North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Supplier Sharing Call

May 24, 2023

Open Distribution for Supply Chain Materials
Copyright © 2023 North American Transmission Forum ("NATF"). All rights reserved.

The NATF permits the use of the content contained herein ("Content"), without modification; however, any such use must include this notice and reference the associated NATF document name & version number. 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.

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

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)
- Heath Knakmuhs (US Chamber of Commerce)
- Michael Pyle (SE)

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)*
- What do regulations require of your customers? – *Tony Hall (LG&E and KU)*
- How can suppliers partner with customers for efficient compliance management? – *Supplier and NATF Member Companies Panel Discussion*
- Use of Software Bills of Materials – *Supplier and NATF Member Companies Panel Discussion*
- 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
  - July 18
  - July 19, 2023 – This call has been replaced with an in-person supplier workshop on July 18
  - Sept 27, 2023
  - Nov 29, 2023
- Calls are not recorded
- Slides will be available

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Supply Chain Regulations

Tony Hall
Manager Cyber Infrastructure Protection Program, LG&E and KU Energy

NERC Supply Chain Reliability Standards

In response to FERC Order No. 829, NERC Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management developed new Reliability Standard CIP-013-1 and modified Reliability Standards CIP-005-6 and CIP-010-3, which collectively have become known as the "supply chain standards."

- CIP-013-1, CIP-005-6, and CIP-010-3 became effective 10/1/2020

Currently effective standards became effective on 10/1/2022

- CIP-013-2, CIP-005-7 and CIP-010-4

These standards are a part of the Critical Infrastructure Protection (CIP) standards family.

NERC CIP Reliability Standards

CIP-002 – Critical Cyber Asset Identification
CIP-003 – Security Management Controls
CIP-004 – Personnel & Training
CIP-005 – Electric Security Perimeter(s)
CIP-006 – Physical Security of Critical Cyber Assets
CIP-007 – Systems Security Management
CIP-008 – Incident Reporting and Response Planning
CIP-009 – Recovery Plans for Critical Cyber Assets
CIP-010 – Configurations Change Management and Vulnerability Assessments
CIP-011 – Information Protection
CIP-012 – Communications between Control Centers
CIP-013 – Supply Chain Risk Management
CIP-014 - Physical Security

NERC CIP-013 R1 Requirements*

R1. 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 and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated remote access.

* Draft CIP-013-2_QR (nerc.com)

NERC CIP-013 R1 Measures*

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

* Draft CIP-013-2_QR (nerc.com)

NERC CIP-013 R2 Requirements*

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

* Draft CIP-013-2_ QR (nerc.com)

NERC CIP-013 R2 Measures*

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

* Draft CIP-013-2_QR (nerc.com)

NERC CIP-013 R3 Requirements*

R3. 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. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

* Draft CIP-013-2_QR (nerc.com)

NERC CIP-013 R3 Measures*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

* Draft CIP-013-2_QR (nerc.com)

NERC Projects that could affect Supply Chain

- Current Standards under Development
  - 2016-02 Modifications to CIP Standards
  - 2022-05 Modifications to CIP-008 Reporting Thresholds
  - 2023-04 Modifications to CIP-003

- Standards with upcoming Enforceable dates
  - 2019-02 BES Cyber System Information – enforceable date – 1/1/2024
  - 2020-03 Supply Chain for Low Impact Revisions – enforceable date – 4/1/2026

Discussion

How can suppliers partner with customers for efficient compliance management?

