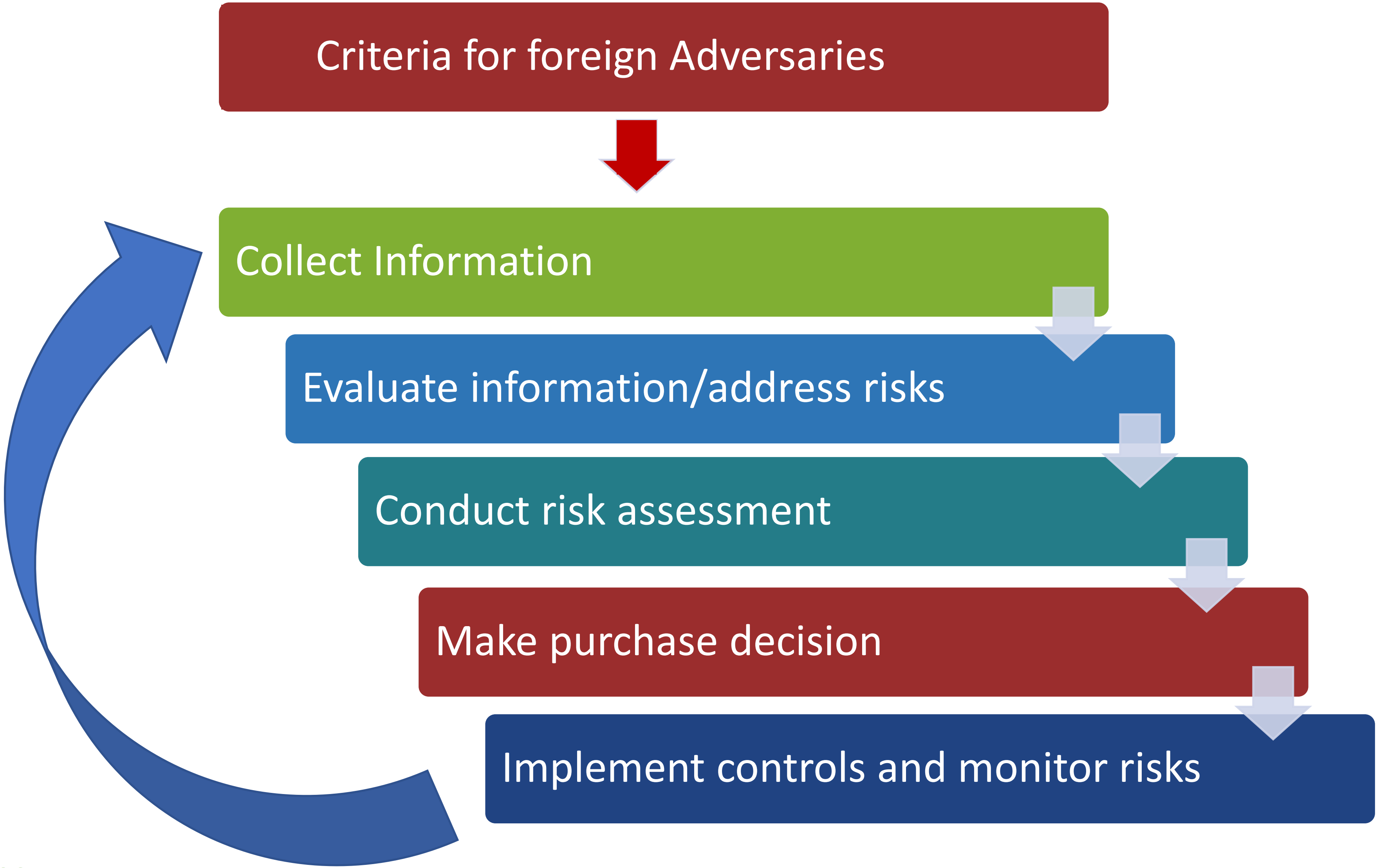
Conduct risk assessment

Make purchase decision

Implement controls and monitor risks

Possible Assessment Process with EO Criteria

Val Agnew (NATF)



Criteria for foreign Adversaries

Collect Information

Evaluate information/address risks

Conduct risk assessment

Make purchase decision

Implement controls and monitor risks

Val Agnew (NATF)

Collect Information

- **Collect it yourself**
  - – NATF Cyber Security Criteria for Suppliers
  - – Energy Sector Supply Chain Questionnaire
  - – Supplement with
    - Historical knowledge
    - Open source research
- **Use a solution-provider service**

Collect Information

Val Agnew (NATF)

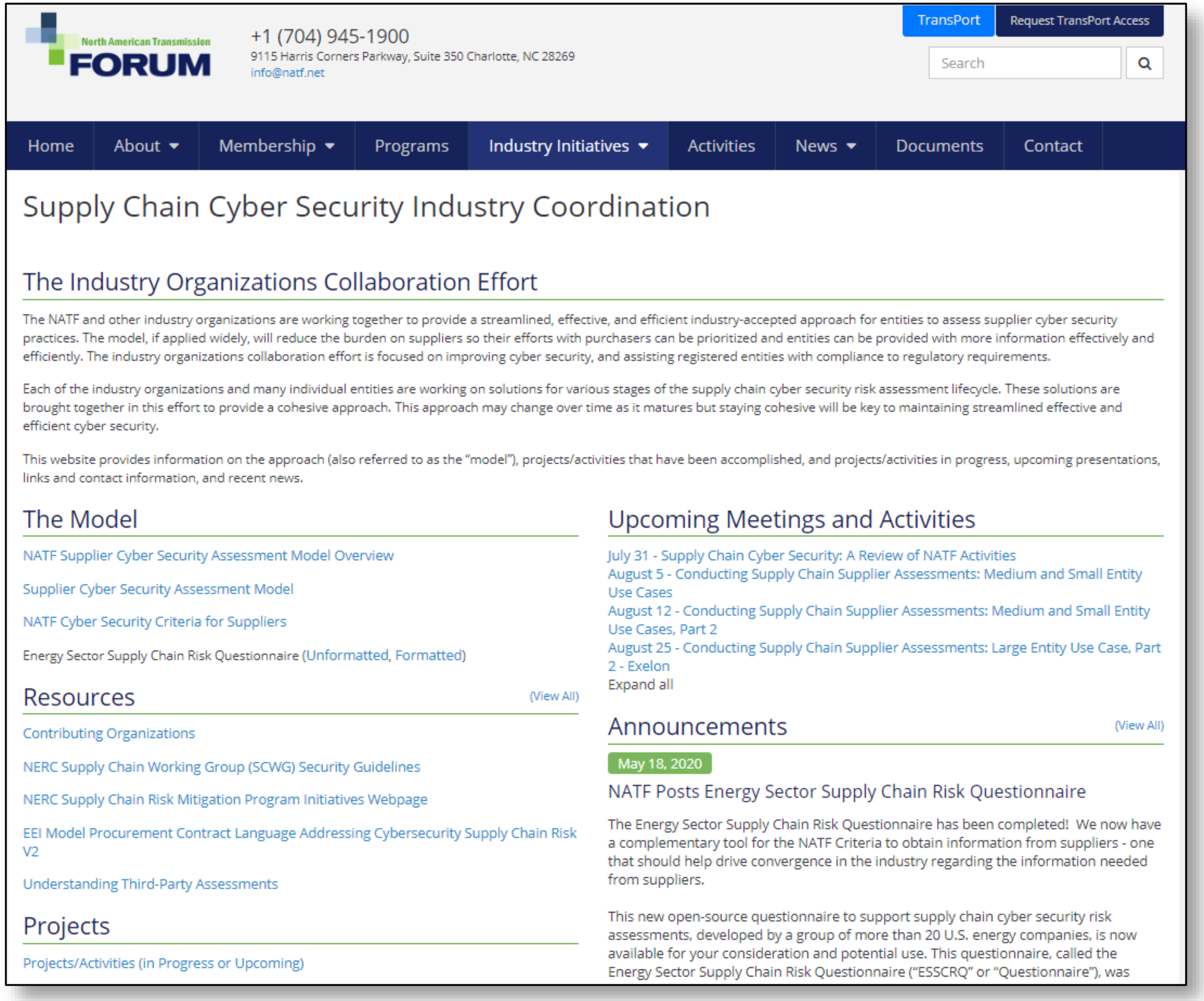
Methods to Obtain Assurance of Accuracy

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

Collect Information

Val Agnew (NATF)

