NATF™
North American Transmission Forum

The NATF Criteria and Questionnaire Update: Mappings to Certifications

May 29, 2024

NATF Members Guidelines for this Call

- This is an open call
- Participants on this call are not employees of NATF member companies
    - Do not share confidential information
    - Avoid conduct that unreasonably restrains competition
    - Adhere to your organization’s standards of conduct
    - Do not share intellectual property unless authorized

Guidelines for this Call

- This call is being recorded
- The recording and slides for the call will be available on the NATF public website at: Supplier Sharing Calls (natf.net)

NATF does not endorse specific solution providers and provides the webinar content for entity awareness of available resources.

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

Agenda and Today's Presenters

Opening remarks –

Thomas Galloway, President and CEO, NATF

NATF Supply Chain Criteria and Questionnaire Updates

David James Earley, Program Manager Cybersecurity & Supply Chain, NATF

Obtaining Assurance with Certifications –

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

Tom Galloway

NATF President and CEO

Opening Remarks

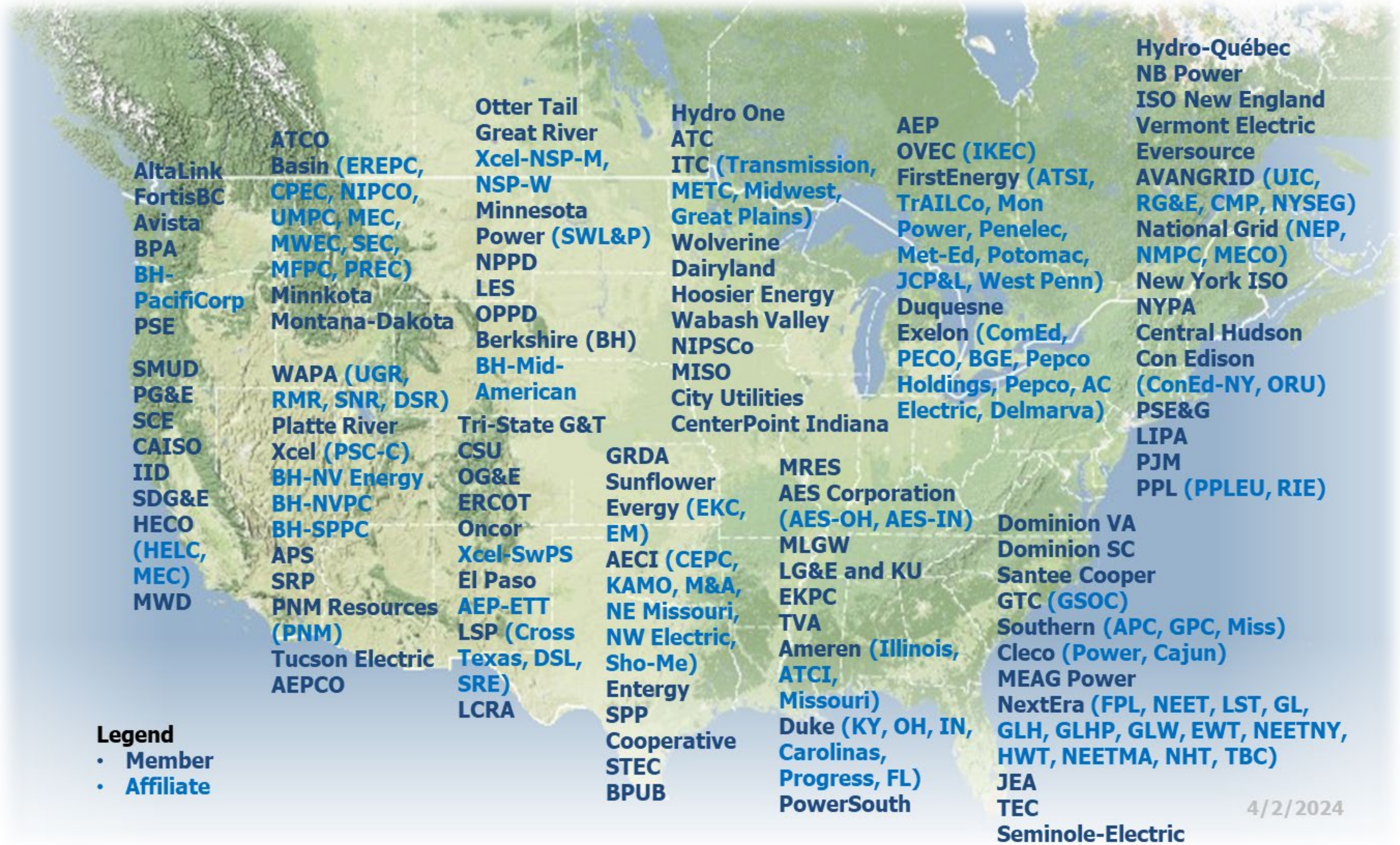
Tom Galloway,

NATF President and CEO

Background

- Membership Organization
- Formed after 2003 blackout
  - Prevent recurrence, pursue excellence
  - Robust information sharing
  - Superior practices (beyond compliance)
  - Confidential venues to increase candor
- Mission: Promote excellence in the safe, reliable, secure, and resilient operation of the electric transmission system.
- Headquarters – Charlotte, NC

NATF Members



AltaLink
FortisBC
Avista
BPA
BH-PacifiCorp
PSE

SMUD
PG&E
SCE
CAISO
IID
SDG&E
HECO (HELC, MEC)
MWD

ATCO
Basin (EREPC, CPEC, NIPCO, UMPC, MEC, MWEC, SEC, MFPC, PREC)
Minnkota
Montana-Dakota

WAPA (UGR, RMR, SNR, DSR)
Platte River
Xcel (PSC-C)
BH-NV Energy
BH-NVPC
