



Community

Confidentiality

Candor

Commitment

Large Entity Use-Case Webinar: Conducting Supply Chain Supplier Assessments

June 2020

Open Distribution

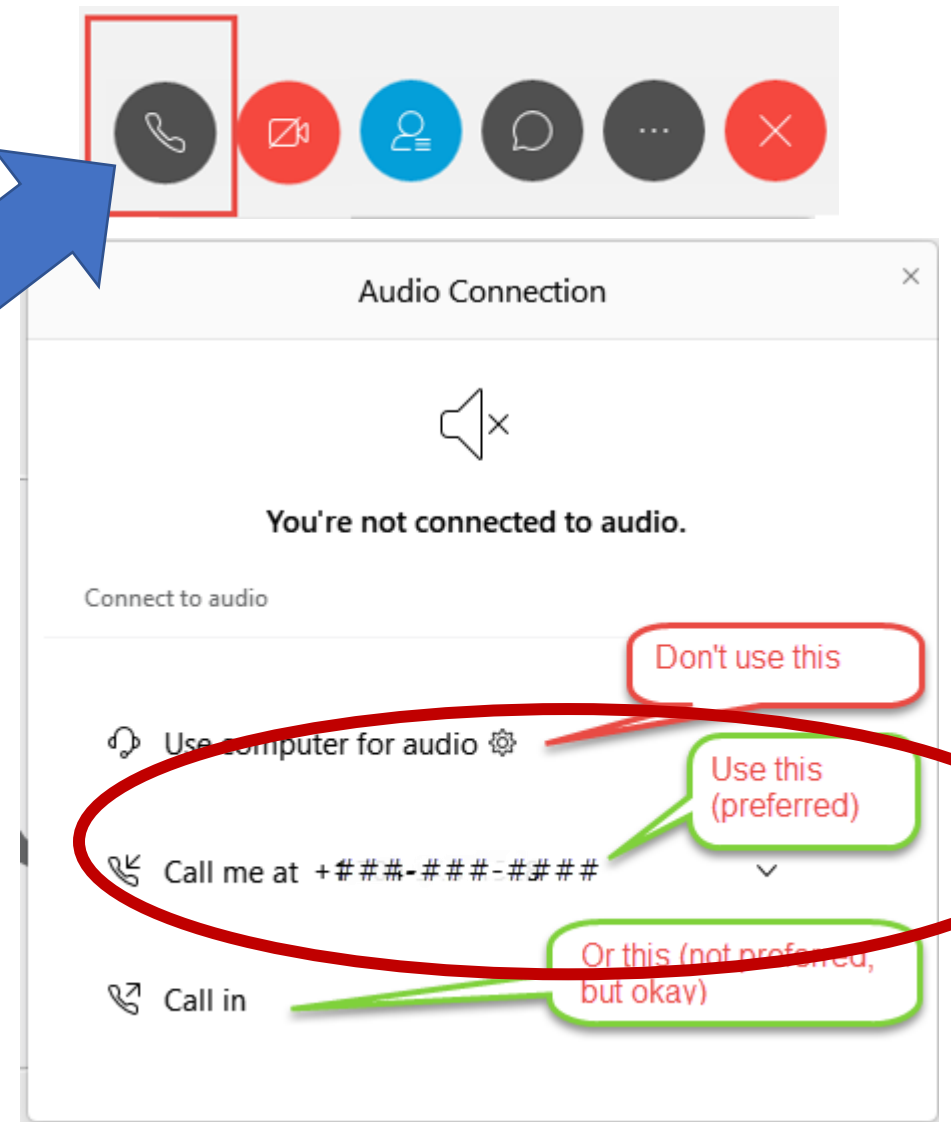
Copyright © 2020 North American Transmission Forum (“NATF”). All rights reserved.

No Representation or Warranty


The Content is provided on an “as is” basis. The NATF makes no and hereby disclaims all representations or warranties (express or implied) relating to the Content. The NATF shall not be liable for any damages arising directly or indirectly from the Content or use thereof. By using the Content, you hereby agree to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use.