NATF-hosted Industry Organizations Web Page



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

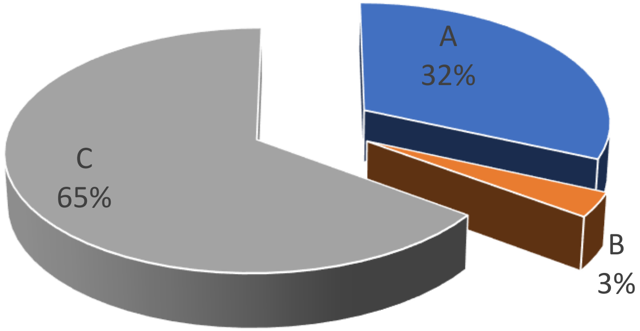
Participoll Question!

What function are you with in your organization?

A. Cyber Security
B. Procurement
C. Compliance

Vote Now!

https://natfvote.participoll.com/



60

Val Agnew (NATF)

Participoll question!

How are you currently collecting information from suppliers?

A. NATF Criteria

B. NATF Questionnaire

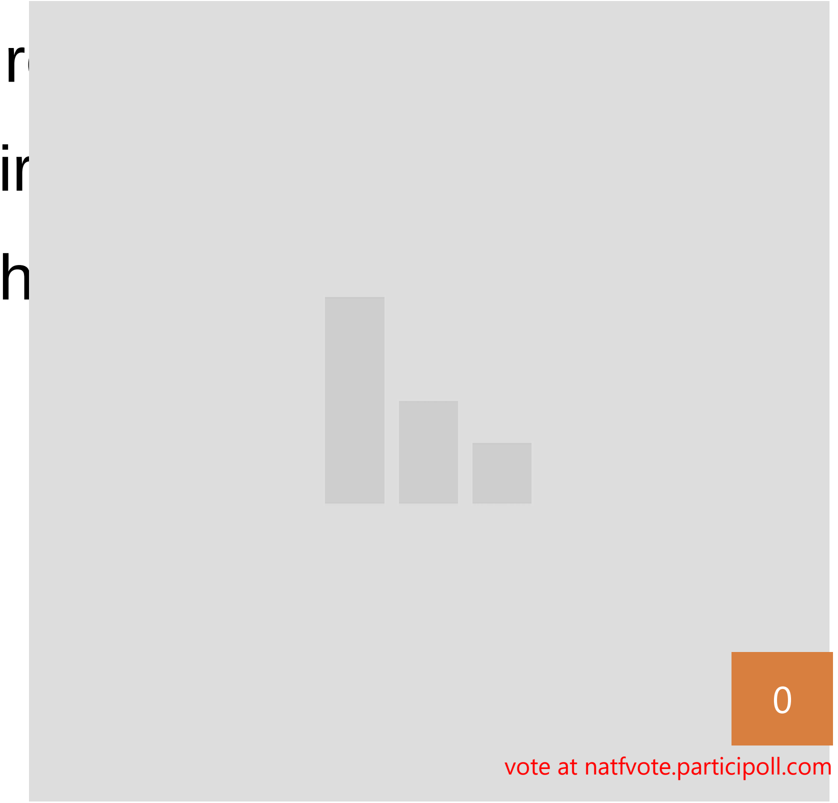
C. Modified NATF Criteria

D. Modified NATF Questionnair

E. My own custom questionnair

F. I use a solution provider with their questions

G. I use a solution provider to collect the Criteria and Questionnaire information



Vote Now!

https://natfvote.participoll.com/

North American Transmission FORUM

Val Agnew (NATF)

Open Questions

Overview of the Criteria and Questionnaire

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

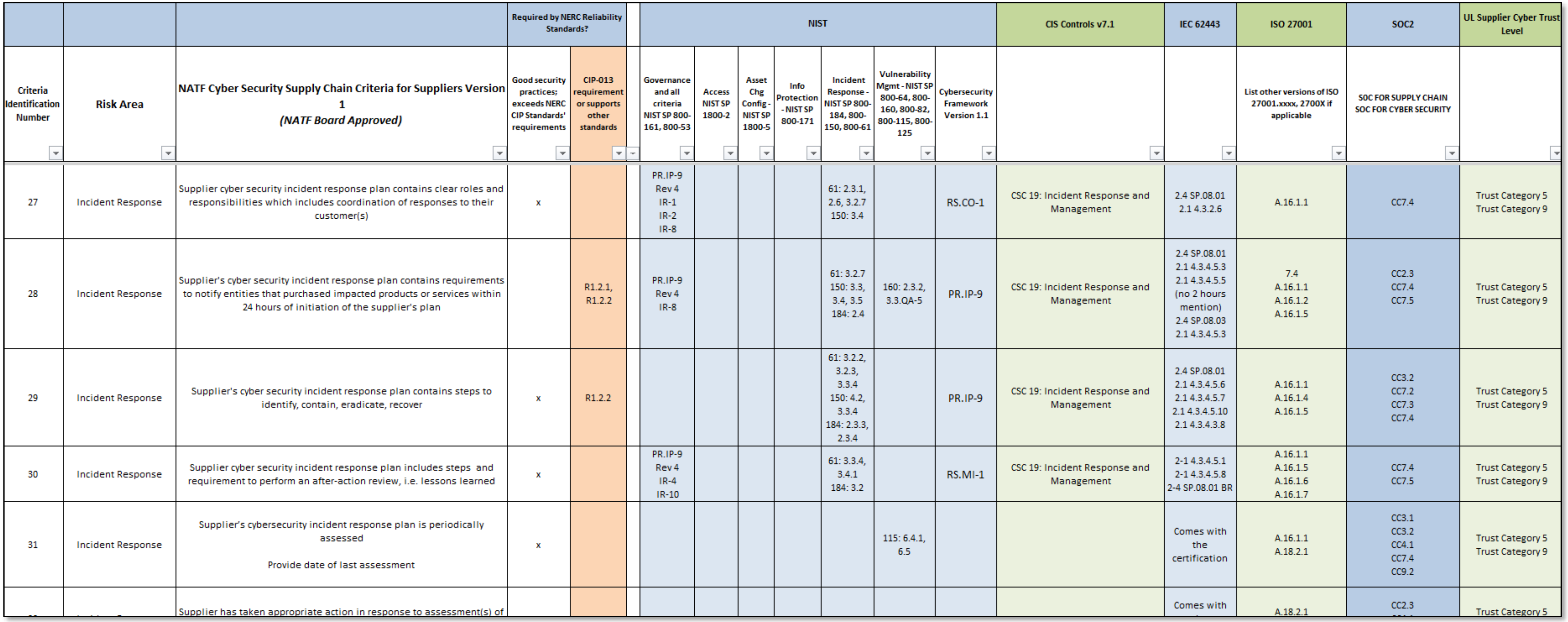
Tony Eddleman
(NPPD)

