North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Supplier Sharing Call

January 25, 2023

Open Distribution for Supply Chain Materials

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

Opening Remarks

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

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

Today’s Agenda and Presenters

- Comments from a Customer - Jennifer Couch (Southern Co)
- Being Prepared for Government Actions – Michael Pyle (Schneider Electric) and Heath Knakmuhs (US Chamber of Commerce)
- Provenance Concerns – Michael Pyle (Schneider Electric)
- Use of Software Bills of Material – Frank Harrill (SEL), Chris Fitzhugh (Siemens Energy) and Andre Ristaino (ISA)
- Cyber Readiness Institute – Lessie Longstreet
- Future Topics – 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

Participants Available for Discussion/Questions

- Andre Ristaino (ISA)
- Steve Griffith (NEMA)
- Michael Pyle (Schneider Electric)
- Frank Harrill (SEL)
- Chris Fitzhugh (Siemens Energy)
- Heath Knakmuhs (US Chamber of Commerce)
- Jon Terrell (Hitachi Energy)

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

Future Calls

- Planned for approximately every 2 months from 1-2:30pm ET
  - March 22, 2023 – Open to NATF Members
  - May 24, 2023 – Open to NATF Members
  - July 19, 2023
  - Sept 27, 2023
  - Nov 29, 2023
- Could keep a main topic for the call to 1 hour with a special group break-out (e.g., small suppliers) for the last half hour
  - There will be a poll at the end of the call
- Calls are not recorded
- Slides will be available

slido

Join at slido.com
#5022163

ⓘ Start presenting to display the joining instructions on this slide.

Being Prepared for Government Actions

Michael Pyle
Director of Product Cyber Security, Schneider Electric
and
Heath Knakmuhs
Vice President and Policy Counsel, US Chamber of Commerce

Staying One Step Ahead

- *Status quo* of rational regulation from most governments
  - Any forcing mechanism upends this dynamic
  - Executive and Legislative interest remains high in the absence of a forcing “event”
- Adopt best practices/pragmatic approaches to security – both for individual and collective industry benefit
- Well-developed and vetted industry practices/structures are preferable to rushed regulations of government origin
- Relationship between establishment of security practices/hygiene and identification of new vulnerabilities
  - Practices to combat new vulnerabilities should feed into security practices
  - Security practices should support the identification and defense from new vulnerabilities

If suppliers can prevent “bad things” from happening the need for spontaneous and unvetted regulation should be mitigated