BH-SPPC
APS
SRP
PNM Resources (PNM)
Tucson Electric
AEPCO

Otter Tail
Great River
Xcel-NSP-M, NSP-W
Minnesota Power (SWL&P)
NPPD
LES
OPPD
Berkshire (BH)
BH-Mid-American

Tri-State G&T
CSU
OG&E
ERCOT
Oncor
Xcel-SwPS
El Paso
AEP-ETT
LSP (Cross Texas, DSL, SRE)
LCRA

Hydro One
ATC
ITC (Transmission, METC, Midwest, Great Plains)
Wolverine
Dairyland
Hoosier Energy
Wabash Valley
NIPSCo
MISO
City Utilities
CenterPoint Indiana

GRDA
Sunflower
Evergy (EKC, EM)
AECI (CEPC, KAMO, M&A, NE Missouri, NW Electric, Sho-Me)
Entergy
SPP
Cooperative
STEC
BPUB

MRES
AES Corporation (AES-OH, AES-IN)
MLGW
LG&E and KU
EKPC
TVA
Ameren (Illinois, ATCI, Missouri)
Duke (KY, OH, IN, Carolinas, Progress, FL)
PowerSouth

AEP
OVEC (IKEC)
FirstEnergy (ATSI, TrAILCo, Mon Power, Penelec, Met-Ed, Potomac, JCP&L, West Penn)
Duquesne
Exelon (ComEd, PECO, BGE, Pepco Holdings, Pepco, AC Electric, Delmarva)

Hydro-Québec
NB Power
ISO New England
Vermont Electric
Eversource
AVANGRID (UIC, RG&E, CMP, NYSEG)
National Grid (NEP, NMPC, MECO)
New York ISO
NYPA
Central Hudson
Con Edison (ConEd-NY, ORU)
PSE&G
LIPA
PJM
PPL (PPLEU, RIE)

Dominion VA
Dominion SC
Santee Cooper
GTC (GSOC)
Southern (APC, GPC, Miss)
Cleco (Power, Cajun)
MEAG Power
NextEra (FPL, NEET, LST, GL, GLH, GLHP, GLW, EWT, NEETNY, HWT, NEETMA, NHT, TBC)
JEA
TEC
Seminole-Electric
LUMA

Legend
- Member
- Affiliate

4/2/2024

101 members
98 affiliates

Member Types
IOUs
Federal/Provincial
Cooperatives
State/Municipal
ISOs/RTOs

Coverage (US/Canada)
~85% miles 100 kV+
~90% net peak demand

NATF Supply Chain Activities

- NATF supply chain activities were initiated at the NERC BOT's request in August 2017
- NATF Board approved the NATF working industry-wide (beyond membership)
- NATF activities streamline supply chain risk management
  - Relying upon the work of others
  - Qualified, third-party certifications offer entities (asset owners) assurance of the accuracy of information provided by suppliers