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)

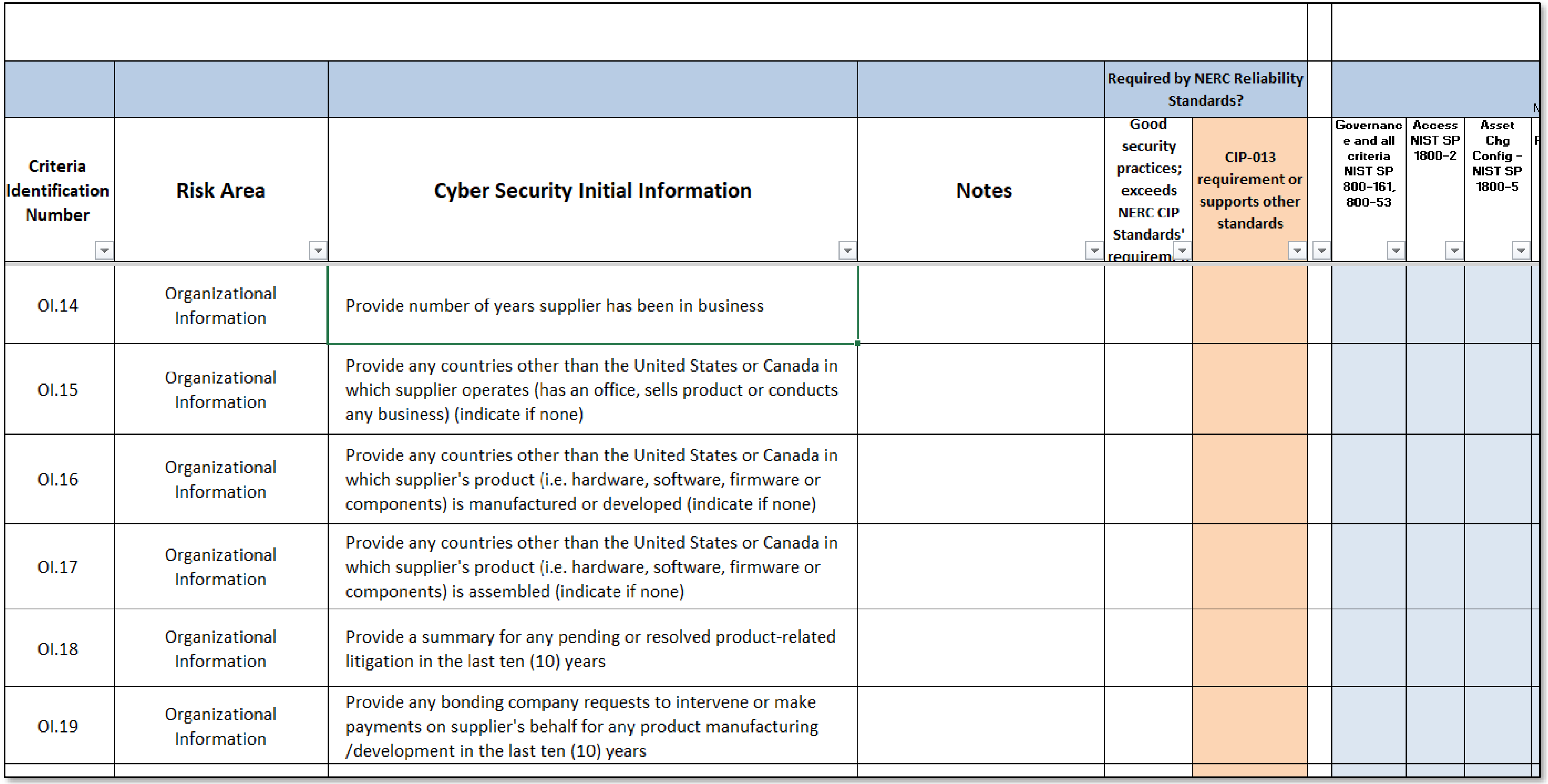
NATF Criteria Spreadsheet: Criteria



			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

NATF Criteria Spreadsheet: Organizational Information

Tony Eddleman (NPPD)



				Required by NERC Reliability Standards?					
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
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

Dina Mangialino (ConEd)

North American Transmission FORUM

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

Open Distribution

Questionnaire Overview

Dina Mangialino (ConEd)

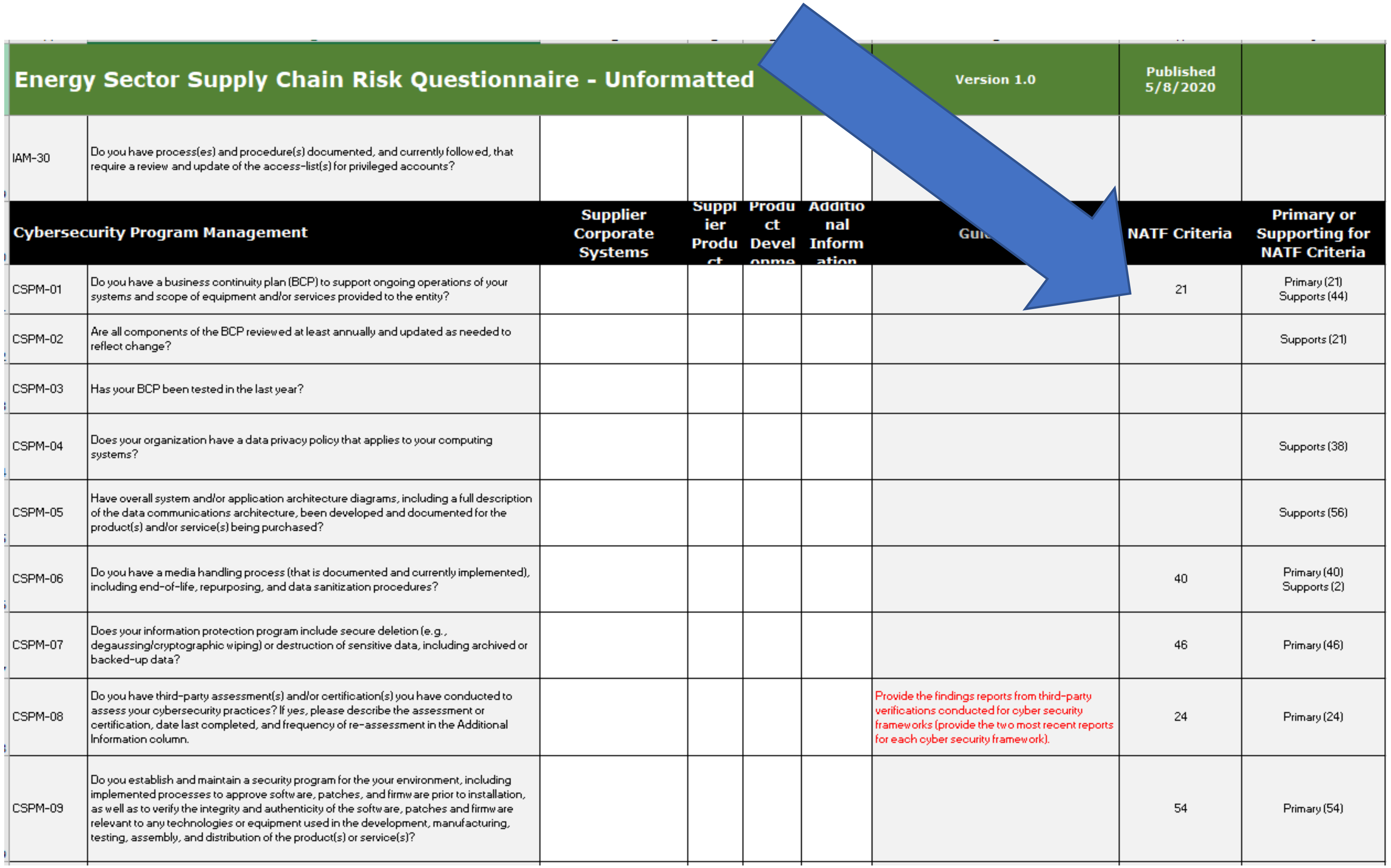
- Posted on the NATF Public Website
- Formatted and Unformatted versions
- 223 Questions plus 20 General Information questions
- Three responses per question addressing:
  - Supplier Corporate Systems
  - Supplier Product
  - Product Development Systems
- Twelve categories:

