

# Supplier Sharing Call

December 7, 2022

## **Open Distribution for Supply Chain Materials**

Copyright © 2022 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*

# Opening Remarks

Frank Harrill, Schweitzer Engineering Labs (SEL)

# Purpose of the Sharing Calls

Chris Fitzhugh, Siemens Energy

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

# Contributing Organizations

Chris Fitzhugh, Siemens Energy

- Hitachi Energy
- International Society of Automation (ISA)
- National Electrical Manufacturers Association (NEMA)
- Schneider Electric
- Schweitzer Engineering Labs (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

Chris Fitzhugh, Siemens Energy

- Introductions – Chris Fitzhugh (Siemens Energy)
- Entity Remarks - Jennifer Couch (Southern Co)
- Future calls – Steve Griffith (NEMA)
- Certifications and Security Frameworks – Andre Ristaino (ISA)
- Future Topics – Andre Ristaino (ISA)

# Participants Available for Discussion/Questions

- Andre Ristaino (ISA)
- Steve Griffith (NEMA)
- Andy Turke (Siemens)
- Chris Fitzhugh (Siemens Energy)
- Frank Harrill (SEL)
- 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.*

# 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

Steve Griffith, NEMA

- Planned for approximately every 2 months from 1-2:30pm ET
  - Jan 25, 2023
  - March 22, 2023
  - May 24, 2023
  - 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](https://slido.com)  
#5022163

ⓘ Start presenting to display the joining instructions on this slide.  
**CONFIDENTIAL – Restricted Distribution**

slido



What is your end use market?

① Start presenting to display the poll results on this slide.  
**CONFIDENTIAL – Restricted Distribution**

slido



**What is the annual revenue of your company?**

ⓘ Start presenting to display the poll results on this slide.  
**CONFIDENTIAL – Restricted Distribution**

slido



**How many employees does your company have?**

① Start presenting to display the poll results on this slide.  
**CONFIDENTIAL – Restricted Distribution**

slido



**In what country(ies) does your company sell products or provide services?**

① Start presenting to display the poll results on this slide.  
**CONFIDENTIAL – Restricted Distribution**

# slido



**What certifications or assessments offered by qualified third parties does your company have?**

ⓘ Start presenting to display the poll results on this slide.  
**CONFIDENTIAL – Restricted Distribution**

# slido



**If you responded "other" to the prior question, please identify the certification or assessment.**

① Start presenting to display the poll results on this slide.  
**CONFIDENTIAL – Restricted Distribution**



# Certifications and Security Frameworks

Andre Ristaino, International Society of Automation

# Definitions

## What is a Standard?

Examples: NIST 800-52, ISA/IEC 62443

A standard is a specification developed and published by an accredited standards development organization (SDO) or accredited standard setting organization (SSO) or authoritative government entity such as a regulatory authority (NERC, TSA).

Standards contain language describing specific controls or security requirements in this discussion that can be used for assessments and/or certification of the operating site security capabilities; or supplier product security capabilities .

Standards include requirements with language that use words like 'shall' or 'must'. These are known as 'normative requirements' (shall, must) that can be assessed.

# Definitions

## Best Practices

Examples: CISA Guidance, FDA cGMP, Industry Guidance (AMA)

Best practices are less formal than standards and known to produce good outcomes if followed. Best practices are often based on normative standards.

# Definitions

## Security Framework

NIST CSF is a good example

The NIST CSF provides a structured approach for addressing security at operating sites based on a repeating set of practices. However, the framework does not contain specific controls or security requirements that can be used for assessments of the operating site security capabilities. A framework is not a standard.

The NIST CSF does include informational references to other NIST standards and other industry standards for ‘implementation details’, such as ISA/IEC 62443-2-1, ISA/IEC 62443-3-3 and, ISO 27001. The referenced standards include normative requirements (shall, must) and controls that can be assessed.

# Definitions

## Assessment

An assessment measures the **extent to which an entity conforms** to a standard or specification. It is not a certification.

An assessment typically produces a report identifying requirements that have been met and requirements that have not been met for a standard/specification. Assessments are often conducted by an internal auditor for gap analysis and process/product improvement.

Assessments can include multiple dimensions such as process reviews, testing, product capabilities identification. Assessments do not need to be conducted by an accredited certification body.

# Definitions

## Certification

Certifications are a confirmation that **all requirements** are met for a standard. The following discussion is based on certifying commercial off the shelf (COTS) products; not solutions deployed at an operating site.

Certifications are also known as ‘conformity assessments’ because they certify that a product, process, entity, person **conforms to all requirements** in a standard or specification.

For example, an ISA/IEC 62443-4-2 product certification certifies that a COTS industrial device conforms to all 120 requirements in the ISA/IEC 62443-4-2 cybersecurity standard.