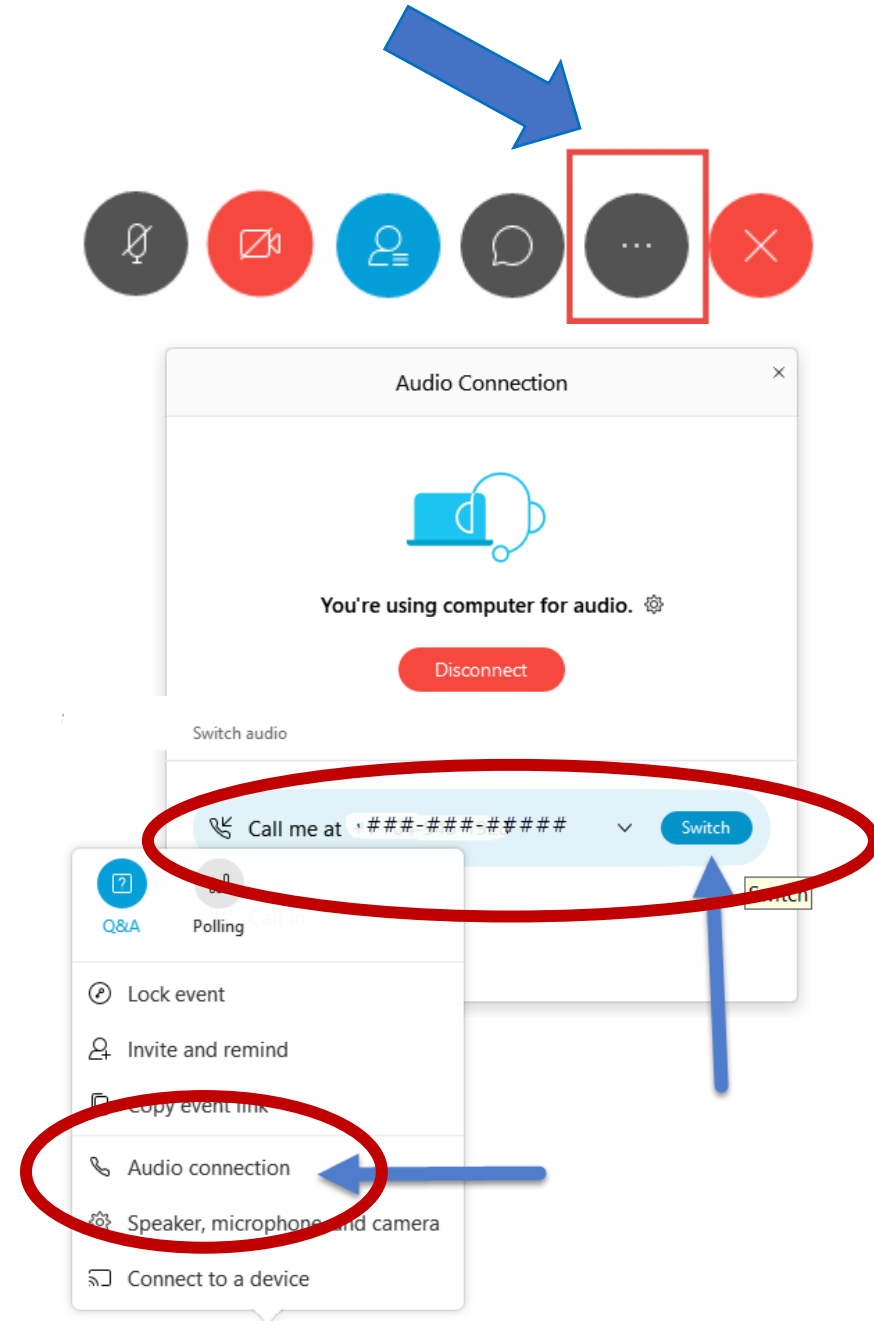
Webex Audio Connection

- **Don't dial in separately**
- **Do have webex CALL YOU**
- Select  to connect to audio
 - Select the "Call me at..." option
 - Don't select "Use computer for audio"
 - Don't select "Call in" unless "Call me at..." does not work



If you connect to audio the wrong way, you can change it

1. Select the “More Options” menu 
2. Select “Audio connection”
3. Select “Disconnect” or select “Switch” next to “Call me at...”