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

Questionnaire Mapping

Dina Mangialino (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 softw are, patches, and firmw are prior to installation, as well as to verify the integrity and authenticity of the softw are, patches and firmw are 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)

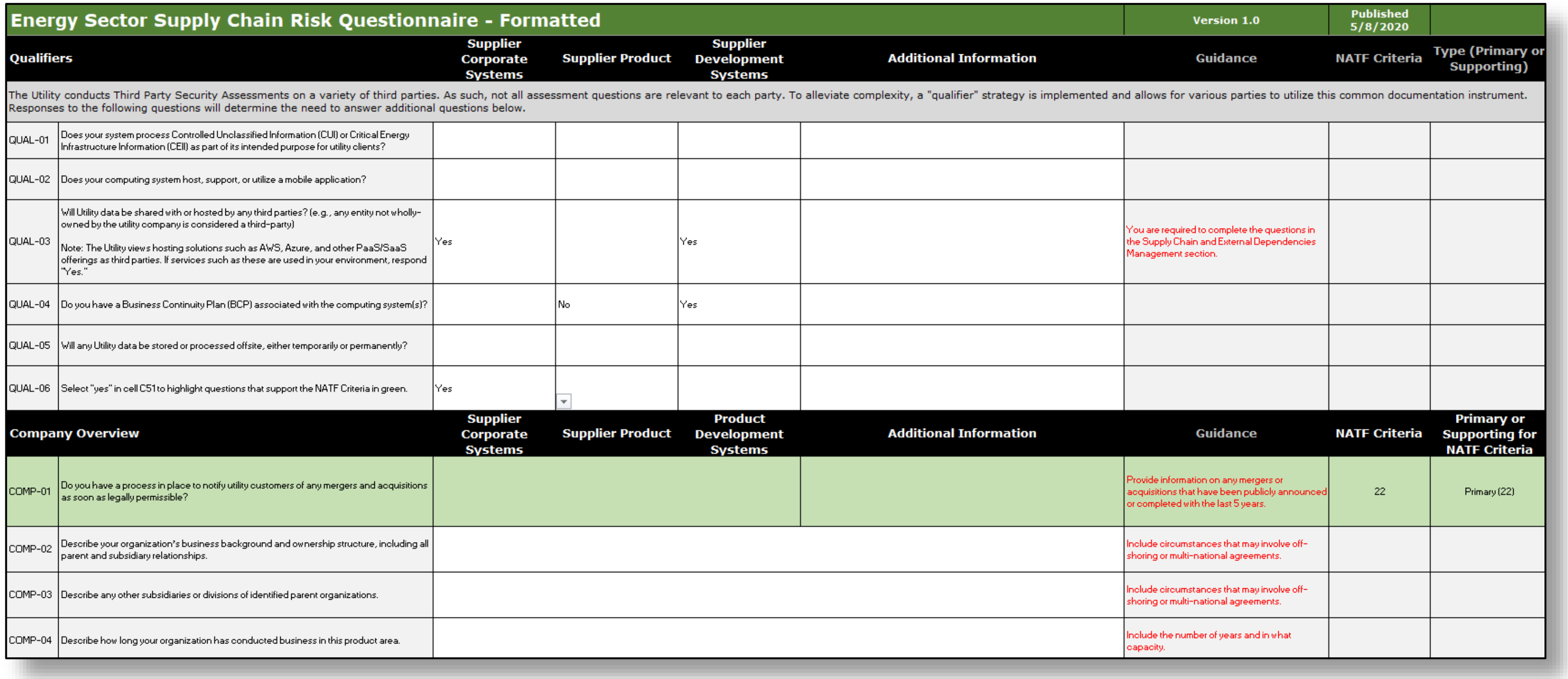
North American Transmission FORUM

Open Distribution

Dina Mangialino (ConEd)

Formatted Version of Questionnaire

- Selection of qualifiers will identify specific questions that could be optional or that support the NATF Criteria