Certifications are conducted by certification bodies (CB) that have been ‘accredited’ by ISO 17011 Accrediting Authorities (AB) for competence and independence to perform the certifications.

The International Society of Automation operates a global certification scheme under the ISASecure brand that certifies that supplier *components, systems, and development processes conform to the ISA/IEC 62443-4-2, ISA/IEC 62443-3-3, and ISA/IEC 62443-4-1 standards respectively.*

# Definitions

## Certifications continued

1. A certification may consist of **testing** only. FCC radio testing for power output is an example.
2. A certification may consist of an **audit** only. NERC-CIP audits to confirm operator adherence to operational process, policies, and procedures is an example.
3. A certification may consist of an **inspection**. A review of product documentation to confirm that it includes a description of security settings and secure installation instructions.
4. A certification may consist of an **assessment**. A review of product security capabilities like MFA, encryption, for example; and the assessor guidance may require **hands-on** validation or product **document reviews**.

# Definitions - Certifications: point-in-time versus ongoing

A certification may consist of a **single assessment of the COTS product** that provides assurances for a product/version/release as submitted on a specific date without any re-assessments as the product evolves. This is **point-in-time** certification.

- Pros – less administrative complexity, lower cost, gives a quick snapshot
- Cons – Does not represent the security capabilities of an evolving product. It can be misleading and out-of-date.



# Definitions – Certifications with ongoing maintenance policies

For example, ISASecure ISA/IEC 62443 product certifications consist of:

1. **Initial evaluation**-Product must be under configuration control.
  - a) product security capability **assessment** (ISA/IEC 62443-4-2)
  - b) product development process **audit** (ISA/IEC 62443-4-1 includes review of testing artifacts and BOMs)
  - c) product known vulnerability identification **test**. (Tenable Nessus scans against US CERT NVDB)
2. **Maintenance of certification** – for product is based on *updates vs upgrades* as defined by the ISA/IEC 62443-4-2 standard.
  - a) Updates (security/bug patch)
  - b) Upgrades (version release with added functionality).

# Definitions – Maintenance of Certification for a product *upgrade*

Ongoing **maintenance of certification** as the product evolves. For product *upgrades* as defined in the ISA/IEC 62443-4-2 standard:

1. The scope of product upgrades (version release changes) are evaluated by the CB and the product is re-assessed like an initial certification, possibly bypassing non-applicable assessment steps based on scope evaluation and risk.
  - When support for a product version is terminated by the supplier, the certification is also voided.
  - For industrial automation systems, product *upgrade* cycles are typically 3-7 year version release cycles.

# Definitions – Maintenance of Certification for a product *updates*

Ongoing **maintenance of certification** as the product is ***updated***. For product ***updates*** as defined in the ISA/IEC 62443-4-2 standard:

1. No CB review is performed when suppliers issue product ***updates*** for bug fixes and security patches.
  - The product must stay under configuration control within the suppliers SDL already certified to the ISA/IEC 62443-4-1 standard.
  - The supplier SDL is audited every 36 months after initial certification.
  - Suppliers are audited every 24 months to ensure they meet specified market response times for addressing new vulnerabilities identified in their certified products.

# Definitions

## Statements of Applicability (SoA)

A SoA for ISO 27001 summarizes your organization's position on each of the 114 information security controls outlined in Annex A of ISO 27001. Under the SoA approach, the entity under evaluation specifies which requirements are applicable.

Clause 6.1.3 of the Standard states an SoA must:

- Identify which controls an organization has selected to tackle identified risks;
- Explain why these have been selected;
- State whether or not the organization has implemented the controls; and
- Explain why any controls have been omitted.

Every control should have its own entry, and in cases where the control has been selected, the SoA should link to relevant documentation about its implementation.

# Definitions

## Attestation / Self-Attestation

A supplier or entity provides a written document declaring conformance/compliance to a specification/standard/regulation.

This approach may be an informal, voluntary activity conducted by a supplier.

Attestation/Self-attestation may also operate under a formal certification scheme with the supplier agreeing to specific terms such as random audits and/or penalties for non-conformance violations.

# Definitions

## Qualified Third Party

A qualified third party (3PAO-third party assessment organization) is an independent assessment organization that has been accredited to conduct assessments and/or certification activity in a specific domain.

A 3PAO is typically evaluated by an accrediting authority using consensus accrediting requirements developed by an industry group or other oversight organization to certify the 3PAO. Typical accreditation topics include conflicts of interest, technical capabilities, and credentialing of assessors/auditors.

Product certification bodies and testing laboratories are examples; typically accredited to ISO 17065 and/or ISO 17025 such as with the ISASecure scheme.