Agenda

- Opening Comments 11:00-11:15am
- Large Entity Presentations
 - Exelon 11:15-11:45am
 - FirstEnergy 11:45-12:15pm
 - ConEd 12:15-12:45pm
- Break 12:45-1:00pm
- Panel Discussion 1:00-2:00pm

Opening Information

- Webinar will not be recorded
- Obey Anti-Trust Laws
- Webinar is open
 - Attendees may not be subject to NATF confidentiality agreement
 - Members of press or regulators may be present
- Please use chat, Q&A or raise your “hand” to ask a question

Disclaimer

- The slides provided are for discussion purposes only
- The slides and discussion are offered to support sharing security programs
- The approaches here are offered to be informative, however individual companies may use alternative and/or more specific approaches that they deem more appropriate



Community

Confidentiality

Candor

Commitment

Opening Remarks

Tom Galloway, President and CEO

Industry Organization Team Members

Organizations, Forums and Working Groups

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

Suppliers

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

Third-Party Assessors

- Ernst & Young
- KPMG LLP
- PWC
- Deloitte

Vendor Organizations for support products or services

- EPRI
- Fortress/A2V

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)

Supplier Assessment Model Process Overview



What Information to Collect

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

Collect Information

Methods to Collect Information

- Obtain a **qualified assessors' third-party assessment** or independent audit that addresses NATF Criteria
- Obtain **third-party vendor's risk assessment**
 - Includes shared assessments
- Obtain **evidence from supplier to conduct evaluation**

Collect Information

Conduct Supplier Evaluation/Risk Assessment

- Evaluate the level of adherence to the established practices (e.g., NATF Criteria)
- Evaluate level of assurance / trustworthiness of information
- Identify potential risks
- Evaluate whether risks could be remediated, mitigated, or, if there would not be an impact on the reliability of the bulk power system, accepted
 - Risks could be mitigated by the supplier, the purchasing entity or through contractual requirements