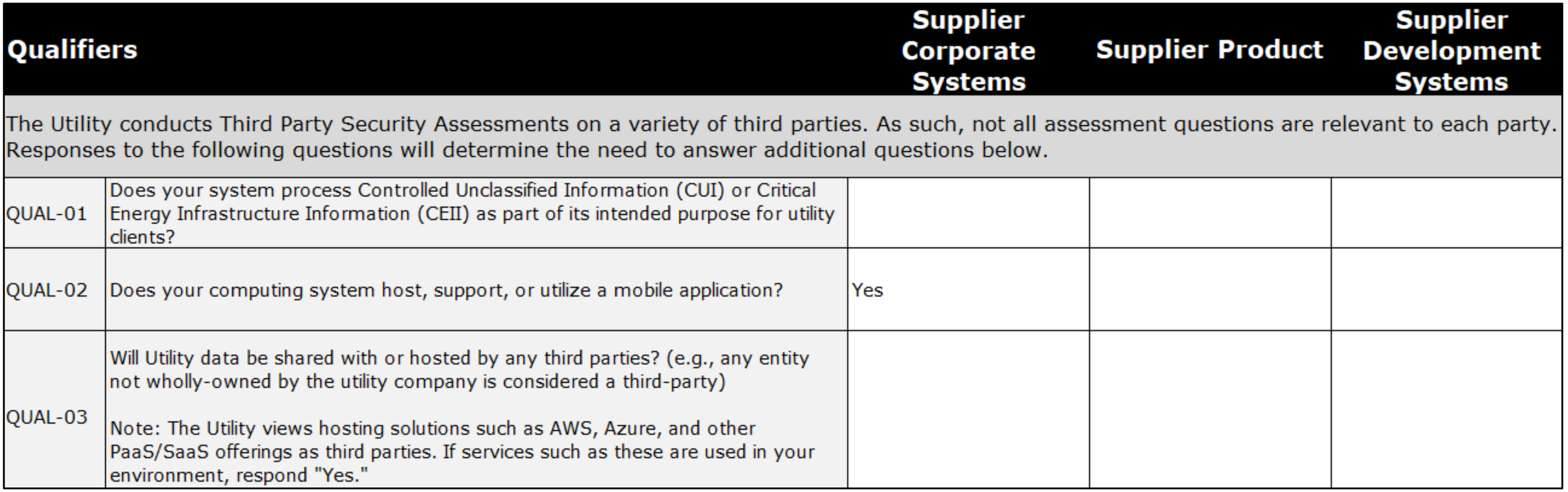


Energy Sector Supply Chain Risk Questionnaire - Formatted						Version 1.0	Published 5/8/2020	
Qualifiers		Supplier Corporate Systems	Supplier Product	Supplier Development Systems	Additional Information	Guidance	NATF Criteria	Type (Primary or Supporting)
The Utility conducts Third Party Security Assessments on a variety of third parties. As such, not all assessment questions are relevant to each party. To alleviate complexity, a "qualifier" strategy is implemented and allows for various parties to utilize this common documentation instrument. 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 offerings as third parties. If services such as these are used in your environment, respond "Yes."	Yes		Yes		You are required to complete the questions in the Supply Chain and External Dependencies Management section.		
QUAL-04	Do you have a Business Continuity Plan (BCP) associated with the computing system(s)?		No	Yes				
QUAL-05	Will any Utility data be stored or processed offsite, either temporarily or permanently?							
QUAL-06	Select "yes" in cell C51 to highlight questions that support the NATF Criteria in green.	Yes						
Company Overview		Supplier Corporate Systems	Supplier Product	Product Development Systems	Additional Information	Guidance	NATF Criteria	Primary or Supporting for NATF Criteria
COMP-01	Do you have a process in place to notify utility customers of any mergers and acquisitions as soon as legally permissible?					Provide information on any mergers or acquisitions that have been publicly announced or completed with the last 5 years.	22	Primary (22)
COMP-02	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.					Include circumstances that may involve off-shoring or multi-national agreements.		
COMP-03	Describe any other subsidiaries or divisions of identified parent organizations.					Include circumstances that may involve off-shoring or multi-national agreements.		
COMP-04	Describe how long your organization has conducted business in this product area.					Include the number of years and in what capacity.		

Dina Mangialino (ConEd)

Formatted Version of Questionnaire

- Selection of qualifiers will identify specific questions that could be optional or that support the NATF Criteria

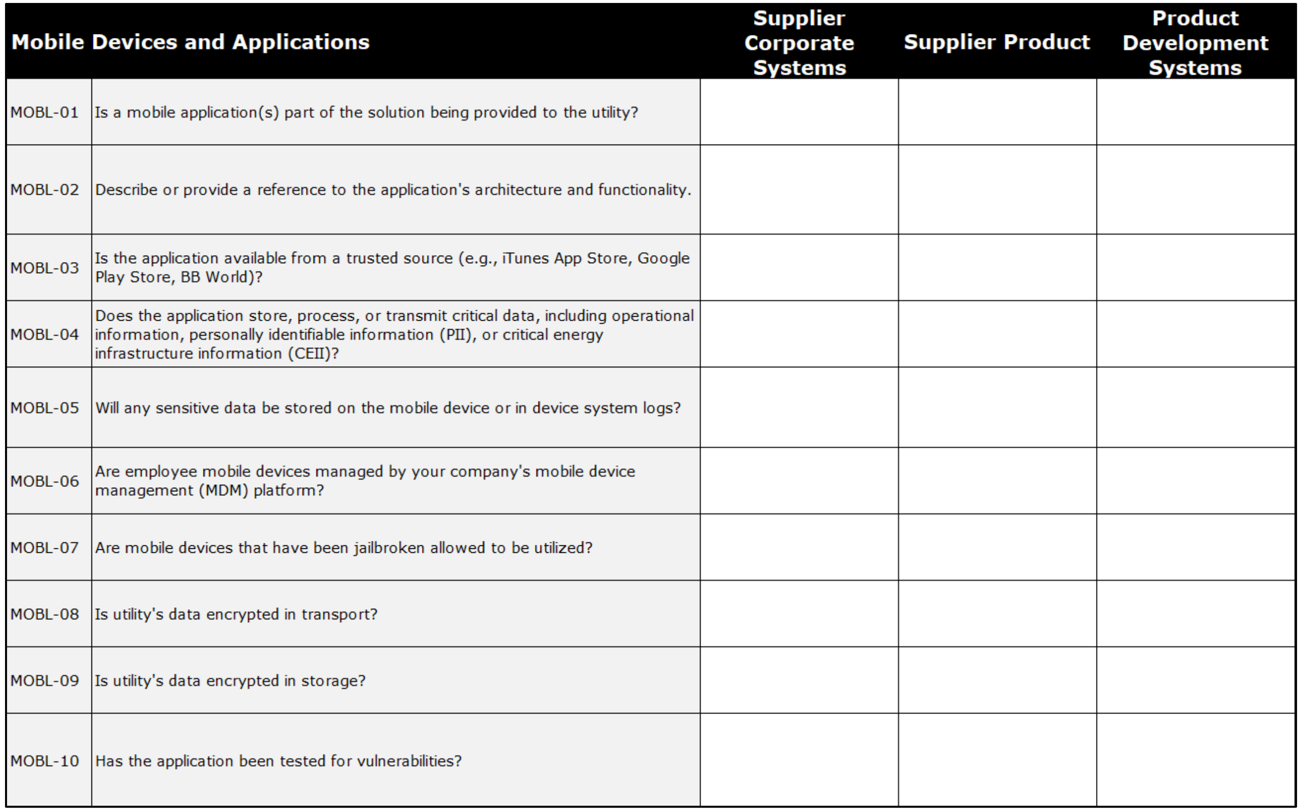


Qualifiers		Supplier Corporate Systems	Supplier Product	Supplier Development Systems
The Utility conducts Third Party Security Assessments on a variety of third parties. As such, not all assessment questions are relevant to each party. Responses to the following questions will determine the need to answer 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?	Yes		
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 offerings as third parties. If services such as these are used in your environment, respond "Yes."			

Dina Mangialino (ConEd)

Formatted Version of Questionnaire

- Selection of qualifiers will identify specific questions that could be optional or that support the NATF Criteria



Mobile Devices and Applications		Supplier Corporate Systems	Supplier Product	Product Development Systems
MOBL-01	Is a mobile application(s) part of the solution being provided to the utility?			
MOBL-02	Describe or provide a reference to the application's architecture and functionality.			
MOBL-03	Is the application available from a trusted source (e.g., iTunes App Store, Google Play Store, BB World)?			
MOBL-04	Does the application store, process, or transmit critical data, including operational information, personally identifiable information (PII), or critical energy infrastructure information (CEII)?			
MOBL-05	Will any sensitive data be stored on the mobile device or in device system logs?			
MOBL-06	Are employee mobile devices managed by your company's mobile device management (MDM) platform?			
MOBL-07	Are mobile devices that have been jailbroken allowed to be utilized?			
MOBL-08	Is utility's data encrypted in transport?			
MOBL-09	Is utility's data encrypted in storage?			
MOBL-10	Has the application been tested for vulnerabilities?			