Today’s Webinar

- Updates to the NATF criteria and questionnaire
  - Criteria provide key areas to measure a supplier’s security practices
  - Questionnaire provides additional questions for more in-depth coverage
- Leveraging certifications for assurance

NATF Supply Chain Criteria and Questionnaire Updates

David James Earley, NATF

Objectives of NATF Supply Chain Initiatives

Security

Identify and address security risks introduced via supply chain

Industry Convergence

Achieve industry and supplier convergence on an approach (NATF Model) to facilitate assessment of suppliers' security posture

Efficiency and Effectiveness

Convergence on manageable amount of information to achieve reasonable assurance of suppliers' security practices

Compliance

Implementation guidance to meet supply chain related CIP standards

NATF Supply Chain Security Assessment Model

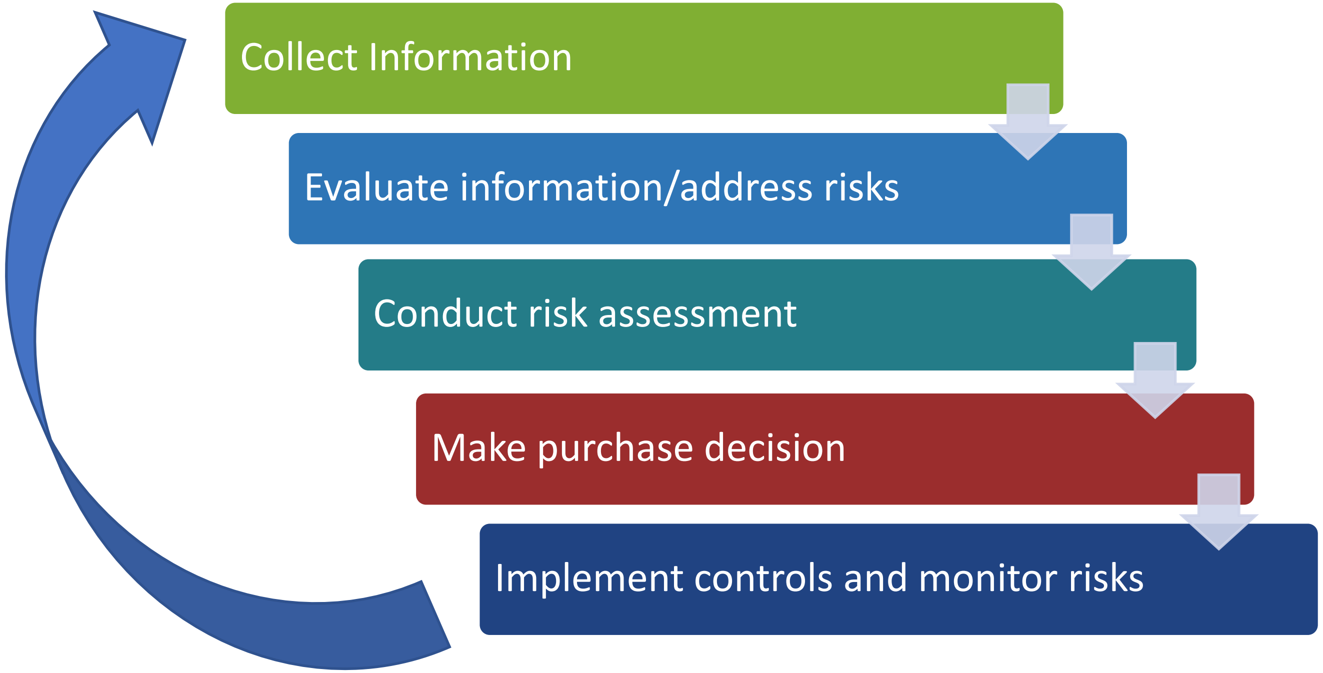
North American Transmission
FORUM
Community Confidentiality Candor Commitment

Supply Chain Security Assessment Model

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.