Panelists

Entities/Customers

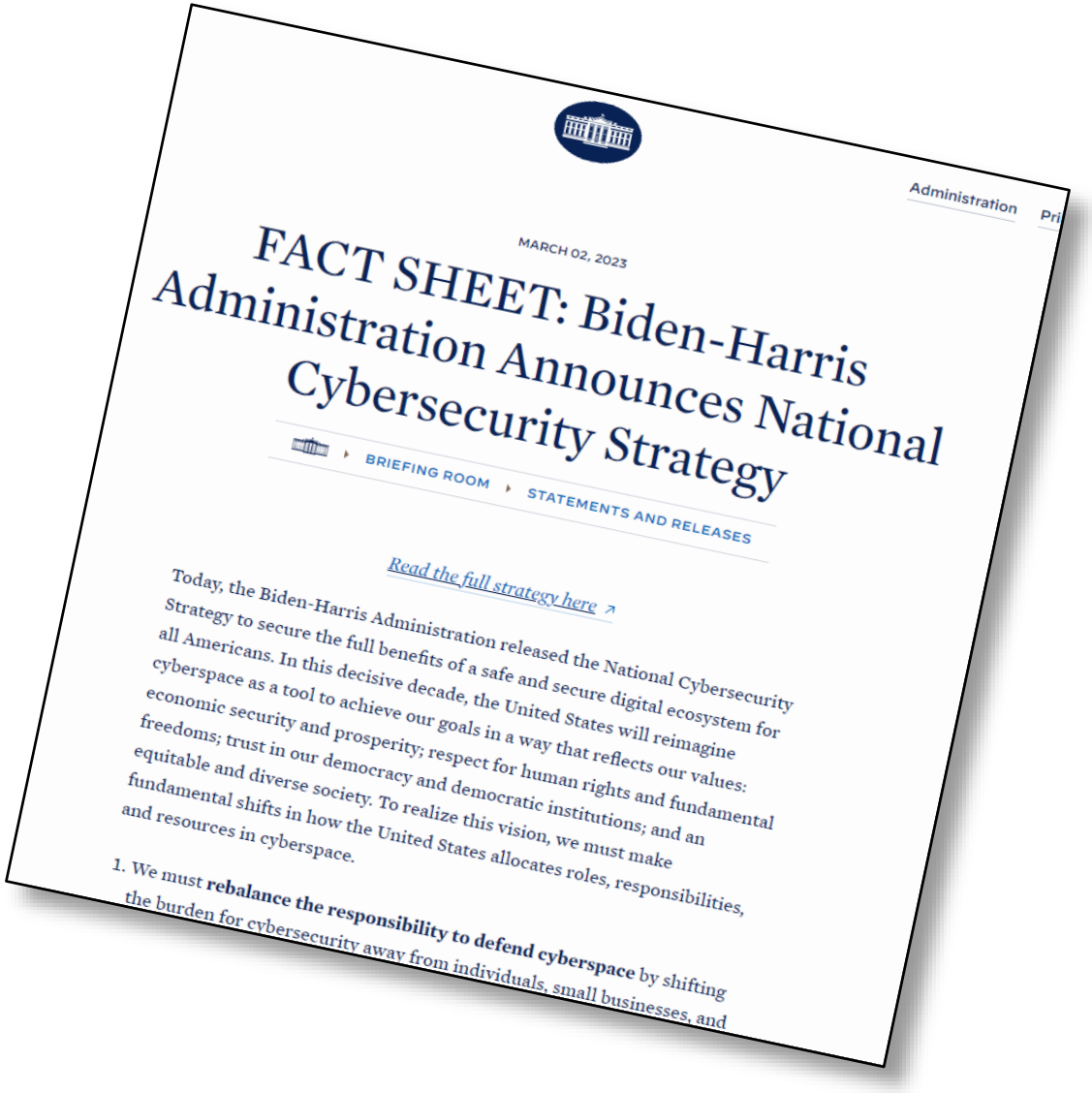
- Mikhail Falkovich, ConEd
- Valerie Ney, First Energy
- Tony Hall, LG&E and KU
- Jennifer Couch, Southern Company

Suppliers

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

Direction: National Cybersecurity Strategy

NCS Fact Sheet:
https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/



Administration

MARCH 02, 2023

FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy

BRIEFING ROOM › STATEMENTS AND RELEASES

Read the full strategy here ↗

Today, the Biden-Harris Administration released the National Cybersecurity Strategy to secure the full benefits of a safe and secure digital ecosystem for all Americans. In this decisive decade, the United States will reimagine cyberspace as a tool to achieve our goals in a way that reflects our values: economic security and prosperity; respect for human rights and fundamental freedoms; trust in our democracy and democratic institutions; and an equitable and diverse society. To realize this vision, we must make fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace.

1. We must **rebalance the responsibility to defend cyberspace** by shifting the burden for cybersecurity away from individuals, small businesses, and