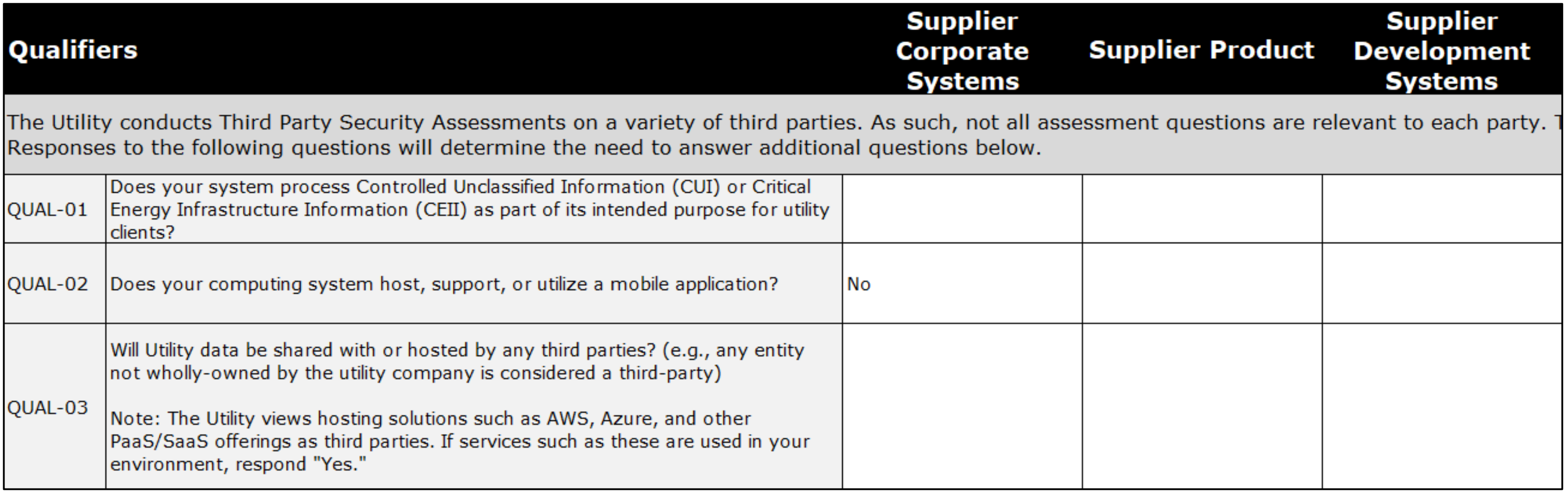
North American Transmission FORUM

Open Distribution

Dina Mangialino (ConEd)

Formatted Version of Questionnaire

- Selection of qualifiers will identify specific questions that could be optional or that support the NATF Criteria

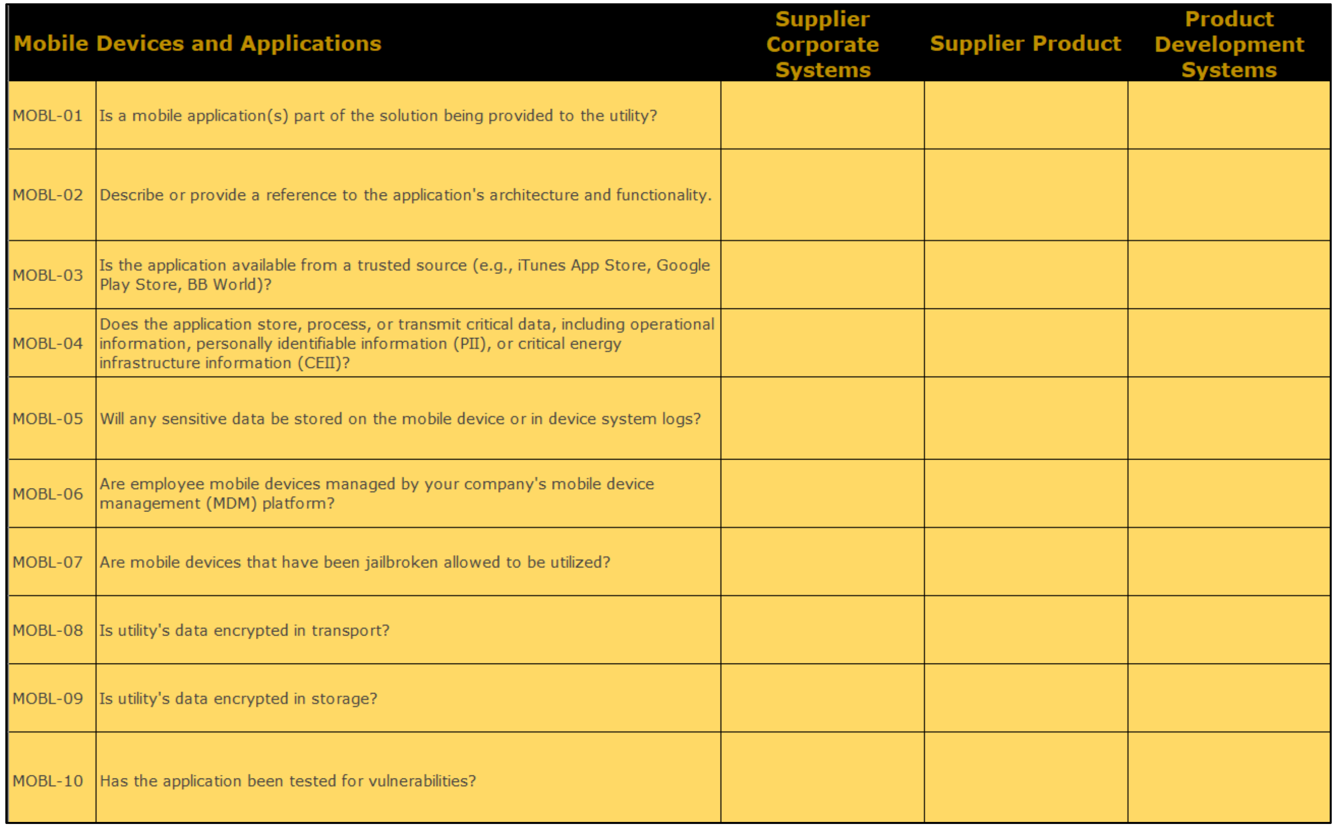


Qualifiers		Supplier Corporate Systems	Supplier Product	Supplier Development Systems
The Utility conducts Third Party Security Assessments on a variety of third parties. As such, not all assessment questions are relevant to each party. T Responses to the following questions will determine the need to 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?	No		
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 offerings as third parties. If services such as these are used in your environment, respond "Yes."			

Dina Mangialino (ConEd)

Formatted Version of Questionnaire

- Selection of qualifiers will identify specific questions that could be optional or that support the NATF Criteria



Mobile Devices and Applications		Supplier Corporate Systems	Supplier Product	Product Development Systems
MOBL-01	Is a mobile application(s) part of the solution being provided to the utility?			
MOBL-02	Describe or provide a reference to the application's architecture and functionality.			
MOBL-03	Is the application available from a trusted source (e.g., iTunes App Store, Google Play Store, BB World)?			
MOBL-04	Does the application store, process, or transmit critical data, including operational information, personally identifiable information (PII), or critical energy infrastructure information (CEII)?			
MOBL-05	Will any sensitive data be stored on the mobile device or in device system logs?			
MOBL-06	Are employee mobile devices managed by your company's mobile device management (MDM) platform?			
MOBL-07	Are mobile devices that have been jailbroken allowed to be utilized?			
MOBL-08	Is utility's data encrypted in transport?			
MOBL-09	Is utility's data encrypted in storage?			
MOBL-10	Has the application been tested for vulnerabilities?			

