North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Supplier Sharing Call

March 22, 2023

Please Participate

- Raise your hand
  - We will unmute you
  - Make sure you are identified in the participant list
- Put a question or comment in the chat
- Put a question or comment in the Q&A

If you put a question or comment in the chat or Q&A but want to remain anonymous, please open with your request

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Opening Remarks

Tom Galloway
President and CEO, NATF
and
Frank Harrill
Vice President, Security, Schweitzer Engineering Laboratories (SEL)

Purpose of the Sharing Calls

- Provide an opportunity for suppliers to talk about cyber security issues and practices ranging from
  - How establish a security program, to
  - In-depth discussions on a specific technical challenge
- Leverage knowledge from lessons learned
- Share information
- Calls will be limited to suppliers unless otherwise noted

Contributing Organizations

- Aspen Technology / OSI
- Hitachi Energy
- International Society of Automation (ISA)
- National Electrical Manufacturers Association (NEMA)
- Schneider Electric
- Schweitzer Engineering Laboratories (SEL)
- Siemens
- Siemens Energy
- US Chamber of Commerce
- With support from:
  - Nebraska Public Power District
  - Southern Company
  - North American Transmission Forum (NATF)

Participants Available for Discussion/Questions

- Andre Ristaino (ISA)
- Andy Turke (Siemens Industry)
- Chris Fitzhugh (Siemens Energy)
- Frank Harrill (SEL)
- Rob Koziy (Aspen Technology / OSI)
- Steve Griffith (NEMA)

Please remember to either raise your hand to ask a question or you can put your question into the chat or Q&A.

Today's Agenda and Presenters

- Comments from a Customer - Jennifer Couch (Southern Co)
- Supplier Information and Good Responses
  - Entity/Customer and Supplier Panelists
- Use of Software Bills of Materials
  - Entity/Customer and Supplier Panelists
- Future Calls – Frank Harrill (SEL)

Comments from a Customer

Jennifer Couch, Southern Company

- View from the customer
- Value of the partnership
- We are in this together
- We’re all suppliers to someone

Future Calls

- Planned for approximately every 2 months from 1-2:30pm ET
  - May 24, 2023 – Open to NATF Members
  - July 19, 2023 – Suppliers only
  - Sept 27, 2023
  - Nov 29, 2023
- Calls are not recorded
- Slides will be available

Supplier Information

What information customers need,
what constitutes “good” responses to questions, and
the challenges for suppliers

Panelists

Entities/Customers

- Chuck Abell, Ameren
- Mikhail Falkovich, ConEd
- Tony Hall, LG&E and KU
- Tony Eddleman, NPPD
- Jennifer Couch, Southern Company

Suppliers

- Rob Koziy, Aspen Technology / OSI
- Frank Harrill, SEL
- Andy Turke, Siemens Industry
- Chris Fitzhugh, Siemens Energy

Supplier Panel Leads

How do you prepare for customer requests?

Entity Panel Leads

What information are you having difficulty obtaining from suppliers?

Areas of Information

- Top three
  - Vulnerability management
  - Asset, change and configuration Management
  - Event and incident response
- Followed by
  - Information/data protection
  - Cybersecurity tools and architecture
  - Risk management
- Then
  - Access control and management
  - Governance
  - Workforce management
  - Cybersecurity Program management
  - Mobile devices and applications

Information by NATF Criteria Number

•1 – Supplier establishes and maintains an **identity and access management program** that ensures sustainable, secure product manufacturing/development

•3 (a&b) – Supplier's personnel vetting process **allows supplier to share background check criteria and results with entity** for confirmation of process or verification of sampled employees

•8 - Supplier **maintains an access list** of all individuals with access to entity's assets, information and facilities

•13 - Supplier **notifies entity of any revocations** affecting electronic or unescorted physical access into entity's assets or facilities **within 4 hours** of either a change in business need for access or termination

- If supplier cannot notify entity in 4 hours, provide the number of hours supplier needs

Information by NATF Questionnaire Number

•IAM-02 - Do you establish and maintain an identity and **access management program** that ensures sustainable, secure product manufacturing and development?

•IAM-06 - Do you maintain an **access list of all individuals** with access to utility's assets, information and facilities?

•CHNG-08 - Will the utility be **notified of major changes to the computing system environment** that could impact the utility's security posture?

•EIR-02 - Does your cyber incident response plan contain a requirement to **notify purchasers of the impacted products or services** within 24 hours of initiation of your plan? (Criteria #36 = within 2 hours)

Information by NATF Questionnaire Number

•RISK-03 - Do you use **trusted and controlled distribution for electronic shipment** of all products?

•RISK-04 - Do you have a means by which **purchaser can verify the source of software, firmware, patch, and data downloads is authentic**?

•RISK-05 - Do you have a process through which **you investigate whether computer viruses or malware are present** in any software or patches before providing such software or patches?

•RISK-09 - Do you establish and maintain **a security program** for the product(s) or service(s) being purchased, including implemented processes to **verify the integrity and authenticity of the software, patches, and firmware** relevant to the product(s) or service(s) being delivered to the utility?

•RISK-10 - Do you use a **secure central software repository** after software, patches, and firmware authenticity and integrity have been validated, so that authenticity and integrity checks do not need to be performed before each installation?

