North American Transmission FORUM

Community   Confidentiality   Candor   Commitment

Supplier Sharing
Virtual Workshop

November 7, 2023

Guidelines for this workshop/seminar

- This is an NATF open virtual workshop/seminar
  - Notice of the webinar was distributed beyond the NATF membership
  - Attendees include individuals not in the NATF membership
    - Do not share NATF confidential information
  - May include members of the press or media

- All attendees
  - Obey anti-trust laws and guidelines; avoid conduct that unreasonably restrains competition
  - Adhere to your organization's standards of conduct regarding sharing of any non-public transmission information
  - Respect and do not share intellectual property unless authorized

North American Transmission FORUM

Open Distribution for Supply Chain Materials

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

Open Distribution for Supply Chain Materials

Opening Remarks

Tom Galloway,
NATF President and CEO

Tom Galloway

NATF President and CEO

Purpose of the NATF Supplier Sharing Activities

- 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

Open Distribution for Supply Chain Materials

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)

Agenda and Today's Presenters

- Streamlining Supply Chain Risk Management with Customers

  Frank Harrill, VP, Security Schweitzer Engineering (SEL)

- Managing Software Bills of Materials and Inventories of Software Components

  Andre Ristaino, Managing Director, Global Consortia, Conformity Assessment, International Society of Automation (ISA)

  Dmitry Raidman, CTO, Cybeats

  Gonda Lamberink, VP of Sales, Cybeats

  Chris Blask, VP of Strategy, Cybeats

- Break (15 min)

- Leveraging Certifications

  Andy Turke, Siemens Industry, Inc.

  Andre Ristaino, Managing Director, Global Consortia, Conformity Assessment, International Society of Automation (ISA)

- Cloud Security

  Kristine Martz, Industry Specialist – Energy & Utilities, Amazon Web Services

North American Transmission FORUM

Open Distribution for Supply Chain Materials

Streamlining Supply Chain Risk Management with Customers

Frank Harrill
VP, Security Schweitzer Engineering (SEL)

Streamlining Supply Chain Risk Management with Customers

Frank Harrill
SEL Vice President of Security

November 7, 2023

CIP-013 requires an entity to create, implement, and periodically review an effective process to identify and assess cybersecurity risks to the Bulk Electric System from vendor products and services

External Surface Quick Looks

https://securityscorecard.com/security-rating/____.com

https://www.upguard.com/webscan

The NATF with cross-industry collaboration created and curates two supply chain risk assessment instruments:
- The Criteria
- The Questionnaire

natf.net/documents

Security and Supply Chain
NATF Supply Chain Risk Management Guidance
NATF Supply Chain Security Criteria
Energy Sector Supply Chain Risk Questionnaire
NATF CIP-013 Supply Chain Risk Management Plans (ERO Endorsed)
NATF CIP-013 Using Independent Assessments of Vendors (ERO Endorsed)
NATF Industry Collaboration - Using Solution Providers for Third-Party Risk Management
Cyber Security – Vendor Support via Web Conferencing - Implementation Guidance for CIP-005-6 Parts 2.4 and 2.5
NATF Implementation Guidance for CIP-010-3 Software Integrity
Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Supply Chain Security Criteria
Supply Chain Security Assessment Model
NATF Practices Document for CIP-014-2 R5
NATF Practices Document for CIP-014-2 R4

The NATF criteria is mapped to a variety of standards and frameworks

NATF guidance endorsed by NERC ERO Enterprise, validates the use of independent assessments of suppliers to satisfy CIP-013 requirements.
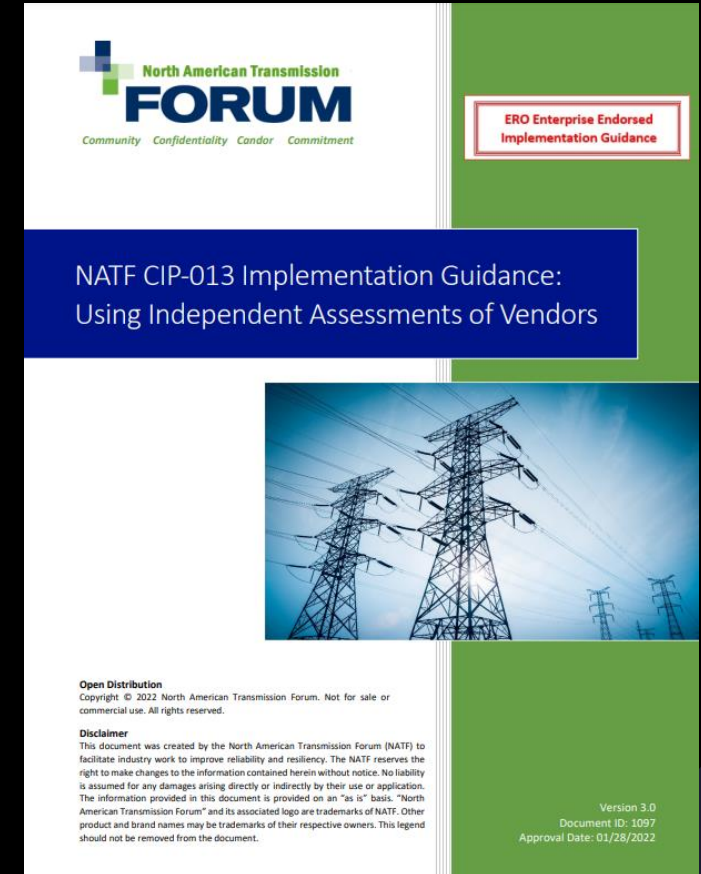
ISO/IEC 27001

IEC 62443-4-1

Acceptance of the NATF questionnaire <u>or</u> a independently audited certification to internationally recognized standards is becoming a common approach to supplier qualification

Questions?

Managing
Software Bills of Materials
and
Inventories of Software Components

Presenters

- Andre Ristaino, ISA Managing Director, Conformance Programs and Consortia, Conformity Assessment, International Society of Automation (ISA)

- Gonda Lamberink, VP of Sales, Cybeats

- Chris Blask, VP of Strategy, Cybeats

- Dmitry Raidman, CTO, Cybeats

Agenda

- Introduction

- ISA/IEC 62443 Inventory Requirements

- What is an SBOM vs. Inventory Overview and Status

- Who are the SBOM Creators and Users?

- Use Cases - Zero Trust and how to incorporate it

- What's Next?

ISA/IEC 62443-4-1 Inventory Requirements

The ISA/IEC 62443-4-1 standard includes a number of supplier requirements for maintaining an 'inventory' of items comprising the component/system. SBOM's are an approach for meeting the inventory requirements. Inventory requirements include:

- Software components

- Hardware components

- Compilers

- Configuration control

- Development and test applications (SUM-1, others)

- Third party and open-source components (SM-9, SM-10, others)

You can scan the ISASecure specification for all of the requirements by downloading it for free using the following link for the ISASecure SDLA-312 document:

· **ISASecure ISA/IEC 62443-4-1 assessment matrix**

CYBEATS
SBOM/VEX Analogy

You wouldn't give your allergic kid a snack with nuts to school! Why would you install vulnerable software in production?