Evaluate information/address risks

Available to Industry Today

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

EEl Procurement Language

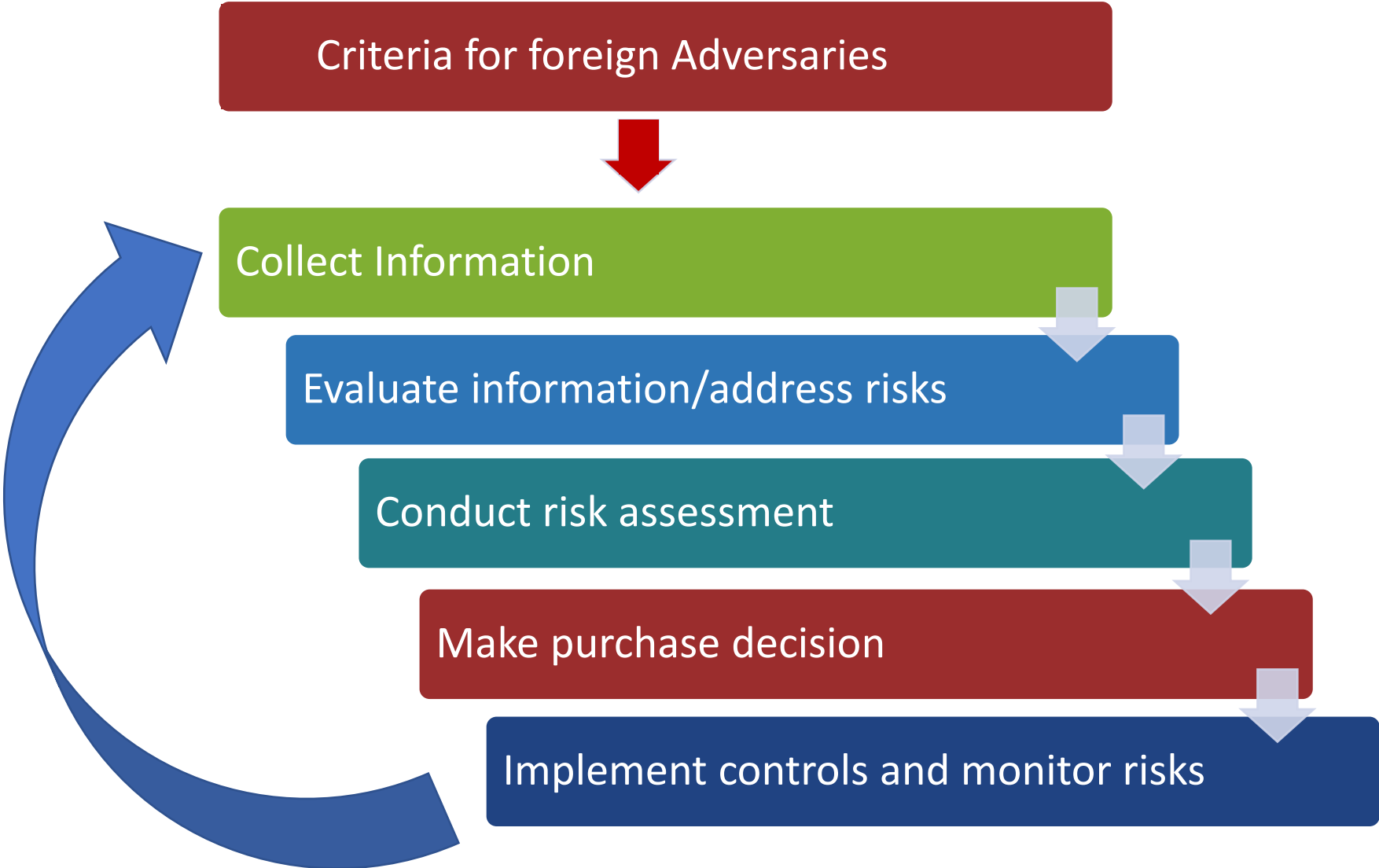
- Sample contract language to mitigate risk and provide assurances of supplier performance

NATF-hosted Industry Organizations Web Page

May 1 Executive Order

- [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*

Possible Assessment Process with EO Criteria



Exelon

Betsy Soehren-Jones - Director, Security Governance

Jennifer Burke – Director IT, IT NERC CIP Compliance

Erin Holloway – Sr. Manager, Supply Sourcing

Third Party Risk Management Webinar June 2020

For Discussion Purposes Only



Introduction

Supply Chain Risk Management – Presenters

- **Elizabeth (Betsy) Soehren-Jones** | Director, Cyber and Physical Security Governance & Strategy and NERC CIP Security Enterprise Standard Owner (ESO)
- **Jennifer Burke** | Director, IT, NERC Compliance
- **Erin Holloway** | Sr Manager, Supply Sourcing, Exelon's Procurement Group



NERC CIP-013 – Cybersecurity Supply Chain Risk Management Standard

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standard 013-1 Cyber Security – *Supply Chain Risk Management* states that each Responsible Entity (i.e., Exelon) shall mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber systems.

There are three requirements within NERC CIP-013-1:

- ❑ Requirement 1 states that each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber systems
 - Exelon’s implementation plan = Security Risk Assessment

- ❑ Requirement 2 states that each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.
 - Exelon’s implementation plan = Security Risk Assessment

- ❑ Requirement 3 states that each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.
 - Exelon’s implementation plan = documented reviews on an annual basis across the enterprise with all stakeholders

Exelon's Procurement Process with Embedded Security Standards

Program Overview

- ❑ Enterprise-wide program that begins with a requisition request from the line of business
 - Is this a CIP purchase or not?

- ❑ “Security Gate” Questions
 - Do I want to do business with this organization?