Version 2.0
Document ID: 1302
Approval Date: 06/04/2021



Collect Information
Evaluate information/address risks
Conduct risk assessment
Make purchase decision
Implement controls and monitor risks

Collect Information: The NATF Criteria and Questionnaire

- Were developed in collaboration with industry
- Identify a manageable set of key information needed from suppliers for SCRM
- Are endorsed by the regulator (NERC and the Regions)
- Offer an annual revision process to help drive convergence
- **Are mapped to security frameworks and certifications to support assurance**
- **Are offered at no charge for industry use**

NATF Supply Chain Security Criteria

64 criteria for supplier security practices within 6 risk areas

- Access control and management
- Asset, change and configuration management
- Governance
- Incident response
- Information protection
- Vulnerability management

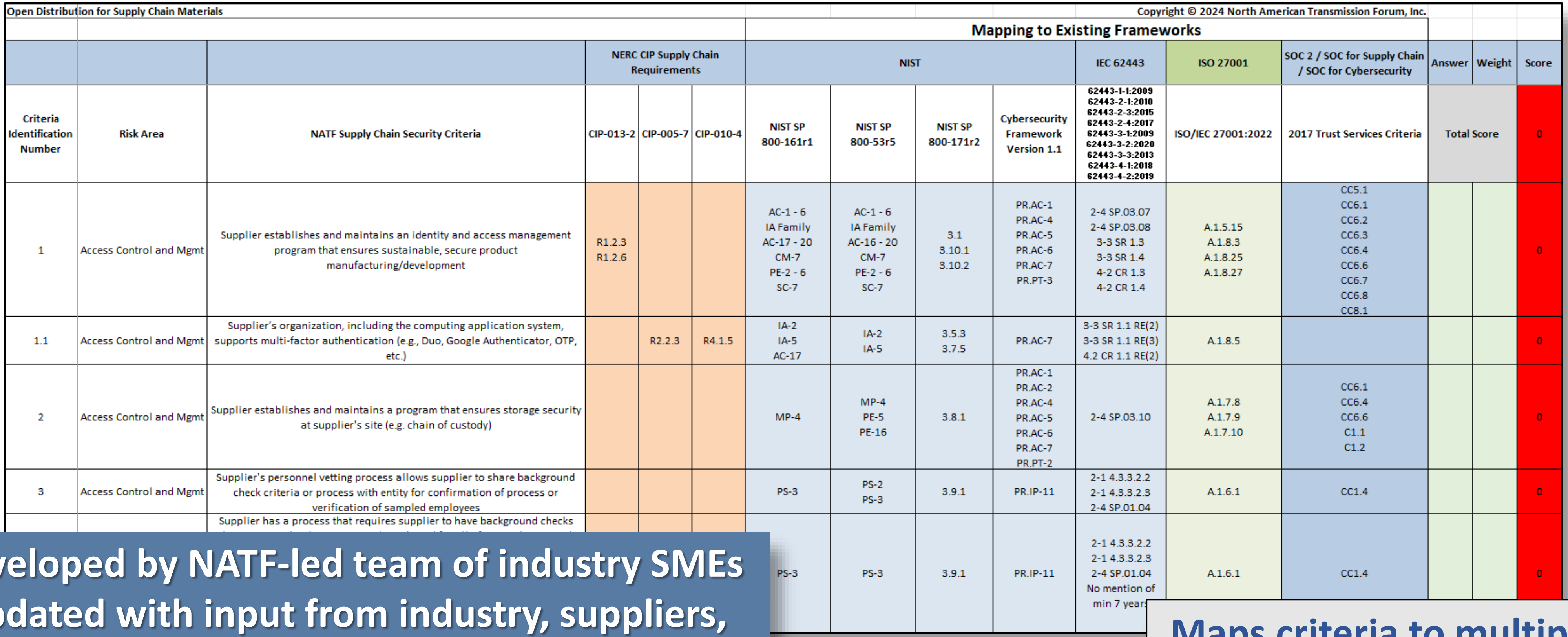
24 organizational information considerations

NATF Supply Chain Security Criteria

- Changes to Criteria for v5 (approved 5/21/2024):
  - Complete refresh of all framework mappings
  - Revised frameworks:
    - CIP-013-2, NIST 800r5, NIST 800-161r1, NIST 800-171r2, ISO 27001:2022
  - Addition of brand-new CIP-005-7 and CIP-010-4 mappings
    - Complete set of NERC CIP Supply Chain Standards now listed
  - New optional scoring mechanism
    - Identical to entity-driven approach used in Questionnaire

NATF Supply Chain Security Criteria

Provides a basis for measuring a supplier's security posture/practices (i.e., a "best practices" list)