- Allergies

- Food sensitivities

- People want to know what they eat

- Healthy living

Why do people not ask about the ingredients of their devices and software?

CYBEATS | Software Made Certain

CYBEATS
What is in an SBOM?

✔ Author

✔ Supplier Name

✔ Software Component Name

✔ Software Component Version

✔ Dependency Relationship

✔ Assembly Timestamp

✔ SBOM Generation Tool

✔ Component Unique IDs

```
{
  "bomFormat" : "CycloneDX",
  "specVersion" : "1.3",
  "serialNumber" : "urn:uuid:290804a5-75cd-49cd-afeb-366ffab26bac",
  "version" : 1,
  "metadata" : {
    "timestamp" : "2022-04-20T21:04:53Z",
    "tools" : [
      {
        "vendor" : "CycloneDX",
        "name" : "CycloneDX Maven plugin",
        "version" : "2.5.1",
        "hashes" : [
          {
            "alg" : "MD5",
            "content" : "1a5528adfeb75e1fef6264a90a0de94b"
          },
          {
            "alg" : "SHA-1",
            "content" : "bcbf4d76880f8b7b9008bd08fb72454e7f666957"
          },
          {
            "alg" : "SHA-256",
            "content" : "42fc254f37585624de9ed2dd9e1701d44e34cb5856433075afc851f4ae37857e"
          },
          {
            "alg" : "SHA-384",
            "content" : "6dc2adf4e002def6c49f1593f3d490c8ef5de6df77b390f0177ee84637fa9263e6948c0bb8daaef6f352a2f5f06714b6"
          },
          {
            "alg" : "SHA-512",
            "content" :
```

Action Item: Ask about components in your software! Through SBOM in SPDX or CycloneDX format.

You are as secure as the weakest link of your supply chain

Over **90%** of Commercial Applications Contain **Outdated** or **Abandoned** Open Source Software Components

Product you buying

This is your vendor's code

~25%

This is **NOT** his code

~75%

ALL MODERN DIGITAL INFRASTRUCTURE

Software Made Certain

CYBEATS
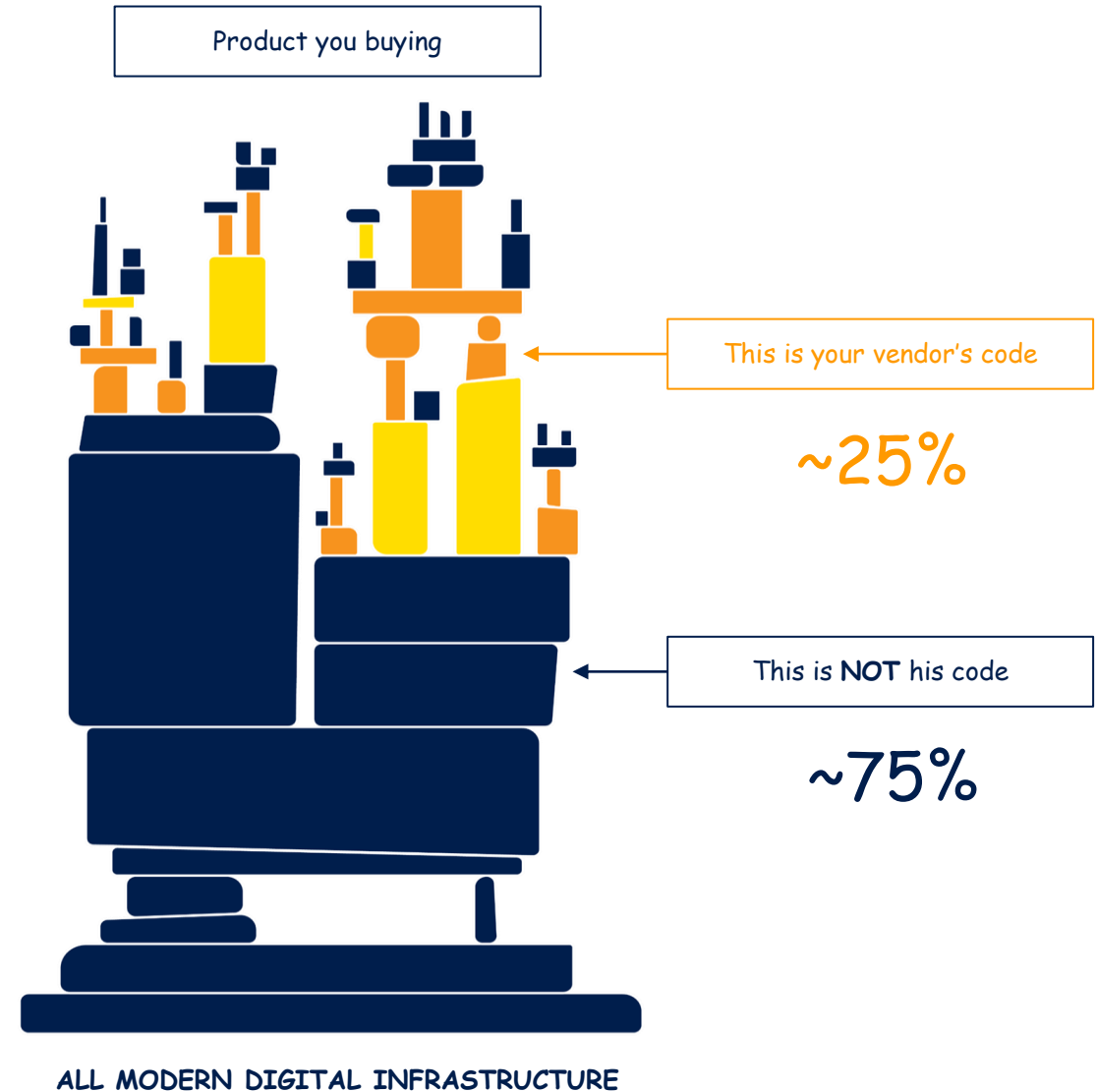
Upstream Open Source	Vendor	Integrator	Regulator	Service Provider	Industry Association
Private Sector Information Sharing	Public Sector Information Sharing	Data Value Addition Providers	Utility	Utility Customers	
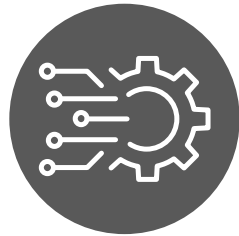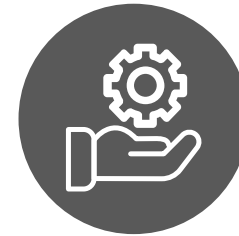
Open source Library Author	Firmware Author	Sub-Assembly Manufacturer	OEM	Integrator	Utility
SBOM Producer	SBOM Distributor	SBOM Distributor	SBOM Distributor	SBOM Distributor	SBOM Consumer
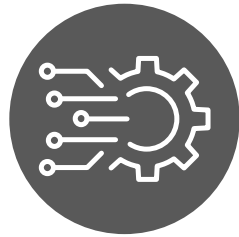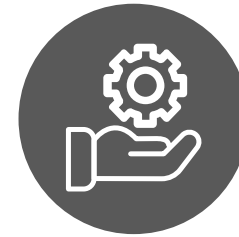
SBOM **Producer**: Actor who creates an SBOM and makes it available.
SBOM **Distributor**: Actor who makes an SBOM available they did not produce.
SBOM **Consumer**: Actor who makes use of an SBOM for a purpose other than making it available.