- ❑ Competitive vendors are selected then receive remaining security hygiene criteria and technical reviews (answers are utilized to determine final selection).
 - Hygiene and technical reviews based on NATF criteria
 - Technical reviews also include the applicability and ability to install the IT/OT devices within the environment

- ❑ Information criticality determines appropriate terms and conditions as well as amendments (contractually obligate/EEI Language)

Examples of Minimum Security Standards

- 1) Do you have an industry recognized Information Security Policy published and available to all employees, including contractors and Part-time temporary employees (e.g., NIST CSF, ISO 27001)?
- 2) Are employees obligated as condition of employment to adhere to the information Security Policy?
- 3) Do you have written policies/procedures for maintaining and monitoring the security of customer data?
- 4) Do you use anti-virus software on corporate devices or devices owned by employees that will be utilized to process Exelon information?
- 5) Are your anti-virus signatures updated on a defined regular basis?
- 6) Do you contract with subcontractors (fourth party vendors to Exelon) in the development or delivery of your application, device, and/or service you are purposing to Exelon?
- 7) Are you an affiliated entity of or do you procure products or services from the vendors listed below or their subsidiaries/affiliates? (*Federal government, DFARS, and FARS requirement*)
 - Kaspersky
 - Huawei Technologies Company
 - ZTE Corporation
 - Hytera Communications
 - Hangzhou Hikivision Digital Technology Company
 - Dahua Technology Company
- 8) Do you conduct background checks (e.g., credit, criminal, drug employment checks) for all employees? (CIP requirement)

Post Implementation Conclusions

Program Results

- Response rate; Utilized economy of scales and other RFP's to force compliance

- Red at the onset (i.e. cant meet the minimum 8 questions)
 - Results indicate the vendors will need to implement additional security measures
 - Follow up calls needed; remediation plans required; attached to contract
 - Process is providing the results NERC was looking to achieve – all boats rising

Program Challenges/Areas for Maturity

- Industry questionnaire standardization needed; cautiously optimistic as to a successful rollout; balance operating needs and security
- Ensuring compliance when incorporating Executive Order requirements
- No Central Repository for Vendor Responses across the industry
- No Certifying Body to Verify Responses across the industry

Overall Successes: Corporate and Information Security Services (CISS) Engagements:

- CISS, Legislative Affairs, and Legal are monitoring dockets and proposed legislation
- Proactive outreach to public service commissions, including tours of the Cyber Operations Center

Executive Order Coordination Team

A Tiger Team has been established to analyze the order, develop and support Exelon’s regulatory advocacy in coordination with industry allies, and help Exelon prepare for new compliance obligations. The Tiger Team is reaching out to all potentially affected areas of the company for input. The EO Tiger teams include participants from Supply, Strategic Sourcing, Legal, IT, Compliance, CISS, Nuclear, Exelon Utilities, and Internal Audit.

Group	Details	Meeting Frequency
<u>Core Team Meeting</u>	The Core Team will include leads from Supply, CISS, Government Affairs, Legal, Compliance, Exelon Utilities (EU), EU OpCos, and Exelon Generation (Nuclear and Power). The Core Team will develop the list of risks and propose mitigation strategies to the Stakeholder group	Weekly
<u>Stakeholder Tiger Team Meeting</u>	The Stakeholder Team identified and prioritized the risks of the EO to Exelon. The results of this work are included in the appendix.	Weekly
<u>Exelon Senior Leadership Update</u>	The co-leads will review the work of the stakeholder group with Senior Leadership for awareness, review and approval	Biweekly

This Tiger Team is co-led by **Betsy Soehren-Jones** (Director, Security Governance, CISS), **Paul Ackerman** (Associate General Counsel, Compliance), and **Jackie Carney** (Director, Federal Government Affairs). **Joe Quinn** (Manager, Security Public Policy, CISS) serves as project manager.

Questions



FirstEnergy

Scott Hipkins – Manager, NERC CIP Compliance

Marcus Noel – Manager, Cyber Security & TSOC

Jason McCormick – Supervisor, Cyber Security

Supply Chain Risk Management Process

1. Vendor identification from design process
2. Vendor assessment performed (CIP-013 R1.1)
 - Questionnaire based on NATF questions; modified for scorable format
 - BitSight vendor risk score
3. Contract negotiation with vendor to add CIP-013 R1.2 items
4. Approvals as necessary based on scoring and contract terms
5. Documentation of the vendor “package”