Strategic and Tactical Approach

Tactical Actions

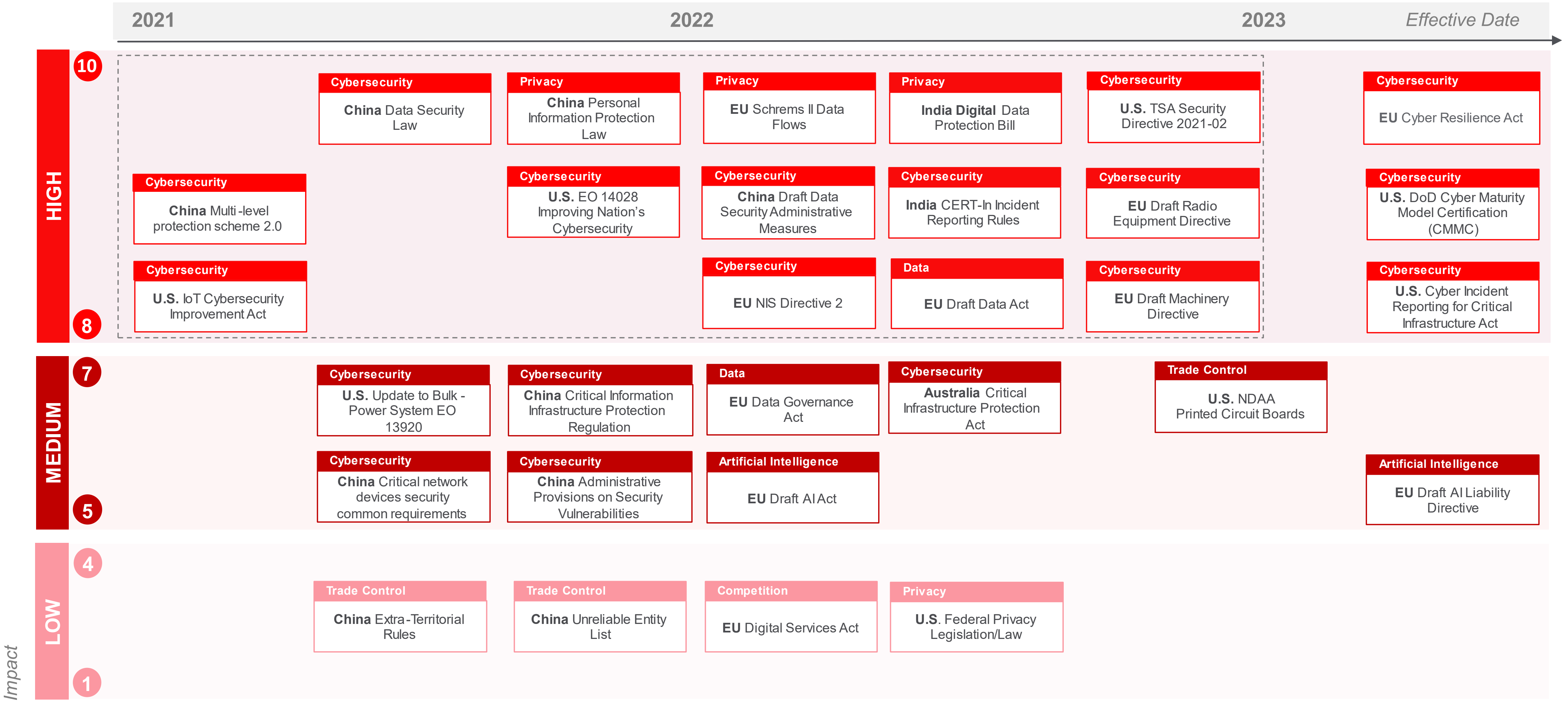
- Adopt best practices/pragmatic approaches to security for both product development and your enterprise aligned with relevant International Standards e.g., ISA/IEC 62443, CISA cross-sectoral cyber performance goals, etc.
- Implement policies and processes to comply with regulations for your own systems
- Encourage customers to adopt best practices for their Enterprise & OT systems

Strategic Actions

- Incorporate capabilities into products that facilitate end user compliance with regulations
- Threat modeling to ensure your controls keep pace with the evolving threat landscape
- Invest in a regulatory tracking position/function for your business

Global Digital Policy Heatmap (for Illustrative Purposes Only)

One example method for tracking regulations



HIGH

- Cybersecurity: China Data Security Law
- Privacy: China Personal Information Protection Law
- Privacy: EU Schrems II Data Flows
- Privacy: India Digital Data Protection Bill
- Cybersecurity: U.S. TSA Security Directive 2021-02
- Cybersecurity: EU Cyber Resilience Act
- Cybersecurity: China Multi-level protection scheme 2.0
- Cybersecurity: U.S. EO 14028 Improving Nation's Cybersecurity
- Cybersecurity: China Draft Data Security Administrative Measures
- Cybersecurity: India CERT-In Incident Reporting Rules
- Cybersecurity: EU Draft Radio Equipment Directive
- Cybersecurity: U.S. DoD Cyber Maturity Model Certification (CMMC)
- Cybersecurity: U.S. IoT Cybersecurity Improvement Act
- Cybersecurity: EU NIS Directive 2
- Data: EU Draft Data Act
- Cybersecurity: EU Draft Machinery Directive
- Cybersecurity: U.S. Cyber Incident Reporting for Critical Infrastructure Act

MEDIUM

- Cybersecurity: U.S. Update to Bulk -Power System EO 13920
- Cybersecurity: China Critical Information Infrastructure Protection Regulation
- Data: EU Data Governance Act
- Cybersecurity: Australia Critical Infrastructure Protection Act
- Trade Control: U.S. NDAA Printed Circuit Boards
- Cybersecurity: China Critical network devices security common requirements
- Cybersecurity: China Administrative Provisions on Security Vulnerabilities
- Artificial Intelligence: EU Draft AI Act
- Artificial Intelligence: EU Draft AI Liability Directive

LOW

- Trade Control: China Extra-Territorial Rules
- Trade Control: China Unreliable Entity List
- Competition: EU Digital Services Act
- Privacy: U.S. Federal Privacy Legislation/Law