Summary: National Cybersecurity Strategy

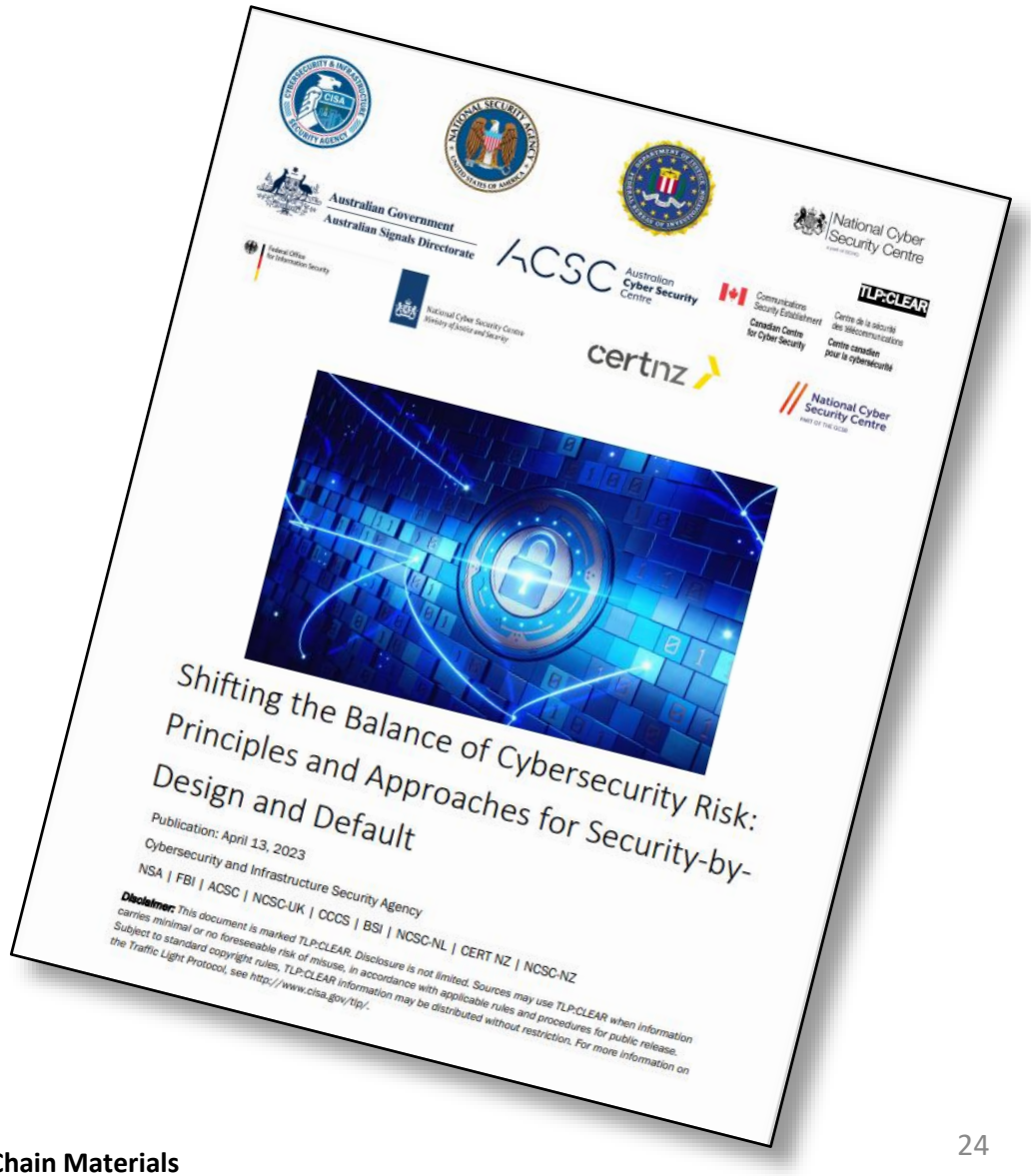
Complex threat environment and evolving technologies demand a more intentional, more coordinated, and more well-resourced approach to cyber defense

- Defend Critical Infrastructure
- Disrupt and Dismantle Threat Actors
- Shape Market Forces to Drive Security and Resilience
- Invest in a Resilient Future
- Forge International Partnerships to Pursue Shared Goals

Supporting the National Cybersecurity Strategy

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default

https://media.defense.gov/2023/Apr/13/2003198917/-1/-1/0/CSI_SECURE_BY_DESIGN_DEFAULT.PDF



Use of Software Bills of Materials (SBOMs)

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

Panelists

Entities/Customers

- Mikhail Falkovich, ConEd
- Valerie Ney, First Energy
- Tony Hall, LG&E and KU
- 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 Workshop and Calls

- **Supplier Workshop: July 18 in Charlotte, NC**

Mark your calendar for future calls – all are from 1pm-2:30pm eastern!

- **Sept 27, 2023**
- **Nov 29, 2023**

Let us know what topics you would like to have on the agendas!

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