CYBEATS

NVD

Utility

If indicator of compromise, request mitigation from integrator if needed

Integrator

Procurement

Operations

See VEX/VDR from Integrator or Vulnerability Database

Search through Deployed SBOM (to Build SBOM and maybe to Source SBOM) to determine if impacted.
→ If source is not included in build, or not reachable via configurations, document and no further action required.
→ Else determine mitigation.

Get 'Product' update from Integrator with new Build SBOM, and confirm Safety Profile (when applicable) has been considered.

Create **New Deployed SBOM** to document new 'Product' installed and record new Deployed SBOM

Integrator

Deployed SBOM

New Build SBOM

Change monitoring to use **new** Build & Deployed SBOMs for monitoring

New Deployed SBOM

What are the SBOM Formats & High-Level Use Cases?

Business Unit 1	Business Unit 2	Business Unit 3	Supplier 1
SCA/BCA Tool 1	SCA/BCA Tool 2	SCA/BCA Tool 3	SCA/BCA Tool 4

CycloneDX SPDX

.json XML BIN

MANAGE SBOMS

SBOM Sharing

VEX - Vulnerability Exploitability eXchange

Accelerated Vulnerability Management

Compliance Management

Install Base Management

Reduced Cost of Protection

Open Distribution for Supply Chain Materials

- Do you track due dates for Known Exploited Vulnerabilities by CISA/EPSS?

- Do you understand your device firmware dependencies and their risk in depth?

- Are you aware of Outdated or Abandoned software?

- If there is a new critical vulnerability can you get answers in seconds not in weeks?

- Are you aware of software End of Life, End of Support events?

- Can you collect and observe all the data in one place?

- What would be the effort to perform it continuously?

Software Made Certain

- Aligning with globally recognized standard instead of a tool or method

- Cross referencing with the asset management data gaining in depth view

- Knowing about dependency vulnerabilities at the same time as the vendor?

- Optimization of MTTD and MTTR for cases like log4j, solarwinds

- Knowing what you have, software asset inventory and transparency

- Better understanding of transitive supply chain

- Vulnerability Assessment from Point In Time to Continuous

- Better Risk insights and faster communication

Software Made Certain

Thank you!

We meet you
where you are

CYBEATS

Open Distribution for Supply Chain Materials

BREAK

Return at 3:05

Leveraging Certifications

Andy Turke, Cyber Security Officer, Siemens Industry, Inc.
and
Andre Ristaino, Managing Director, Global Consortia, Conformity Assessment, International Society of Automation (ISA)

Open Distribution for Supply Chain Materials

Cybersecurity Certification
ISO 27001 and ISA/IEC 62443

ISA/IEC 62443 - Family of Standards
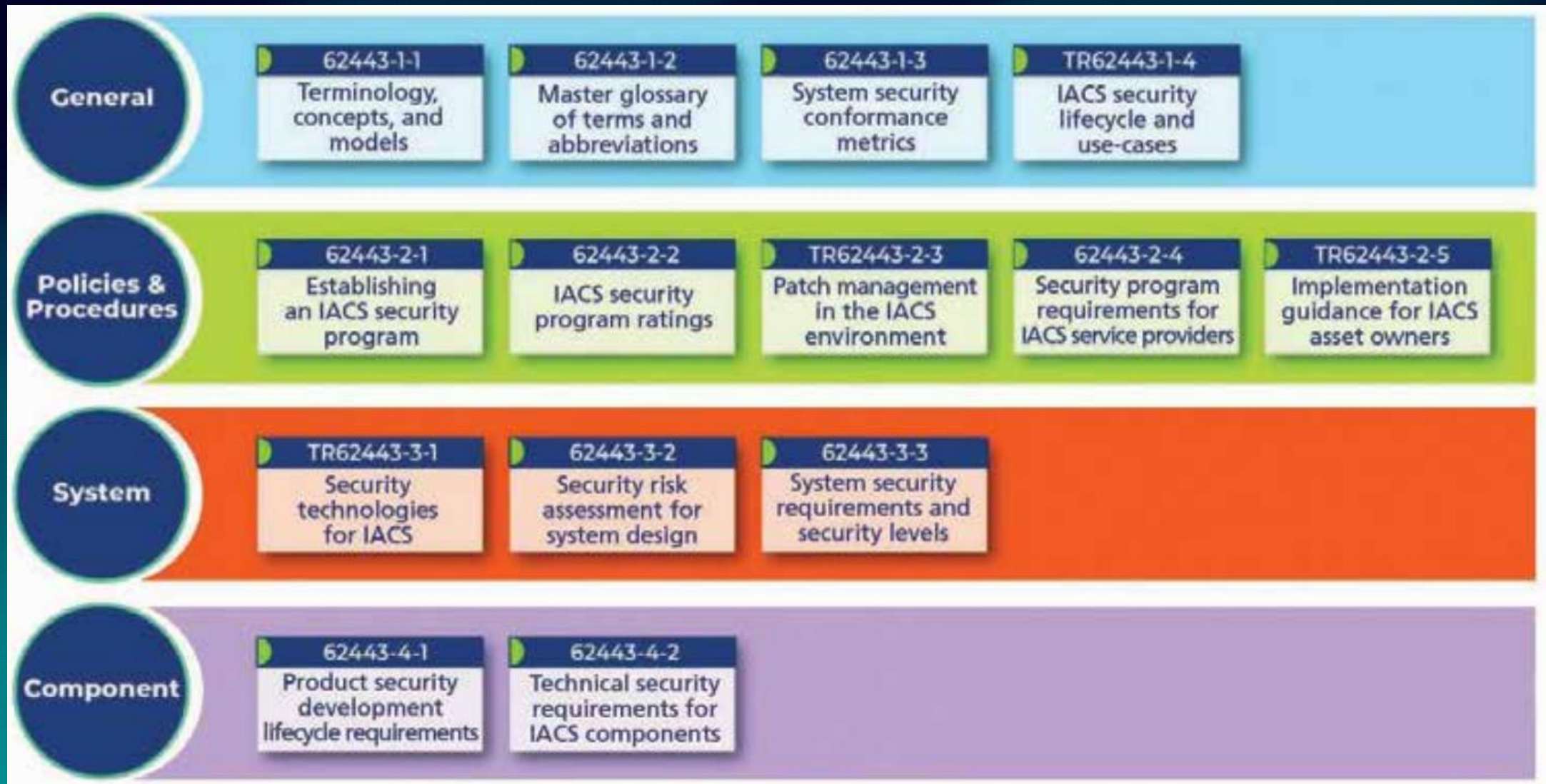
ISA/IEC 62443 4-1
Maturity Levels in Product Development Processes