North American Transmission FORUM

Open Distribution

The revision process will also keep the Criteria and Questionnaire current with the changing environment

Changing Environment - SCRM Government and Regulatory Actions – Specific to Power Industry

Jack Cashin (APPA)

Document	Date Released	Date Comments Due	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
FERC White Paper - Cyber Security Incentives	18-Jun-20	17-Aug-20	https://www.ferc.gov/sites/default/files/2020-06/notice-cybersecurity.pdf
FERC NOI - CIP Enhancements	24-Jun-20	24-Aug-20	https://www.federalregister.gov/documents/2020/06/24/2020-13618/potential-enhancements-to-the-critical-infrastructure-protection-reliability-standards
DOE RFI - BPS Executive Order	8-Jul-20	24-Aug-20	https://www.federalregister.gov/documents/2020/07/08/2020-14668/securing-the-united-states-bulk-power-system
NERC Alert - Supply Chain Risk	8-Jul-20	21-Aug-20	https://portal.natf.net/document-viewer?id={7b2edb47-a3f2-6307-be03-ff00005e4fde}
FERC NOI - Equipment and Services	17-Sep-20	23-Nov-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

Changing Environment - Power Industry SCRM Interdependencies and the Need for Broadening Coordination

Jack Cashin (APPA)

- ESCC
- Canada
- Gas Industry
- Telecom

Open Questions

Tony Eddleman (NPPD)
Dina Mangialino (ConEd)
Jack Cashin (APPA)

Betsy Soehren-Jones (Exelon)

Use of the Criteria and Questionnaire

How you use the Criteria and Questionnaire depends upon your risk assessment process

Use of Criteria and Questionnaire in Supplier Risk Assessments

- Exelon – Betsy Soehren-Jones
- NPPD – Tony Eddleman
- Ameren – Chuck Abell

Based on your environment and based on the product interacts with your environment, you will have additional questions

Participoll Question!

Betsy Soehren-Jones (Exelon)

How do you approach evaluations for supply chain cyber security?

A. A risk-based approach

B. Apply across the board to all suppliers and purchases

Vote Now!

https://natfvote.participoll.com/

North American Transmission FORUM

0

vote at natfvote.participoll.com

Participoll Question!

Betsy Soehren-Jones (Exelon)

How do you determine where to conduct supply chain cyber security analysis?

A. Use a risk-based approach - OT

B. Use a risk-based approach – OT and IT

C. Apply to all suppliers and purchases or services - OT

D. Apply to all suppliers and purchases or services - OT and IT

Vote Now!

https://natfvote.participoll.com/

North American Transmission FORUM

0

Participoll Question!

Betsy Soehren-Jones (Exelon)

What do you use in your supplier evaluations?

A. All of the NATF Criteria

B. All of the questions in the Questionnaire

C. All of the Criteria and Questionnaire

D. All of the Criteria and Questionnaire plus additional questions

E. Selected NATF Criteria

F. Selected Questions in the Questionnaire

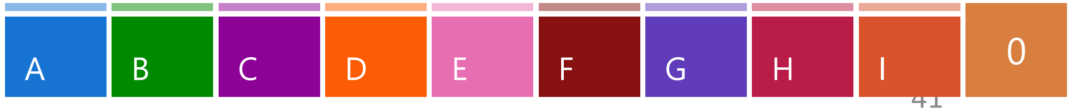
G. Some of each - a combination of selected Criteria and questions in the Questionnaire

H. Some of each - a combination of selected Criteria and questions in the Questionnaire plus additional questions

I. My own questionnaire and I'm not sure if the Criteria or Questionnaire addresses my questions

Vote Now!

https://natfvote.participoll.com/



Betsy Soehren-Jones (Exelon)

Get the information that you need and are using

And help suppliers help us

Solution Providers

Can assist getting information and conducting analysis, among other services

Rob Koziy (OSI)
Sam Chanoski (Hitachi-ABB)

Suppliers

Can provide you with verified information that you need and are using; you can help them help you

How to approach suppliers and solution providers with requests

Rob Koziy (OSI)
Sam Chanoski (Hitachi-ABB)

Provide supplier with the NATF Criteria and/or Questionnaire and let them know what information you need

- ***All*** - you are requesting responses to all criteria and questions
- ***All, but in stages*** - you will be requesting responses to all of the criteria and questions, but in stages (i.e., you are using a "gate" system)
- ***Some*** - If you don't need responses to all, add in a column for indicating and filtering the criteria and questions you want responses to
  - This helps suppliers recognize that you are using the Criteria and the Questionnaire
- ***Additional or modified*** - If you want additional or modified information, put those criteria or questions in an addendum
  - ***Don't modify the Criteria or questions in the Questionnaire***

Collect Information

Rob Koziy (OSI)

Supplier Questionnaires

- Use the NATF Criteria and/or Questionnaire
- Adjust your risk assessment process for suppliers that are certified to accepted industry standards such as ISO-27001, IEC-62443, SOC2, NIST, etc. (e.g. adjust questionnaires and evaluation)
- Ensure that risk questionnaires are relevant to the products and services being provided by the supplier (e.g. don’t use a cloud service IT questionnaire for an on-premise EMS system).
- Know ahead of time how you will evaluate the risk for all questions asked and what mitigations will be needed for negative responses from Suppliers

Collect Information

Open Questions

Betsy Soehren-Jones (Exelon)
Tony Eddleman (NPPD)
Chuck Abell (Ameren)
Tobias Whitney (Fortress A2V)
Rob Koziy (OSI)
Sam Chanoski (Hitachi-ABB)

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Mikhail Falkovich (ConEd)
Chuck Abell (Ameren)

Revision Process for the Criteria and Questionnaire

Open Distribution

North American Transmission FORUM

Mikhail Falkovich (ConEd)

Community *Confidentiality* *Candor* *Commitment*

Industry Convergence

The NATF Criteria and Questionnaire should reflect the information that you need and are using

Mikhail Falkovich (ConEd)

Let the Review Team know

- What information you are using or not using
- What Criteria or questions in the Questionnaire you want modified
- What additional information you requested

Collect Information

Convergence Request

Mikhail Falkovich (ConEd)

- **If not currently using the Questionnaire and Criteria**
  - Compare content to your current tool
  - Determine if you are requesting information not addressed by Questionnaire or Criteria
    - Could a current question be modified?

- **Provide feedback to:**
  - supplychain@natf.net (preferrable)
  - Or you can contact a team member

Collect Information

Participoll Question!

Betsy Soehren-Jones (Exelon)

Will you provide feedback and input for the revision process?

A. Yes

B. No

Vote Now!

