North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Energy Sector Supply Chain Risk Questionnaire ("ESSCRQ" or "Questionnaire")

May 19, 2020

Agenda

Valerie Agnew (NATF)

- Current Environment
- Development of Questionnaire
- How Questionnaire fits into the NATF and Industry Organizations Supply Chain Activities
- Overview of the Questionnaire
- Next Steps
- Take-aways

Mikhail Falkovich (ConEd)

Current Landscape

- Adoption of cloud technologies has increased
- Large amounts of data are sent out to third parties for operational, regulatory, and economic reasons
- Hundreds of risk assessment performed per year
- Regulators and private industry are looking for ways to manage the growing supply chain cybersecurity risk
- New mandatory standard requirements have been approved and more regulation forthcoming
- Inconsistency of assessments between and within organizations

Trending of Cybersecurity Risk Assessments

Mikhail Falkovich (ConEd)

- Supply chain and third-party cybersecurity risk is growing
- Number of risk assessments is doubling year over year
- Companies are adding resources to support risk mitigation activities
- Supply Chain Risk Management standard (CIP-013) compliance programs are being developed

The Energy Sector Supply Chain Risk Questionnaire

Mikhail Falkovich (ConEd)

How the Questionnaire was developed

- ConEd Working Group
- NATF and Industry Organizations

Value Proposition

- Multiple entities within the sector worked to develop a single, common questionnaire to gain the following benefits:
  - Detailed and Consistent approach to supply chain cyber risk assessment
  - Cybersecurity risk management specifically for Energy Sector
  - Increased effectiveness and speed of supplier risk assessments
  - Meeting NATF Criteria
  - Meets regulatory requirements

Contributing Companies

James Chuber (Duke)
Shannon Hammett (Southern Company)
Jake Strickler (PwC)

American Electric Power

Con Edison

DTE Energy

Duke

Eversource

Nebraska Public Power District

New York Power Authority

PJM

Price Waterhouse Cooper

Southern California Edison

Southern Company

Xcel Energy

NATF and Industry Organizations' Supply Chain Activities

Tony Eddleman (NPPD)

- NATF Criteria
- NATF Questionnaire
- Supplier Assessment Model
  - Model anticipated the development of a Questionnaire

Industry Organization Team Members

Tony Eddleman (NPPD)

Organizations, Forums and Working Groups

- APPA
- ConEd Working Group
- EEI
- LPPC
- NAESB
- NAGF
- NATF
- NRECA
- SCWG/CIPC
- TAPS