Level	CMMI	62443	Description
1	Initial	Initial	• Product development typically ad-hoc and often undocumented • Consistency and repeatability may not be possible
2	Managed	Managed	• Product development managed using written policies • Personnel have expertise and are trained to follow procedures • Processes are defined but some may not be in practice
3	Defined	Defined (Practiced)	• All processes are repeatable across the organization • All processes are in practice with documented evidence
4	Quantitively Managed	Improving	• CMMI Levels 4 and 5 are combined • Process metrics are used control effectiveness and performance
5	Optimizing		• Continuous improvement

ISA/IEC 62443 4-2
Security Capability Levels in Automation Components and Systems

Legend:
- 🟩 No attack resistance
- 🟨 Low attack resistance
- 🟧 Medium attack resistance
- 🟥 High attack resistance

Security Level	Attack Type			
	Violation type	Means type	Resources level	Motivation
SL-1	Coincidental	N/A	N/A	N/A
SL-2	Intentional	Simple	Low	Low
SL-3	Intentional	Sophisticated	Moderate	Moderate
SL-4	Intentional	Sophisticated	Extended	High

IEC 62443 Security Standard – Roles based

ISA/IEC 62443 Automation Security Lifecycle and Shared Stakeholder Responsibility for Cybersecurity

Asset Owner – Leverage Standards:
- Part 1-1 – Concepts and models
- Part 2-1 – Security program requirements
- Part 2-2 – Security protection rating
- Part 2-3 – Patch management
- Part 3-2 – Risk assessment and system design

Asset Owners
Operate and Maintain Site Specific Systems

Maintenance Service Provider – Leverage Standards:
- Part 1-1 – Concepts and models
- Part 2-4 – Service providers

Integration Service Provider - Leverage Standards:
- Part 1-1 – Concepts and models
- Part 2-4 – Service providers
- Part 3-2 – Risk assessment and system design
- Part 3-3 – System requirements and security levels

Integrators/Asset Owners
Engineer and Integrate COTS into Site Specific Systems

Product Supplier - Leverage Standards:
- Part 1-1 – Concepts and models
- Part 3-3 – System requirements and security levels
- Part 4-1 – Security development lifecycle
- Part 4-2 – Component requirements

Product Suppliers
Design and Manufacture COTS Control Systems

IEC 62443 Security Standard
 → Addresses different roles, their processes and interactions
 → Covers full range of technical security measures
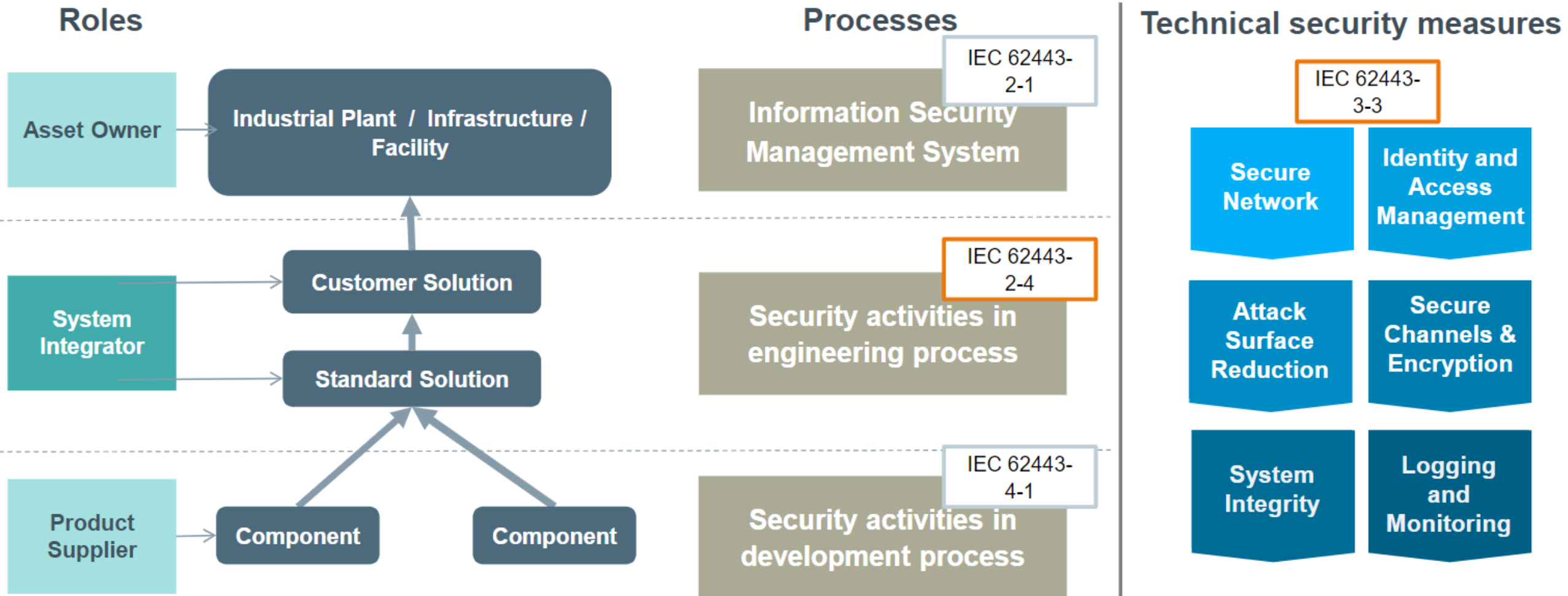
Benefits of Certification to an international standard

- Automation suppliers sell products globally in many countries. Suppliers seek a single security assessment and certificate of conformance to an international standard. This reduces barriers to trade and reduces supplier's cost with one certification mark that is globally recognized.

- Asset owners with international operations desire to use a single engineering specification and an internationally accepted standard for securing their operations.

- Certification provides transparency about a products security capabilities and assurances that it meets the requirements specified in the published security standards.

- Securing automation ultimately:
    - Reduces risk of endangerment of public or employee safety or health
    - Protects industrial automation and control systems from security breaches
    - Reduces risk of violation of legal or regulatory requirements
    - Advocates a holistic approach - not all risks are technology-based & maintains a security culture

- ISA 62443 Quick Start Guide: *https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf*

Asset Owners use of certifications in security programs
(using ISA/IEC 62443 COTS product certifications as an example)

- Have your OT security team study the certification specification to ensure it is applicable to your industry and use-case.

- Ensure that the certification scheme is consistent in applying all requirements from a standard to all products that are assessed (ensures 'apples to apples' comparison of products).

- Be sure to understand what security dimensions the certification covers and what it does not cover

- Add any policy language and/or other requirements not covered in the certification to your procurement document.