Open Distribution for Supply Chain Materials

Mapping to Existing Frameworks

			NERC CIP Supply Chain Requirements			NIST				IEC 62443	ISO 27001	SOC 2 / SOC for Supply Chain / SOC for Cybersecurity	Answer	Weight	Score
Criteria Identification Number	Risk Area	NATF Supply Chain Security Criteria	CIP-013-2	CIP-005-7	CIP-010-4	NIST SP 800-161r1	NIST SP 800-53r5	NIST SP 800-171r2	Cybersecurity Framework Version 1.1	62443-1-1:2009 62443-2-1:2010 62443-2-3:2015 62443-2-4:2017 62443-3-1:2009 62443-3-2:2020 62443-3-3:2013 62443-4-1:2018 62443-4-2:2019	ISO/IEC 27001:2022	2017 Trust Services Criteria	Total Score		0
1	Access Control and Mgmt	Supplier establishes and maintains an identity and access management program that ensures sustainable, secure product manufacturing/development	R1.2.3 R1.2.6			AC-1 - 6 IA Family AC-17 - 20 CM-7 PE-2 - 6 SC-7	AC-1 - 6 IA Family AC-16 - 20 CM-7 PE-2 - 6 SC-7	3.1 3.10.1 3.10.2	PR.AC-1 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.PT-3	2-4 SP.03.07 2-4 SP.03.08 3-3 SR 1.3 3-3 SR 1.4 4-2 CR 1.3 4-2 CR 1.4	A.1.5.15 A.1.8.3 A.1.8.25 A.1.8.27	CC5.1 CC6.1 CC6.2 CC6.3 CC6.4 CC6.6 CC6.7 CC6.8 CC8.1			0
1.1	Access Control and Mgmt	Supplier's organization, including the computing application system, supports multi-factor authentication (e.g., Duo, Google Authenticator, OTP, etc.)		R2.2.3	R4.1.5	IA-2 IA-5 AC-17	IA-2 IA-5	3.5.3 3.7.5	PR.AC-7	3-3 SR 1.1 RE(2) 3-3 SR 1.1 RE(3) 4.2 CR 1.1 RE(2)	A.1.8.5				0
2	Access Control and Mgmt	Supplier establishes and maintains a program that ensures storage security at supplier's site (e.g. chain of custody)				MP-4	MP-4 PE-5 PE-16	3.8.1	PR.AC-1 PR.AC-2 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.PT-2	2-4 SP.03.10	A.1.7.8 A.1.7.9 A.1.7.10	CC6.1 CC6.4 CC6.6 C1.1 C1.2			0
3	Access Control and Mgmt	Supplier's personnel vetting process allows supplier to share background check criteria or process with entity for confirmation of process or verification of sampled employees				PS-3	PS-2 PS-3	3.9.1	PR.IP-11	2-1 4.3.3.2.2 2-1 4.3.3.2.3 2-4 SP.01.04	A.1.6.1	CC1.4			0
		Supplier has a process that requires supplier to have background checks				PS-3	PS-3	3.9.1	PR.IP-11	2-1 4.3.3.2.2 2-1 4.3.3.2.3 2-4 SP.01.04 No mention of min 7 year	A.1.6.1	CC1.4			0

Developed by NATF-led team of industry SMEs
Updated with input from industry, suppliers, third-party assessors, ERO, and FERC

Maps criteria to multiple security frameworks

Energy Sector Supply Chain Risk Questionnaire

219 questions in 13 categories

- Company Overview
- Supply Chain & External Dependencies Management
- Workforce Management
- Identity & Access Management
- Cybersecurity Program Management
- Change & Configuration Management
- Cybersecurity Tools & Architecture
- Data Protection
- Event & Incident Response
- Mobile Devices & Application
- Risk Management
- Vulnerability Management
- Additional Comments