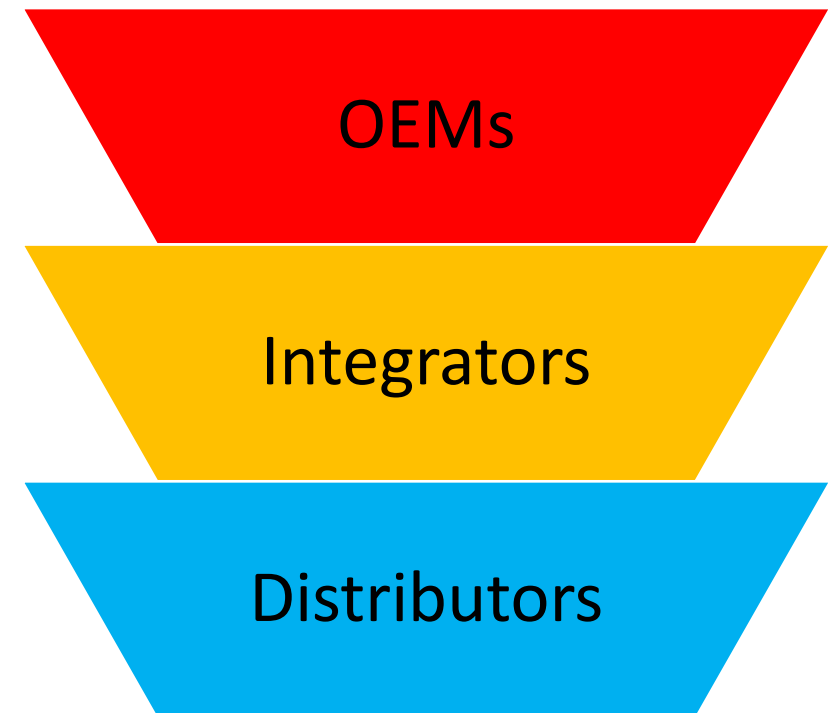
“Vendors” – What are they... exactly?

Identified three categories of vendors

- Original Equipment Maker
- Integrator
- Distributor

Identified seven overall flavors of vendors

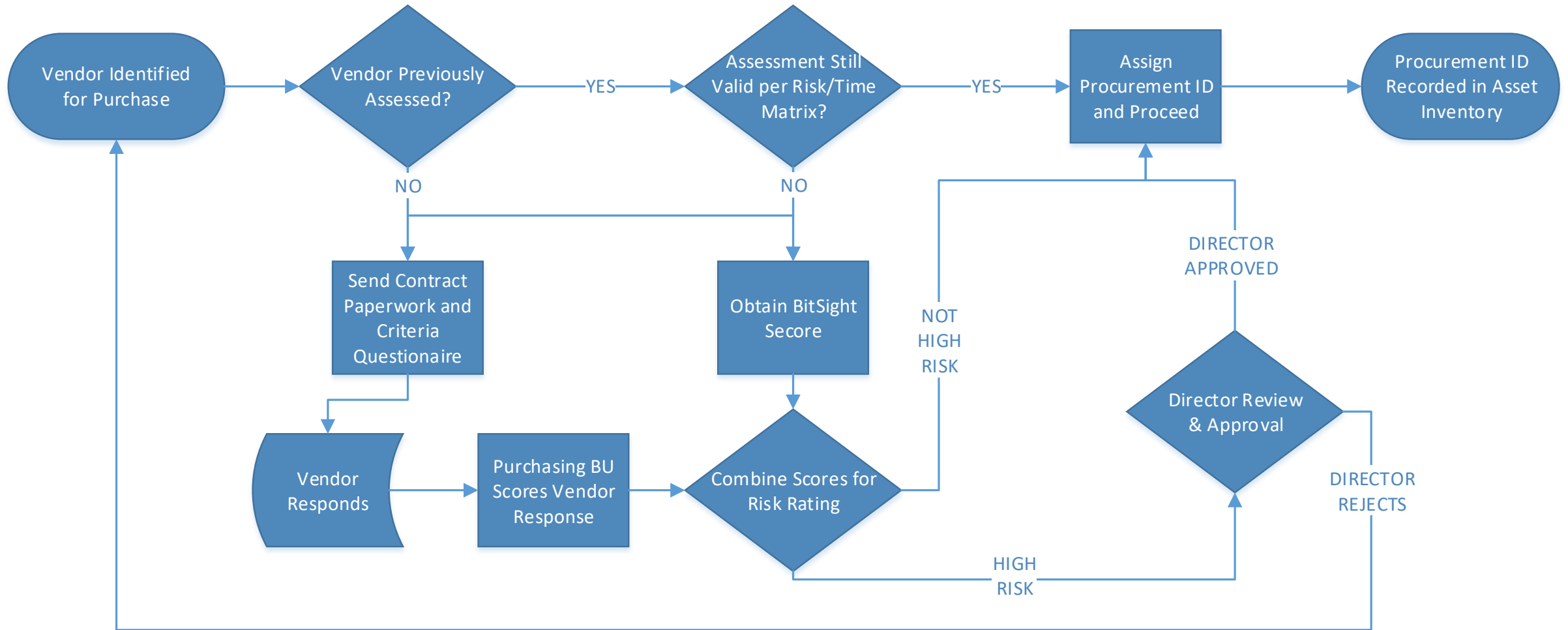
A “Vendor” can simultaneously be more than one type