- Ensure that the certification specification team included asset owners so that your important requirements are properly represented in the certification specification.

- Ensure that the certification body is ISO 17065 accredited.

- Ensure that the certification has policies and procedures for maintaining the certification over time.

- Include the selected certification in your procurement requirements; for example *ISASecure CSA* SAL-2 or *ISASecure CSA* SAL-3

Standards and Regulation
Driving Cyber Security in products, solutions, environments

Following Key-Guidelines
Describing 'What' should be done

NERC

NIST Cyber Security Framework

Cyber Resiliency Act

Compliant with Key-Standards
Describing 'How' should it be done

ISO/IEC 62443 (System Security)

ISO/IEC 62351 (Communication Security)

ISO/IEC 27001/27019 (Security Management)

Conform to regulatory requirements
Describing what 'must' be done

Bundesministerium des Innern
IT Security Law

Bundesnetzagentur
Security Catalogue

Bundesamt für Sicherheit in der Informationstechnik

- Follow industry standard, i.e. bdew
- Report on incidents
- Implementation and Certification of an Information Security Management System (ISMS)
- Cryptographic requirements for Smart Metering

- Assessment and certification of ICS systems

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC
FEDERAL ENERGY REGULATORY COMMISSION

- Auditable compliance (NERC) is required for bulk power systems by regulation

Standards and Regulation
Overlapping with different focus areas

Focus: Power Systems
Focus: Industrial Automation
Focus: Information Systems

Design Details / Technical Aspects

NERC-CIP

IEC 62351

IEC 62443

Details for Operations

Relevance for Products

ISO/IEC 27001/2/19

Completeness / Governance & Policy Aspects
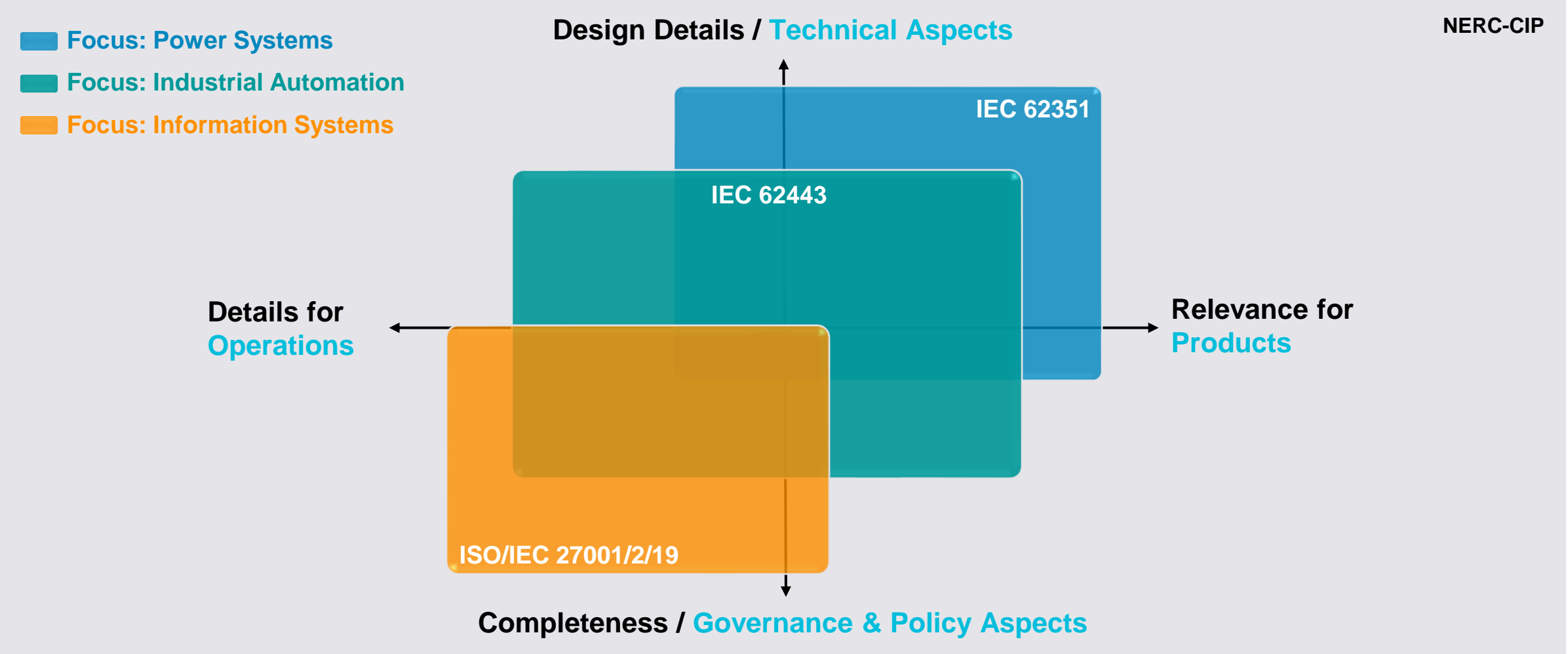
ISO 27001:2022 - Information Security Standard

- ISO/IEC 27001:2022 standard published Oct, 2022. This marks the beginning of the 3-year transition period.

- Last date for initial/re-certification audits according to former ISO 27001:2013 is 18 months after publication of ISO/IEC 27001:2022
(April 2024)

- Transition of existing certificates to ISO/IEC 27001:2022 is 3 years.
(October 2025)

ISO 27001 Annex A Overview

Annex A	Objective
A.5 Information security policies	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
A.6 Organization of information security	To establish a management framework to initiate and control the implementation and operation of information security within the organization.
A.7 Human resource security	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
A.8 Asset management	To identify organizational assets and define appropriate protection responsibilities.
A.9 Access control	To limit access to information and information processing facilities.
A.10 Cryptography	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
A.11 Physical and environmental security	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.
A.12 Operations security	To ensure correct and secure operations of information processing facilities.
A.13 Communications security	To ensure the protection of information in networks and its supporting information processing facilities.
A.14 System acquisition, development and maintenance	To ensure that information security is an integral part of information systems across the entire lifecycle.
A.15 Supplier relationships	To ensure protection of the organization's assets that is accessible by suppliers.
A.16 Information security incident management	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
A.17 Information security aspects of business continuity management	Information security continuity shall be embedded in the organization's business continuity management systems.
A.18 Compliance	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

ISO 27001:2022

The former 14 clauses of Annex A are now focused on the 4 following topics:

- A.5 Organizational controls (with 37 controls)

- A.6 Personal controls (with 8 controls)

- A.7 Physical controls (with 14 controls)

- A.8 Technical controls (with 34 controls)

ISO 27001:2022

Annex A of the new ISO/IEC 27001:2022 version includes 93 security controls. The following 11 controls are new:

- A.5.7 Threat Intelligence
- A.5.23 Information security for the use of cloud services
- A.5.30 ICT readiness for business continuity
- A.7.4 Physical security monitoring
- A.8.9 Configuration management
- A.8.10 Deletion of information
- A.8.11 Data masking
- A.8.12 Data leak prevention
- A.8.16 Activity monitoring
- A.8.23 Web filtering
- A.8.28 Secure coding

Cybersecurity Program Development Approach

Current State

Determine Security Posture/Maturity Level

Develop Security Program

Implement Security Program

Desired state

Maturity level unknown

Not documented

Perform assessment	NIST CSF
	ISO/IEC 62443
	NIST800-82

Identify gaps

Recommendations

Develop security strategy

Develop roadmap

Provide budget estimation

Program management of security strategy and project

Risk management

Security services planning

Initial

Developing

Defined

Managed	✅

Optimized

SIEMENS

Questions?