Suppliers

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

Third-Party Assessors

- Deloitte
- Ernst & Young
- KPMG LLP
- PWC

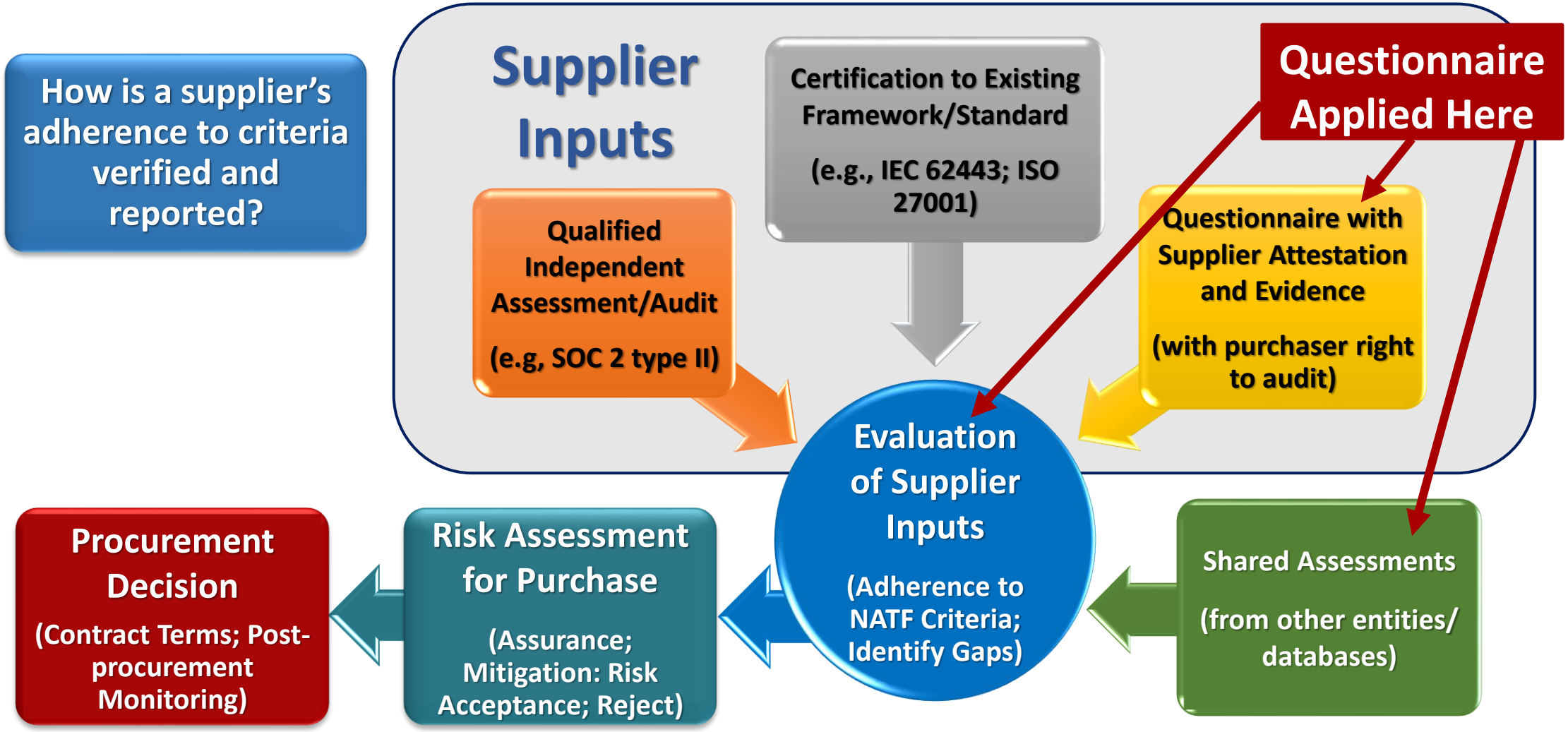
Vendor Organizations for support products or services

- EPRI
- Fortress/A2V

Process Overview

Tony Eddleman (NPPD)

Questionnaire supports Collect and Evaluate Steps



May 1 Executive Order

Valerie Agnew (NATF)

Executive Order (EO) 13920, "Securing the United States Bulk-Power System"

- Authorizes U.S. Secretary of Energy to work with the Cabinet and the energy industry to secure America's bulk-power system (BPS).