“Vendors” – What are they... exactly?

Vendor Category	Vendor Type	Type of Vendor
OEM	A	OEM of hardware, server, etc. if the asset was purchased directly from the OEM
	B	OEM of hardware, server, etc. if: <ol style="list-style-type: none"> 1. the asset was not purchased directly from the OEM and 2. purchased through a Distributor or acquired through an Integrator
	C	OEM of software, firmware, or security updates (e.g. CIP-010 1.1.1, 1.1.2, 1.1.5) and the item(s) were directly purchased from the OEM
	D	OEM of software, firmware, or security updates (e.g. CIP-010 1.1.1, 1.1.2, 1.1.5) and <ol style="list-style-type: none"> 1. the item(s) were not directly purchased from the OEM and 2. purchased through a Distributor or acquired through an Integrator
Integrator	E	Integrator of multiple hardware and software components where the vendor is not directly providing software <i>Note: An Integrator of type E does not preclude the associated assets' vendor types A, B, or G also being applicable to this vendor</i>
	F	Integrator of multiple hardware and software components and the vendor is directly providing software, firmware, or security updates <i>Note: An Integrator of type F does not preclude the associated assets' vendor types A, B, or G also being applicable to this vendor</i>
Distributor	G	Distributor of a BES Cyber System, BES asset, or installable software, firmware, or security updates (Program 100 1.1.1, 1.1.2, 1.1.5)

Process Flow



Obtaining Vendor Information

1. FirstEnergy Supply Chain sends T&Cs and questionnaire to the supplier contact
2. FirstEnergy Supply Chain sends questionnaires and MOUs as necessary to downstream vendors (e.g. OEM bought via Distributor)
3. FirstEnergy does not require artifacts from vendors
4. FirstEnergy Cyber Security uses BitSight to review the vendor(s) score and any additional information if relevant
 - “Service Providers” are a difficult problem even if you’re not using them as a service – e.g. Microsoft, Oracle, etc.
5. Supply Chain executes its contract negotiation process
6. Supply Chain returns the questionnaire(s) to the requesting unit

Obtaining Vendor Information

If risk rating is **Low or Medium**

- Purchase may proceed
- Vendor assessment valid for additional purchases for 24-36 months depending on score

If risk rating is **High**

- Director of the business unit must personally review and approve
- Business Units will review concerns with Cyber Security
- High risk vendors are discouraged for new purchases whenever practical
- High risk vendors must be re-evaluated yearly for additional purchases

Addressing Identified Risks

Is Mitigation Possible?