Cloud Security

Kristine Martz
Industry Specialist – Energy & Utilities
Amazon Web Services

aws FOR ENERGY

Cloud Security for Energy & Utilities

Kristine Martz (she/her)

Security Industry Specialist, Energy & Utilities

Security Assurance

Amazon Web Services

AWS CISO Security Predictions for 2023 and Beyond

1. Security Will Be Integral to Everything Organizations Do
2. Diversity Will Help Address the Continued Security Talent Gap
3. Automation Driven by AI/ML Will Enable Stronger Security
4. People Will Drive Greater Data Protection Investment
5. More Advanced Forms of Multi-Factor Authentication Will Become Pervasive
6. Quantum Computing Will Benefit Security

aws

CJ Moses' Security Predictions for 2023 and Beyond

November 2022

CJ Moses
Chief Information Security Officer, AWS
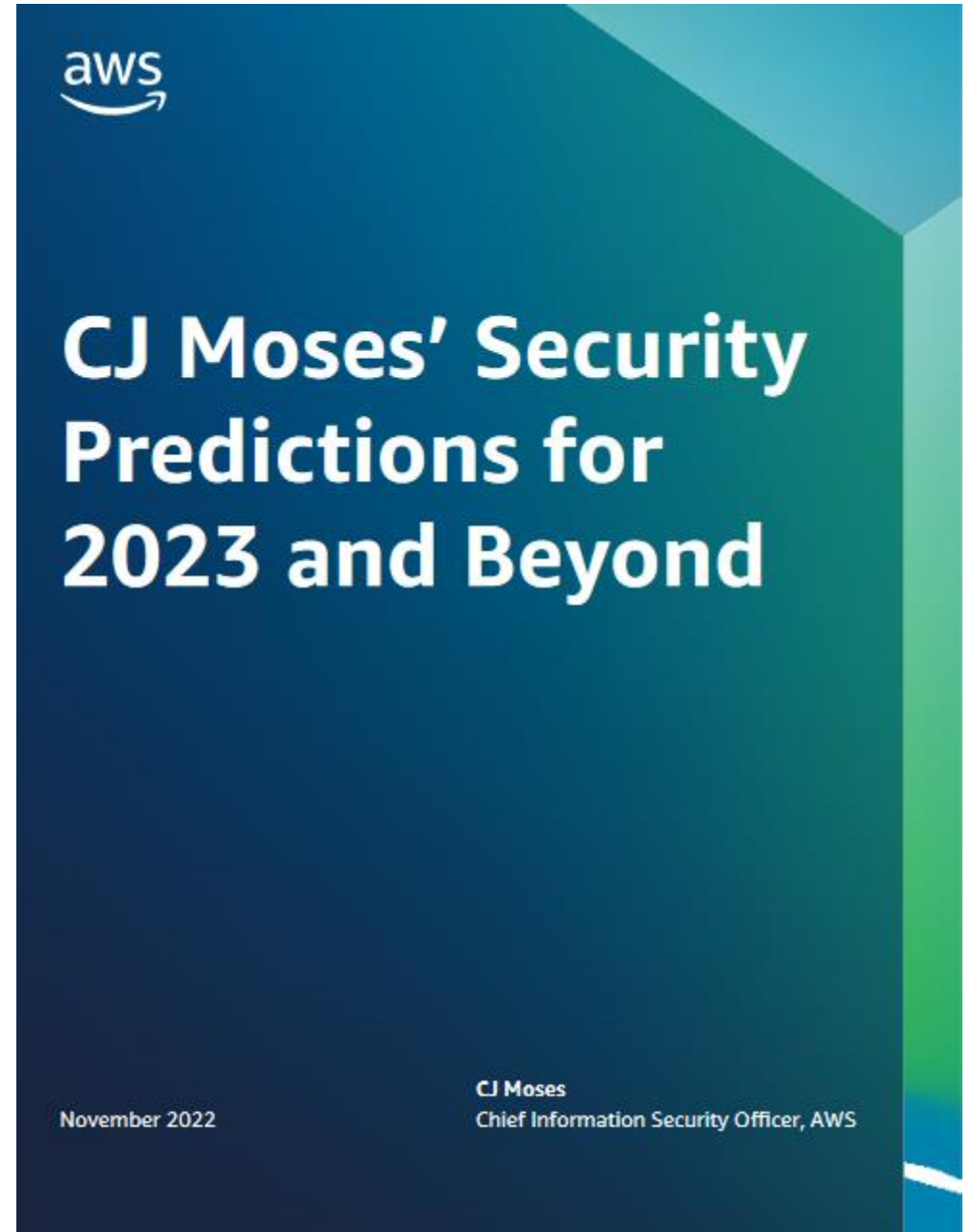
Energy & Utilities customers face unique risk and regulatory challenges

- In its shift to the cloud, the Energy & Utilities industry is
  - confronting a range of familiar and emerging issues

Constantly evolving regulatory requirements

Requirements that vary significantly across regions

Highly dynamic security threat landscape

Stringent reporting and documentation requirements

Limited cloud security & compliance specialists

Rise in Cybersecurity Policies and Regulations

Non-exhaustive list

Timeline of cybersecurity policies and regulations:

2005
- Japan Action Plan on Information Security Measures for CI¹ (2005)
- US Energy Policy Act (2005)

2006
- EU Program for CI¹ Protection (EPCIP) (2006)
- EU Security of Supply Directive (2006)

2007
- US NERC CI¹ Protection (CIP) Standards (2007)
- US Energy Independence and Security Act (2007)

2008
- EU Critical Infrastructure Directive (2008)