# Examples

Security Framework/Standards	Applicable to	Assessment	Certification	Qualified 3rd party
NIST CSF	Owners/ Operators	Yes	No governance	Consultants & 'certified' CSF assessors
CMMC (Controls from NIST 800-171)	Government Suppliers	No	Yes	Yes
FedRamp (Controls from NIST 800-53)	Suppliers Using Cloud	No	Yes	Yes
ISO 27001	Supplier IT	Yes	Yes	Yes
NATF Criteria/Questionnaire (information gathering tools)	Suppliers	Maps to Frameworks	Maps to Frameworks	Looks to ISO, ISA/IEC and other standards
NERC-CIP (Owner/Operator)	Owners/ Operators	No	No	Regulator-audited
ISA/IEC 62443	Suppliers/ Service Providers/ Operators	Yes	Yes	Yes
Industry Best Practice Specification	Owner/ Operator	Yes	Sometimes	Sometimes
Cloud Security Alliance (CSA)	Supplier Controls	Yes	Yes	Yes
SOC 2 Type II	Supplier Controls	Yes	No	Yes

# Supplier Focused Organization Standards and Certifications

- ISO-27001 can be used to provide assurances that a supplier's administrative IT systems meet requirements for ensuring the security of the supplier's information and security of information shared by the supplier's customers.
- ISA/IEC 62443-2-1 can be used to provide assurances that a supplier who is a manufacturer of products (control systems) meets requirements for ensuring the security of its manufacturing/production systems. This adds confidence regarding the continuity of product supply and defends against product defects (accidental or intentional) resulting from malicious tampering, poor development/production security, and/or supply chain vulnerabilities.



# COTS Product Focused Security Standards

- ISA/IEC 62443-4-1, 4-2, 3-3, 2-3
- NERC – n/a
- NISTR 8425 – Consumer IOT security
- ETSI 303 645 – EU Cyber Security for Consumer Internet of Things-baseline
- NIST – 800-xxx
- UL2900
- CIS – (Center for Internet Security) specifications/practices
- CSA- (Cloud Security Alliance) specifications/practices
- *NERC website has a table mapping NERC CIP to other standards*

# Product Focused Example

## ISA/IEC 62443-4-2

- Provides requirements (objective measures) for product **security capabilities** at 4 levels of security.
- Establishes security **development process** requirements in 8 practice areas (based on ISA/IEC 62443-4-1) in a supplier's product development process (SDL).
  - Ensures that the supplier's SDL includes processes necessary for designing security into their products (at one of 4 levels), for secure development, and for testing and release.
  - Ensures supplier has processes/playbook in place for responding to cyber incidents involving their products.

# Controls Focused

- SOC 2 Type 2 – Assessment conducted of a supplier typically done by CPA
- CSA – provides assurances of implementation of CSA defined best practices / controls for cloud providers and offers certifications for cloud providers

# Common Misperceptions

- Certification only shows a point in time for products
  - This may be true where the 'certification' is a single test, 'teardown' or pen test regimen.
  - A good scheme will include policies and practices to ensure that a product maintains its certification as the product is upgraded and updated during its lifecycle.
- Audit reviews are not sufficiently thorough
  - This may be true for a poorly designed audit program.
  - Governance is key to this.
  - A balance must always be struck between designing an overly burdensome audit specification versus a marginally useful 'lightweight' audit specification.
  - For product certifications, audits alone may not be sufficient. Some testing may be necessary along with assessments of product capabilities identified in the product literature.

# Leveraging Your Certifications

- Use your certifications as evidence of your questionnaire responses.
  - It is important to develop a cross reference document to confirm/demonstrate which questionnaire responses are verified by the requirements covered in the certification. You will only need to do this once.
- In negotiations for contract terms
  - Where your certifications demonstrate superior performance in the security dimension of your offerings, highlight the credibility of the certification and seek preferential pricing and terms.

# Meeting Regulatory Requirements

- Questionnaires are necessary to demonstrate compliance to regulatory requirements.
  - Certifications can be linked to show compliance.
  - Suppliers can demonstrate their due diligence efforts. 3PAO certifications provide independent evidence and peace of mind.

# No Cost Resource Awareness

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





# 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](mailto:llongstreet@cyberreadinessinstitute.org) if you have specific questions


CYBER READINESS  
INSTITUTE

# Change Behavior. Be Cyber Ready.

Visit us at

[BeCyberReady.com](https://BeCyberReady.com)

 @cyber-readiness-institute

 @Cyber\_Readiness

 @CyberReadinessInstitute



# Future Calls

Andre Ristaino, ISA

- 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?**

① 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](mailto:supplychain@natf.net)

[dearley@natf.net](mailto:dearley@natf.net)

[rstewart@natf.net](mailto:rstewart@natf.net)

[vagnew@natf.net](mailto:vagnew@natf.net)