Entity Observations

- There are some types of information that are difficult for suppliers to provide, although it varies from supplier to supplier
- Members get more complete information when suppliers have questionnaire responses prepared
- Members can get more information from a supplier if they have a relationship with them
- Confidentiality is a major concern for suppliers
- Suppliers struggle with access controls questions (e.g., background checks, chain of custody/access controls for products in their environment)

Possible Disconnects

- Information is confidential
- Suppliers are more comfortable with customers they do more business with
- Suppliers may not know answers
- Entities may not be asking the right person in the supplier organization
- Suppliers may be under-resourced; smaller suppliers have more difficulty
- Responses are not prepared ahead of time so each request is a unique effort
- Suppliers aren’t sure what customers want in the responses
- The questions may not be clear, may have multiple questions embedded in one or may not be logically organized
- Entities are modifying questionnaires
- Entities may not be clear whether they are asking about the supplier security practices or a product – which may or may not be the same
- Suppliers can create supply chain cyber security policies to align with their customers' needs

Entity Panel Leads

What constitutes a “good” response to a supplier question?

Entities Lead

- What elements do you consider part of a “good” response
  - Timely
  - Certifications or Assessments
  - Honesty
  - A clear response to every question
  - Straight “yes” or “no” response to the question, with “partially” as necessary, supported by:
    - What type of evidence the suppliers has to support the response, including the name/number/revision date of the evidence, even it they can’t provide it
    - If no, why?
    - If the supplier responses “partially”, what they’ve done and if other actions are in progress

Entities Lead

- What elements do you consider part of a “bad” response
  - Inaccurate Reponses
  - “No” is not a bad answer – it allows for risk assessment and mitigations if needed

Potential Paths Forward

- Suppliers should ensure that the questions are answered fully
- Entities can refine questions so there aren’t multiple items to address in each question
- Suppliers could maintain responses to the questionnaire so they could respond to requests rapidly
- Consider the security implications with the use of macros
- Consider using the questionnaire or criteria without modifications
- Drive content convergence across various assessment platforms
- Increase reliance on third-party certifications and assessments

Use of Software Bills of Materials (SBOMs)

How entities/customers are currently using, or envision using, SBOM information

Panelists

Entities/Customers

- Chuck Abell, Ameren
- Mikhail Falkovich, ConEd
- Tony Hall, LG&E and KU
- Tony Eddleman, NPPD
- Jennifer Couch, Southern Company

Suppliers

- Rob Koziy, Aspen Technology / OSI
- Frank Harrill, SEL
- Andy Turke, Siemens Industry
- Chris Fitzhugh, Siemens Energy

Entity Panel Leads

How do you currently use,
or envision using,
SBOM information?

Supplier Panel Leads

What is available for software and hardware Bills of Materials and assurances?

Supplier Panel Leads

What challenges are associated with providing SBOMs or services related to SBOMs?

Values of SBOMs

- SBOMs are invaluable to a supplier
  - Components must be continuously monitored for the existence of vulnerabilities and continuity of support
- The utility of an SBOM to a customer is more difficult to measure
  - Vulnerability Exploitability eXchange (VEX) document
  - Update cadence
  - Depth
  - Third-party solution providers
  - Supplier vulnerability advisories
  - Secure development lifecycle certification

SBOMs – Current State

- The concept should be well-established, even if the SBOM term is new
- EO 14028, *Improving the Nation's Cybersecurity*
  - Minimum elements from NTIA
- CISA workstreams
  - Cloud and online applications
  - On-ramps and adoption
  - Sharing and exchange
  - Tooling and implementation
- Sharing formats
  - CycloneDX (CDX)
  - Software package data exchange (SPDX)

Value of Third-Party Secure Product Development Certification such as the ISA 62443*

For more information, see:
ISASecure SDLA 312-62443-4-1 assessment specification
and
www.isasecure.org

1	Development process
2	Identification of responsibilities
3	Identification of applicability
4	Security expertise
5	Process scoping
6	File integrity
7	Development environment security
8	Controls for private keys
9	Security requirements for externally provided components
10	Custom developed components from third-party
11	Assessing and addressing security-related issues
12	Process verification
13	Continuous improvement
14	Product security context
15	Threat model
16	Product security requirements
17	Product security requirements content
18	Security requirements review
19	Secure design principles
20	Defense in depth design
21	Security design review
22	Secure design best practices
23	Security implementation review
24	Secure coding standards
25	Security requirements testing
26	Threat mitigation testing
27	Vulnerability testing
28	Penetration testing
29	Independence of testers
30	Receiving notifications of security-related issues
31	Reviewing security-related issues
32	Assessing security-related issues
33	Addressing security-related issues
34	Disclosing security-related issues
35	Periodic review of security defect management practice
36	Security update qualification
37	Security update documentation
38	Dependent component or operating system security update documentation
39	Security update delivery
40	Timely delivery of security patches
41	Product defense in depth
42	Defense in depth measures expected in the environment
43	Security hardening guidelines
44	Secure disposal guidelines
45	Secure operation guidelines
46	Account management guidelines
47	Documentation review

**The NATF and this supplier group does not endorse any specific certification*

Questions

Future Calls

- **Mark your calendar for future calls – all are from 1pm-2:30pm eastern!**
- **May 24** – *the call will be open to suppliers and NATF companies*
  - What do regulations require of entities? Overview of NERC CIP standards and CMMC (IEC 27001 & ISA/IEC 62443)
  - How can suppliers partner with entities for efficient compliance management? What are the pain points or gaps for providing information?
- **July 19** – *the call will be exclusively for suppliers to address areas identified on the March and May calls*

Questions

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Thank you for attending!

NATF Contact Information

supplychain@natf.net

dearley@natf.net

rstewart@natf.net

vagnew@natf.net