https://natfvote.participoll.com/

0

North American Transmission FORUM

Open Distribution

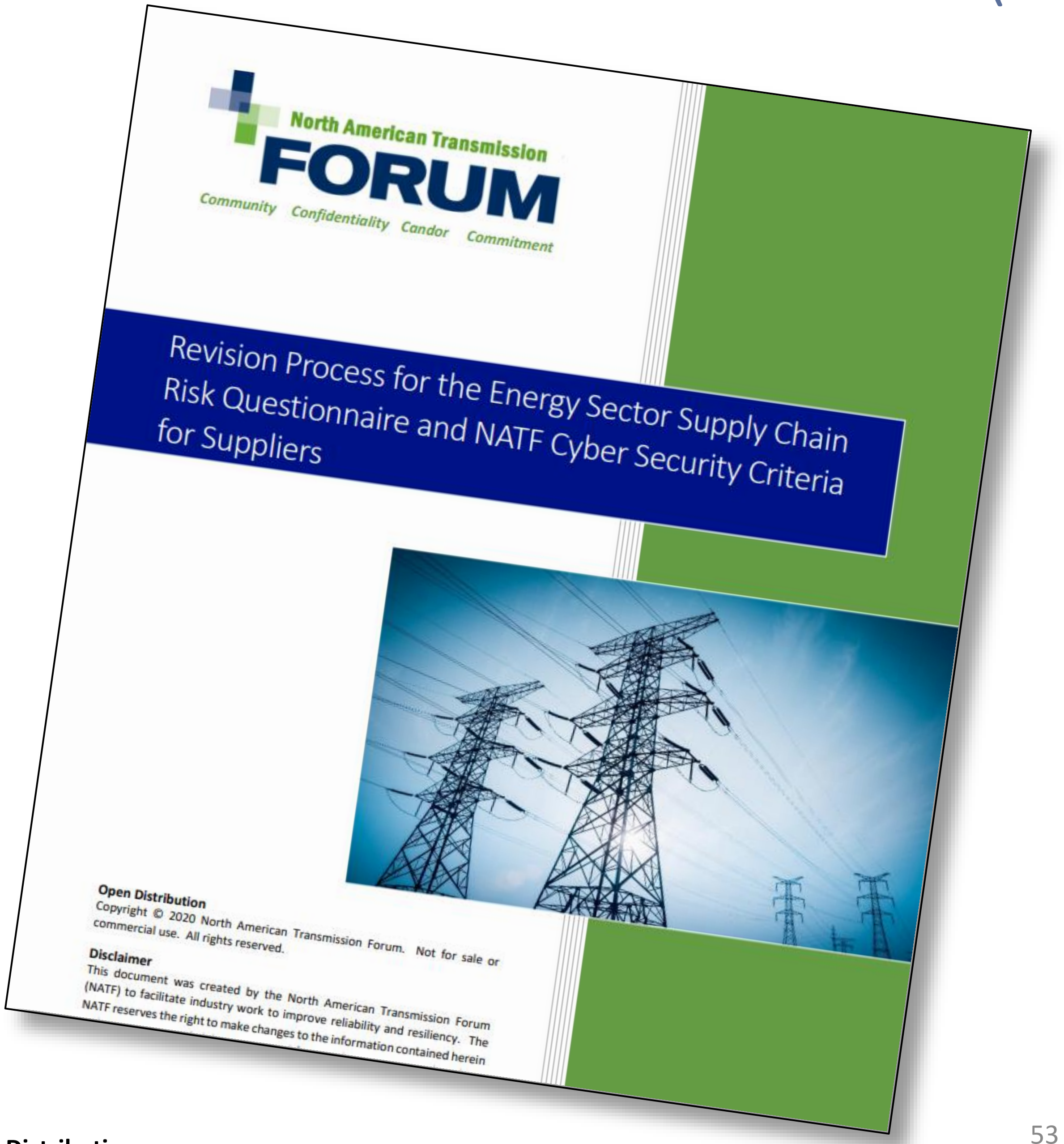
Exception from HRESULT: 0x800A01A8

vote at natfvote.participoll.com

Mikhail Falkovich (ConEd)

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.

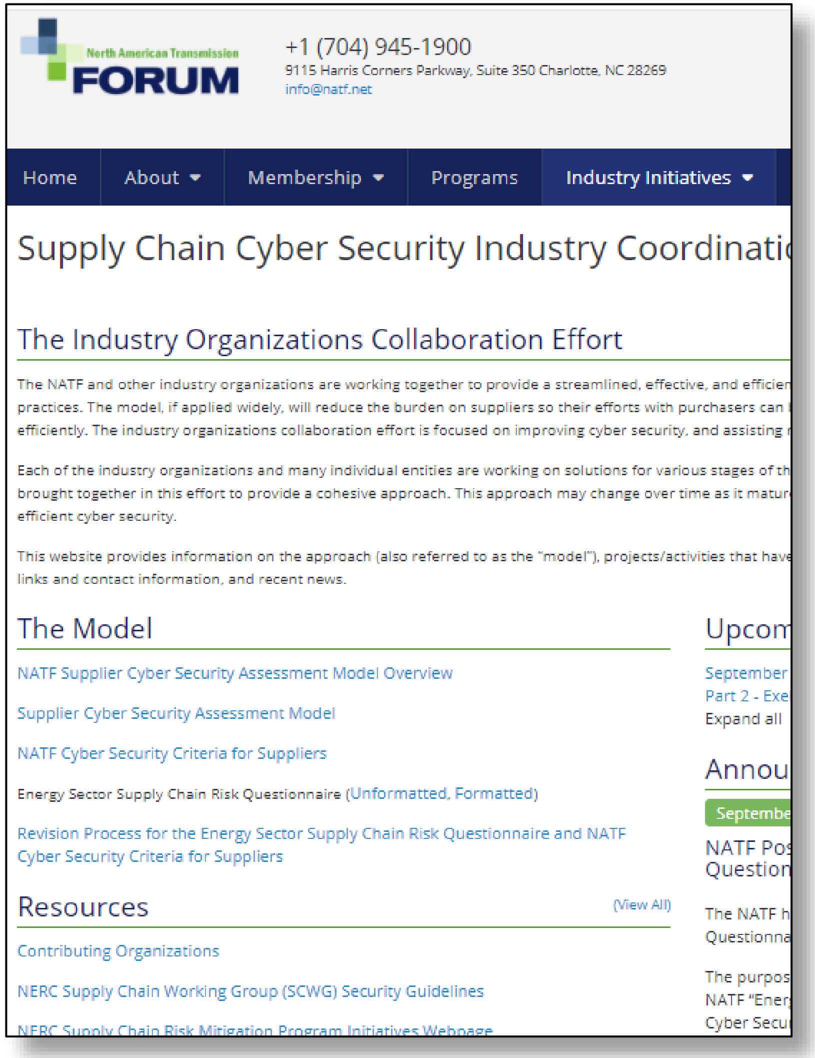
Disclaimer

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



North American Transmission FORUM

+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

Chuck Abell (Ameren)

The Revision Process

- The process establishes two teams
  - Review Team
    - Composed of members from across industry: entities, suppliers, assessors, solution providers
  - Advisory Team
    - Provides a resource for the Review Team to obtain additional opinions/insight
    - Composed of members from entities, trade organizations, and suppliers
- These teams are not hierarchical
- The Review Team may also reach out to the Industry Organizations Team for advice

Chuck Abell (Ameren)

Team Members

- Review team members
- Advisory team

Review Team Member	Company
Jeffrey Sweet	AEP, NATF Steering Team
Chuck Abell	Ameren, NATF Steering Team
Jack Cashin	APPA
Dina Mangialino	ConEd/DOE Working Group
Mikhail Falkovich	ConEd Working Group
James Chuber	Duke, NATF Steering Team
Mary Nettleton	Exelon
Betsy Soehren-Jones	Exelon, NATF Steering Team
Tobias Whitney	Fortress/A2V
Sam Chanoski	Hitachi ABB Power Grids
Jose Flores	NATF
Ken Keels	NATF
Scott Webb	Network and Security Technologies
Tony Eddleman	NPPD, NATF Steering Team
Rob Koziy	OSI
Steve McElwee	PJM, NATF Steering Team
Carl Phillips	PSEG
Jake Stricker	PWC
Roger Blakely	Santee Cooper
Frank Harrill	SEL
Shannon Hammett	Southern Co, NATF Steering Team
Barry Jones	WAPA
Dominick Forlenza	Xcel

Advisory Team Member	Company
Zohaib Hasan	ConEd
Laura Schepis	EEI/ESCC
Tony Eddleman	NATF Steering Team
Rob Koziy	OSI
Victor Calderon	SCE

The Revision Process

Chuck Abell (Ameren)

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

Chuck Abell (Ameren)

The Revision Process

The Review Team meets monthly to review inputs

- Inputs that are needed more urgently may be made prior to the annual update process

Inputs should be provided to NATF at

supplychain@natf.net

It may not be possible to develop a set of Criteria or a single Questionnaire that addresses all information needs

So addendums may be needed, but let's get 90% of the way there!

Mikhail Falkovich (ConEd)
Chuck Abell (Ameren)

Open Questions

Thank you for attending!

NATF Contact Information

supplychain@natf.net

kkeels@natf.net

vagnew@natf.net