2010
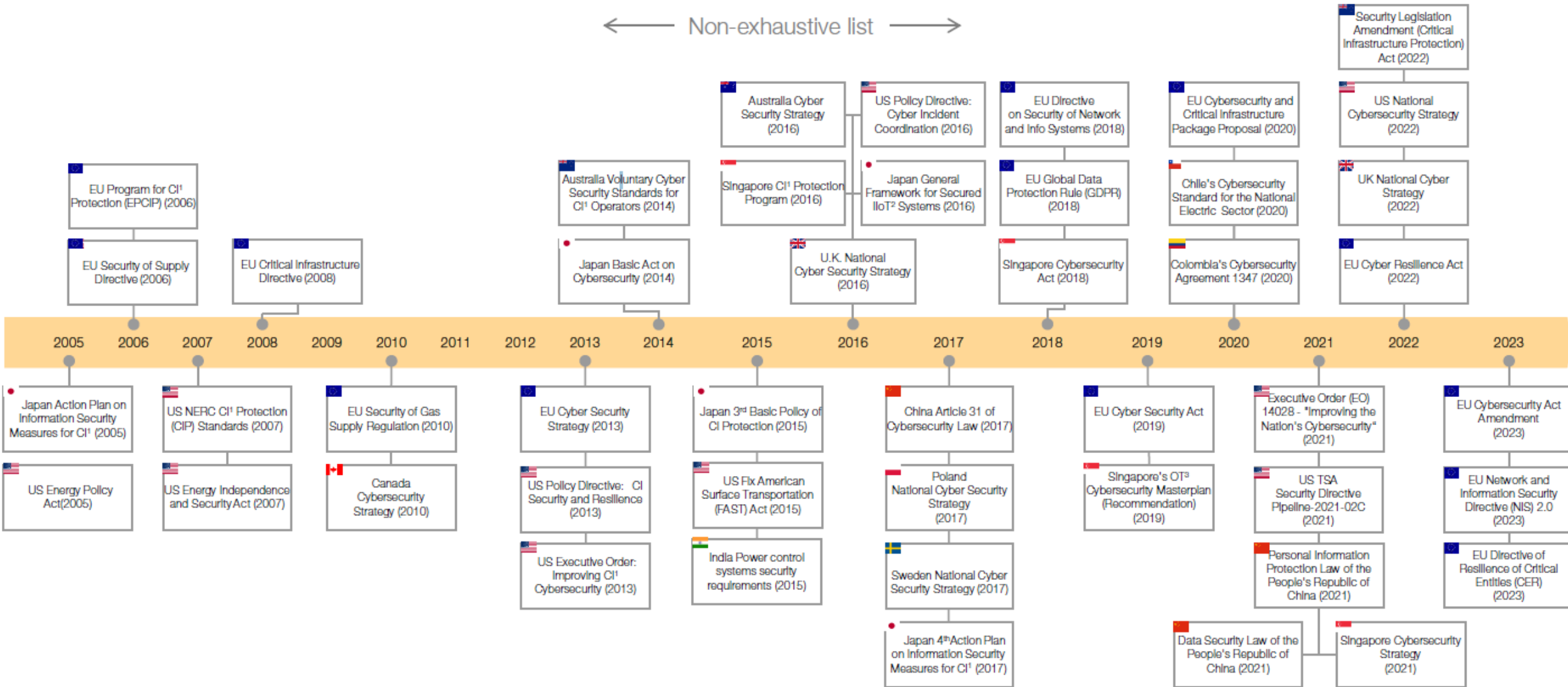- EU Security of Gas Supply Regulation (2010)
- Canada Cybersecurity Strategy (2010)

2013
- EU Cyber Security Strategy (2013)
- US Policy Directive: CI Security and Resilience (2013)
- US Executive Order: Improving CI¹ Cybersecurity (2013)

2014
- Australia Voluntary Cyber Security Standards for CI¹ Operators (2014)
- Japan Basic Act on Cybersecurity (2014)

2015
- Japan 3rd Basic Policy of CI Protection (2015)
- US Fix American Surface Transportation (FAST) Act (2015)
- India Power control systems security requirements (2015)

2016
- Australia Cyber Security Strategy (2016)
- Singapore CI¹ Protection Program (2016)
- US Policy Directive: Cyber Incident Coordination (2016)
- Japan General Framework for Secured IIoT² Systems (2016)
- U.K. National Cyber Security Strategy (2016)

2017
- China Article 31 of Cybersecurity Law (2017)
- Poland National Cyber Security Strategy (2017)
- Sweden National Cyber Security Strategy (2017)
- Japan 4th Action Plan on Information Security Measures for CI¹ (2017)

2018
- EU Directive on Security of Network and Info Systems (2018)
- EU Global Data Protection Rule (GDPR) (2018)
- Singapore Cybersecurity Act (2018)

2019
- EU Cyber Security Act (2019)
- Singapore's OT³ Cybersecurity Masterplan (Recommendation) (2019)

2020
- EU Cybersecurity and Critical Infrastructure Package Proposal (2020)
- Chile's Cybersecurity Standard for the National Electric Sector (2020)
- Colombia's Cybersecurity Agreement 1347 (2020)

2021
- Executive Order (EO) 14028 - "Improving the Nation's Cybersecurity" (2021)
- US TSA Security Directive Pipeline-2021-02C (2021)
- Personal Information Protection Law of the People's Republic of China (2021)
- Data Security Law of the People's Republic of China (2021)
- Singapore Cybersecurity Strategy (2021)

2022
- Security Legislation Amendment (Critical Infrastructure Protection) Act (2022)
- US National Cybersecurity Strategy (2022)
- UK National Cyber Strategy (2022)
- EU Cyber Resilience Act (2022)

2023
- EU Cybersecurity Act Amendment (2023)
- EU Network and Information Security Directive (NIS) 2.0 (2023)
- EU Directive of Resilience of Critical Entities (CER) (2023)

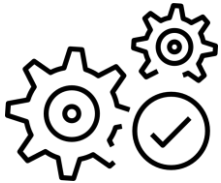**North American Transmission FORUM**

57

Customer Questions

- Where is my data when I put it in the cloud?

- Who owns my data in the cloud?

- What resilience does cloud provide?

- How are connected systems protected over the internet?

- How reliable are workloads in the cloud?

- How is my data secured in the cloud?

- What are the latency impacts of failing over to another Region?

- How much time does failover take for hot standby vs cold standby?

- What contingency plans are in place for multi-Region loss of power?

Tools and guidance to enable compliance

Compliance, Security Tools & Services

Industry Frameworks and Assets

Deep Industry Expertise

Regulatory Engagement

Terms & Conditions

Transparency

Services and assets to automate controls, collect evidence and manage audits demands

Mechanisms to advocate for and share best practices with customers
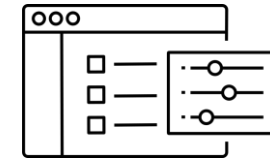
Agreements and third-party audit reports to support energy & utilities compliance objectives

We engage with global regulatory bodies on an ongoing basis

Ongoing engagement with regulators in the U.S. and around the world serves two purposes

To assess and explain policy

Regulatory policy evaluations to assess the potential impact of regulations

Country-by-country impact assessments to map how energy & utilities customers and partners need to operate

Region- and country-specific compliance guides to document key policy changes and responses
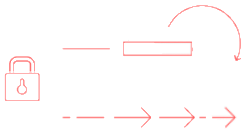
To share our approach and tools