- By Supplier: Usually not; most suppliers aren't interested
- By FirstEnergy:
 - Existing cyber security controls mitigate most potential issues
 - 24x7 SOC operations monitoring for suspicious activity
 - SOC and cyber security program will add additional monitoring and controls as necessary
 - IT process for systems that are connected to the network have additional processes and checklists for additional mitigation activities

Company's experiences

- Many companies won't fill out the questionnaire
- Most companies negotiate hard on the terms, especially liability caps and CIP-013 R1.2 items
- Many companies aren't focused on the utility space and don't care about our compliance challenges

Ongoing Monitoring

Vendors assessments are good for a period of time for additional procurement based on overall assessed risk

Items reported as required by contract will be handled as warranted based on type of report/monitored item

- Cyber Incident Response
- HR/Personnel access management
- Business Unit operational changes

Risky or uncooperative vendors are not selected for additional purchases absent a compelling business driver

Questions



ConEd

Mikhail Falkovich, Director – Information Security

Eric Levenstein, Systems Manager – Information Security

Dina Mangialino, System Analyst – Information Security

Roles & Responsibilities

- Processes
 - Supply Chain Process
 - Regulatory Assessments (CIP-013)
 - Cyber Security Risk Evaluation Process

Vendor Risk Assessment Program

- Risk-based, tiered approach
 - Assessment of data received and/or work performed
 - Less stringent requirements for lower sensitivity engagements
- Attestations and questionnaires
 - Data Security Attestations for ESCOs
 - Light questionnaire for lower risk suppliers
 - Energy Sector Supply Chain Risk Questionnaire
- Security architecture review for solutions
 - Corporate instruction mandates IT review of technology solutions

Conducting Supplier Evaluations

- Evaluating Suppliers
 - Evaluation of supplier responses and security control audit reports
 - Questionnaire automation
 - Vendor categorization and risk identification
- Logistics
 - Completed questionnaires, supporting documentation, and assessments stored in centralized repository
 - Automated monitoring and tracking

Addressing Identified Risks and Ongoing Monitoring

- Vendor approval process
 - Standard process for approval
 - Conditional approval
 - Rejection
- Periodic evaluations
 - Tiered approach
- Contractual obligation to notify of cybersecurity incidents
- Evaluation post incident response

Questions



Panel Discussion and Q&A

We'll resume with the panelists'
discussion at 1:00 pm ET

Panelists

ConEd

- Mikhail Falkovich
- Eric Levenstein
- Dina Mangialino

Exelon

- Betsy Soehren-Jones
- Jennifer Burke
- Erin Holloway

FirstEnergy

- Scott Hipkins
- Marcus Noel
- Jason McCormick

PG&E

- Ray Grippo
- DeClan Kenna
- Ashikur Khan

Southern Company

- Shannon Hammett

TVA

- Vivian Schorle
- Brian Millard
- Frank Tritico
- Steven Briggs

Discussion Question

It's been discussed that collecting too much information could open entities up to risk – what is your perception of that?

Discussion Question

How does supply chain cyber security and/or CIP-013 inform/impact/affect your corporate cyber security program?

Discussion Question

Have you had suppliers refuse to provide information? How do you handle that and how do you consider it in your supplier evaluation?

Discussion Question

When you are narrowing down suppliers from a risk perspective, do you always use the same process or are there allowances for suppliers you've consistently worked with (historical knowledge)?

Discussion Question

How do you resolve differences if procurement favors one supplier (for any reason) but the supplier has more risk than other suppliers that can't be mitigated?

Discussion Question

This was covered by some of the presentations, but to the panelists – what consideration is given to the supplier evaluation in the procurement process?

Discussion Question

A question on logistics –
How do you track/log the supplier
evaluations?

Both by supplier and, if it varies by product,
by product?

Discussion Question

Are entities beginning to consider how to include EACMS, PACS and low impact into their overarching supply chain cyber security program?

Take-aways and Requests

Unite Your Company's Efforts

- Create cross departmental collaboration
- For collecting information, start with the NATF Criteria and Questionnaire
- Track what information you use in your evaluation

Converge Industry

- Provide feedback on
 - what information you're using in your supplier evaluations
 - How you obtain assurance
 - How you mitigate risks
- There are many ways to implement a common approach
- Size for your company keeping your approach effective and efficient

Pool Expertise

- Contributions from many organizations

Questions



NATF Contact Information

supplychain@natf.net

kkeels@natf.net

vagnew@natf.net