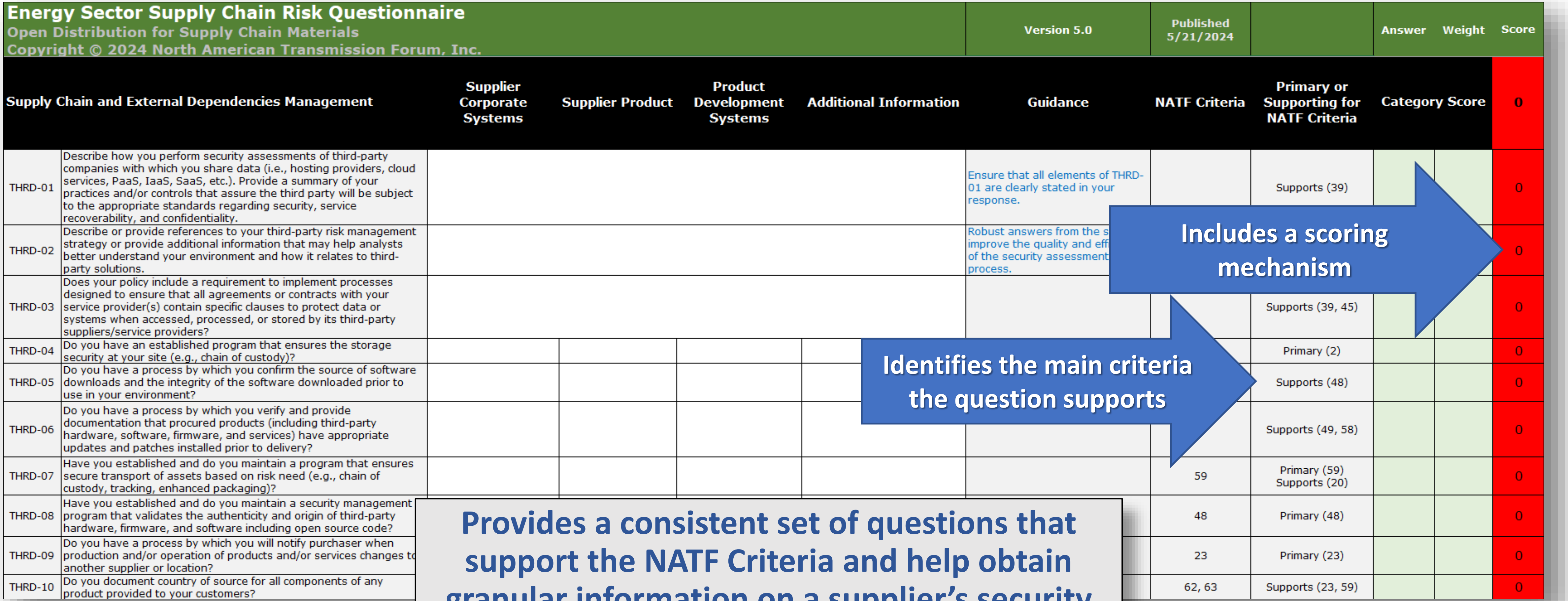
Questions for 3 areas

- Supplier Corporate Systems
- Supplier Product
- Product Development Systems

Energy Sector Supply Chain Risk Questionnaire

- Changes to Questionnaire for v5 (approved 5/21/2024):
  - Merged similar questions
    - COMP-04/COMP-08 and IAM-26/IAM-27
  - Added/reworded guidance text for additional clarity
  - All-new framework mappings
    - First-ever mapping of Questionnaire
    - Identical to frameworks used in Criteria for parity

Energy Sector Supply Chain Risk Questionnaire



Energy Sector Supply Chain Risk Questionnaire
Open Distribution for Supply Chain Materials