North American Transmission FORUM

Provenance Concerns

Michael Pyle

Director of Product Cyber Security, Schneider Electric

Understanding Provenance

NIST 800-53 Rev 5 defines Provenance as:

> *The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data*

Provenance considerations can not only cover software and firmware, including open source, but logic hardware components as well

Suppliers must take ownership for knowing the provenance of components provided by their suppliers, and require the same of those suppliers

Addressing Provenance

Establish a policy and acceptance criteria governing provenance that is applied upfront in the procurement/decision to use process

- For open source, review the location and nationalities of those on the governance board – who is making the commits?
- Where possible use North American suppliers; avoid adversarial environments
- Apply standard contract language covering provenance
- Include provenance when evaluating supplier risk

Addressing Provenance

Utilize the NERC guidance developed by the Supply Chain Working Group:

Security Guideline for the Electric Sector - Supply Chain: Provenance
https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Provenance.pdf

Security Guideline: Risk Considerations for Open Source Software:
https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Risk_Considerations_Open_Source_Software.pdf [nerc.com]

Trust but Verify

- Conduct your own analysis when possible, such as binary code analysis, running in a sand-boxed environment, and even source code review and tear-downs

Use of Software Bills of Materials (SBOMs)

Frank Harrill
Vice President, Security, Schweitzer Engineering Laboratories (SEL)
and
Chris Fitzhugh
Industrial Cybersecurity Consultant for North America, Siemens Energy
with
Andre Ristaino
Managing Director, Global Consortia, Conformity Assessment, International Society of Automation (ISA)

The Importance of an SBOM

- 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

Cyber Readiness Institute

Lessie Longstreet

Global Director of Outreach and Partner Engagement, CRI

CYBER READINESS
INSTITUTE

The Cyber Readiness Institute

- Convenes senior leaders of global companies and supply chain partners
- Shares cybersecurity best practices and resources
- Develops **free** content and tools to improve the Cyber Readiness of small and medium-sized enterprises

ExxonMobil

THE CENTER FOR
GLOBAL
ENTERPRISE

gm

Principal℠

Microsoft

Free Cyber Readiness Institute Resources

- Cyber Readiness Program: *https://cyberreadinessinstitute.org/the-program/*
- Cyber Leader Certification Program: *https://programs.cyberreadinessinstitute.org/courses/cyber-leader-program*
- Starter Kit: *https://cyberreadinessinstitute.org/starter-kit/*
- Ransomware Playbook: *https://cyberreadinessinstitute.org/quick-facts-from-the-ransomware-playbook/*
- Visit **BeCyberReady.com** for even more resources
- Contact: Lessie Longstreet llongstreet@cyberreadinessinstitute.org if you have specific questions

CYBER READINESS
INSTITUTE

Change Behavior.
Be Cyber Ready.

Visit us at BeCyberReady.com

@cyber-readiness-institute

@Cyber_Readiness

@CyberReadinessInstitute

Programs
Starter Kit
Champions
About CRI
Resources
CYBER READINESS INSTITUTE
Be Cyber Ready. Stay Cyber Strong.
Protect Your Business With the Cyber Readiness Program
Start Your Program
Our Story Video
Cyber Readiness Program
0% complete
Learn the 4 Core Cyber Issues

CYBER READINESS
INSTITUTE

Future Calls

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

- **March 22** – *the call will be open to suppliers and NATF companies*
  - What information entities need, but may be having difficulty getting, from suppliers to meet regulatory requirements and/or audits.
  - How are entities using SBOMs?

- **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*

Future Calls

- What would you like to talk about during the next call or a future call? Deeper dive
- Would you like to have a separate break out for small suppliers? Or a different subgroups?
- Several ways to respond to these questions:
  - Respond to the Slido poll
  - Join the conversation (raise your hand or put a comment in the chat or Q&A)
  - Send an email to one of the NATF staff members or to your NEMA or US Chamber of Commerce representatives

slido

What topics would you like to have discussed in depth on future calls?

ⓘ Start presenting to display the poll results on this slide.

slido

Would you like to have specific sessions for the following types of suppliers?

ⓘ Start presenting to display the poll results on this slide.

Questions

Thank you for attending!

NATF Contact Information

supplychain@natf.net

dearley@natf.net

rstewart@natf.net

vagnew@natf.net