Educate regulators to help examiners audit AWS environments

Help shape the regulatory landscape to reflect changes in technology

Facilitate dialogue between the industry and its regulators

AWS security, identity, and compliance solutions

Identity & access management	Detection	Infrastructure protection	Data protection	Incident response	
AWS Identity & Access Management (IAM)	AWS Security Hub	AWS Firewall Manager	Amazon Macie	Amazon Detective	AWS Artifact
AWS Single Sign-On	Amazon GuardDuty	AWS Network Firewall	AWS Key Management Service (KMS)	CloudEndure DR	AWS Audit Manager
AWS Organizations	Amazon Inspector	AWS Shield	AWS CloudHSM	AWS Config Rules	
AWS Directory Service	Amazon CloudWatch	AWS WAF – Web application firewall	AWS Certificate Manager	AWS Lambda	
Amazon Cognito	AWS Config	Amazon Virtual Private Cloud (VPC)	AWS Secrets Manager		
AWS Resource Access Manager	AWS CloudTrail	AWS PrivateLink	AWS VPN		
	VPC Flow Logs	AWS Systems Manager	Server-Side Encryption		
	AWS IoT Device Defender				

Inherit global security and compliance

Certifications / Attestations

C5	DE	✓
Cyber Essentials Plus	GB	✓
DoD SRG	US	✓
FedRAMP	US	✓
FIPS	US	✓
HITRUST	US	✓
IRAP	AU	✓
ISO 9001	🌐	✓
ISO 27001	🌐	✓
ISO 27017	🌐	✓
ISO 27018	🌐	✓
K-ISMS	KR	✓
MTCS	SG	✓
PCI DSS Level 1	🌐	✓
SEC Rule 17-a-4(f)	US	✓
SOC 1, SOC 2, SOC 3	🌐	✓

🌐 = industry or global standard

Laws / Regulations / Privacy

Argentina Data Privacy		✓
CISPE	EU	✓
EU Model Clauses	EU	✓
FERPA	US	✓
GDPR	EU	✓
GLBA	US	✓
HIPAA	US	✓
HITECH	🌐	✓
IRS 1075	US	✓
ITAR	US	✓
My Number Act	JP	✓
UK DPA - 1988	GB	✓
VPAT/Section 508	US	✓
Data Protection Directive	EU	✓
Privacy Act [Australia]	AU	✓
Privacy Act [New Zealand]	NZ	✓
PDPA—2010 [Malaysia]	MY	✓
PDPA—2012 [Singapore]	SG	✓
PIPEDA [Canada]	CA	✓
Spanish DPA Authorization	ES	✓
Spanish DPA Authorization	ES	✓

Alignments / Frameworks

CIS (Center for Internet Security)	🌐	✓
CJIS (US FBI)	US	✓
CSA (Cloud Security Alliance)	🌐	✓
ENS High	ES	✓
EU-US Privacy Shield	EU	✓
FFIEC	US	✓
FISC	JP	✓
FISMA	US	✓
G-Cloud	GB	✓
GxP (US FDA CFR 21 Part 11)	US	✓
ICREA	🌐	✓
IT Grundschutz	DE	✓
MITA 3.0 (US Medicaid)	US	✓
MPAA	US	✓
NIST	US	✓
PHR	US	✓
Uptime Institute Tiers	🌐	✓
Cloud Security Principles	GB	✓

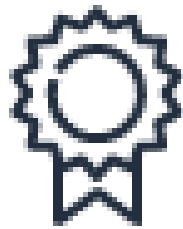North American Transmission FORUM

AWS Partners Lead with Innovation
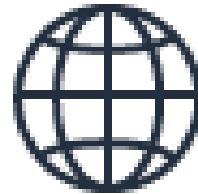
WE'RE IN THIS TOGETHER
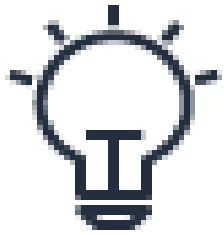
Innovation

- Innovative Vision
- Innovative Culture
- Structure and tools to innovate

Expertise

- Cloud Technology
- Cloud Governance
- Training as you Build

Global Reach

- Drawing on insights from other settings & experience
- Bringing together stakeholders

Informational Resources

Energy & Utilities Security Assurance Resources

The Utility Executive's Guide to Cloud Security

Utility Executive's Guide to AWS Security Control Domains

Power and Utility Path to Production in the AWS Cloud

How Dragos Uses AWS to Empower Collective Defense for Industrial Control Systems (ICS) and Operational Technology (OT)

How energy and utility companies can recover from ransomware and other disasters using infrastructure as code on AWS

Modernize your Utility's SOC and build better security with Splunk Cloud Platform on AWS

How to securely extend utility OT data to the cloud

Is FUD (Fear, Uncertainty & Doubt) Holding You Back From Adopting the Cloud?

Secure and resilient Distribution SCADA on AWS

Regulatory Developments in the Oil & Gas Pipeline Industry: Digital Transformation & OT Cybersecurity Best Practices

Securing Water Utilities with AWS

NERC CIP Thought Leadership Resources

AWS User Guide to Support Compliance with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards

Practical Adoption of Cloud Computing in Power Systems—Drivers, Challenges, Guidance, and Real-World Use Cases

Enabling Security and Resilience with Cloud Technology: AWS Cloud security and architecture for power and utilities

NERC CIP BES Cyber System Information (BCSI)

NERC CIP Standards for BES Cyber System Information on AWS

BES Cyber System Information (BCSI) on AWS
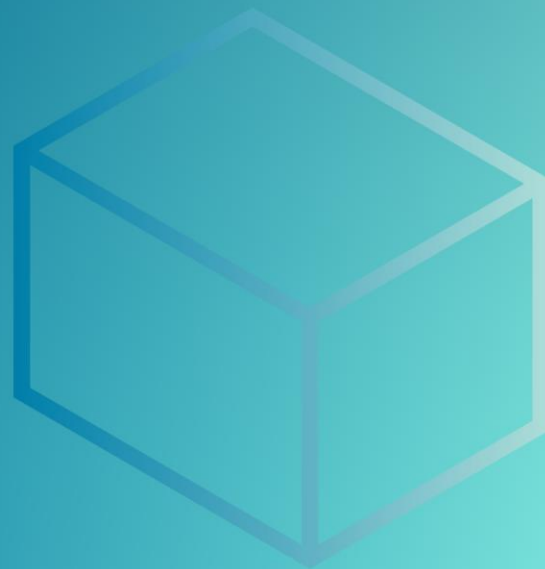
Operational Best Practices for NERC CIP BCSI

Operational Best Practices for NERC CIP BCSI example

aws FOR ENERGY

Thank you!

Kristine Martz

KriMartz@amazon.com

Closing Remarks

Frank Harrill
VP, Security Schweitzer Engineering (SEL)

Frank Harrill

VP, Security, SEL

Thank you for attending!

supplychain@natf.net
dearley@natf.net
vagnew@natf.net

Links from the webinar chat:

OSCAL FYI https://pages.nist.gov/OSCAL/

Reference for the machine-readable controls question https://pages.nist.gov/OSCAL/

https://www.nerc.com/comm/RSTC/Pages/SITES.aspx