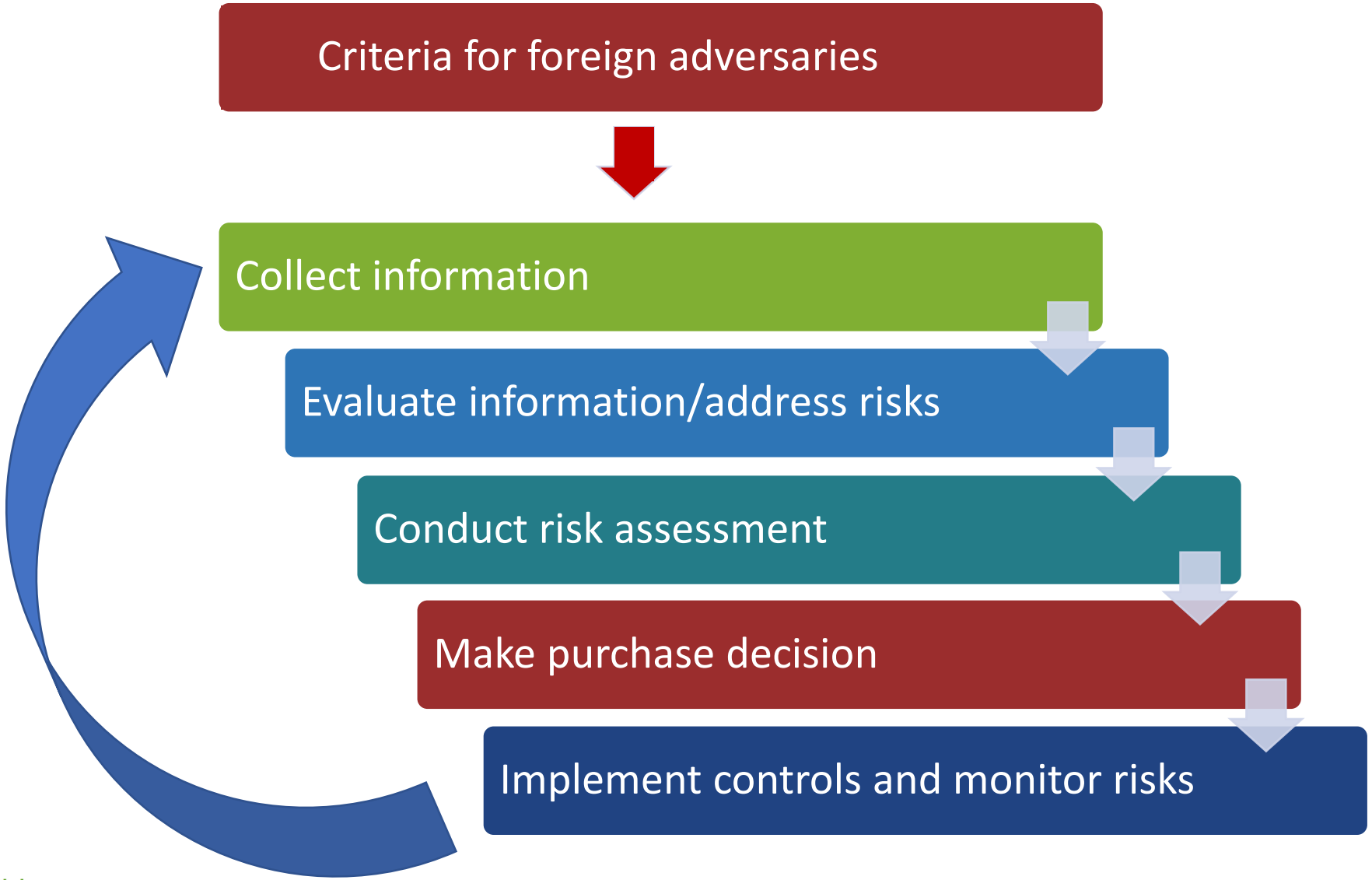
Four Pillars

1. *Prohibit foreign adversaries from providing products where there is a risk that relates to national security*
2. *Establishes the ability for a pre-qualification for suppliers (criteria)*
3. *Identifying things on the system that are at risk today*
4. *Establishment of a Task Force*

DOE Summary of Executive Order, FAQ, and related reference documents: https://www.energy.gov/oe/bulkpowersystemexecutiveorder

Possible Process with EO Criteria

Valerie Agnew (NATF)



Questionnaire Overview

Dina Mangialino (ConEd)

- Approximately 200 questions
- Three responses per question:
  - 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

- Formatted and unformatted versions

Questionnaire Mapping to NATF Criteria

Tony Eddleman (NPPD)

All questions provide support information for the NATF Criteria; the key supporting questions are identified

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 Development**	**Additional Information**	**Guidance**	**NATF Criteria**	**Primary or Supporting for NATF Criteria**
CSPM-01	Do you have a business continuity plan (BCP) to support ongoing operations of your systems and scope of equipment and/or services provided to the 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)

NATF-hosted Industry Organizations Web Page

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

Model
NATF Criteria
Questionnaire

Next Steps

Mikhail Falkovich (ConEd)
Ken Keels (NATF)

Converge industry to a set of effective and efficient questions

- Reduction in number of questions
- Questions pertain to what information entities are using in their supplier evaluations

Use existing frameworks when available

- Criteria is mapped
- Questionnaire to be mapped

NATF will manage Questionnaire

- Living document
- Industry inputs for modification
- Provide feedback to supplychain@natf.net

Take-aways

Valerie Agnew (NATF)

The Questionnaire is available for your use

- The Questionnaire and NATF Criteria obtain information regarding a supplier's cyber security practices
- Entities will need to conduct a supplier evaluation using the information
- Supplier evaluation does not determine an entity's purchase decision; it is one input into an entity's risk assessment

The Questionnaire is a step forward for industry convergence on what information is needed from suppliers

- The Questionnaire and NATF Criteria are living documents and will be updated as industry learns more about what information is necessary and used in their supplier evaluations

Questions

NATF-hosted Supply Chain Cyber Security Industry Coordination webpage:

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

Email for comments and questions:

supplychain@natf.net