Version 5.0 | Published 5/21/2024 | Answer | Weight | Score

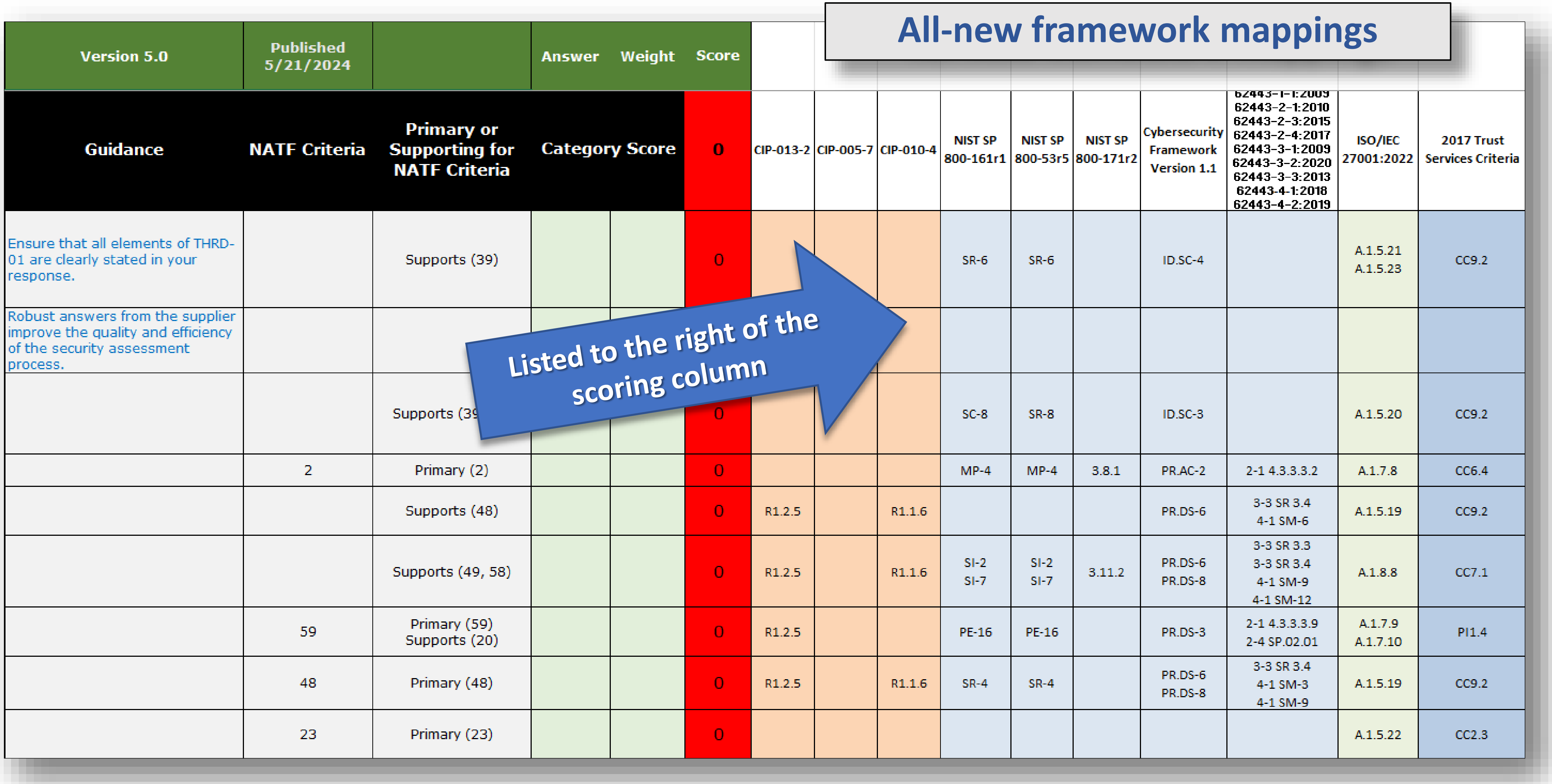
	Supply Chain and External Dependencies Management	Supplier Corporate Systems	Supplier Product	Product Development Systems	Additional Information	Guidance	NATF Criteria	Primary or Supporting for NATF Criteria	Category Score		0
THRD-01	Describe how you perform security assessments of third-party companies with which you share data (i.e., hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices and/or controls that assure the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.					Ensure that all elements of THRD-01 are clearly stated in your response.		Supports (39)			0
THRD-02	Describe or provide references to your third-party risk management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.					Robust answers from the s improve the quality and eff of the security assessment process.					0
THRD-03	Does your policy include a requirement to implement processes designed to ensure that all agreements or contracts with your service provider(s) contain specific clauses to protect data or systems when accessed, processed, or stored by its third-party suppliers/service providers?							Supports (39, 45)			0
THRD-04	Do you have an established program that ensures the storage security at your site (e.g., chain of custody)?							Primary (2)			0
THRD-05	Do you have a process by which you confirm the source of software downloads and the integrity of the software downloaded prior to use in your environment?							Supports (48)			0
THRD-06	Do you have a process by which you verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery?							Supports (49, 58)			0
THRD-07	Have you established and do you maintain a program that ensures secure transport of assets based on risk need (e.g., chain of custody, tracking, enhanced packaging)?						59	Primary (59) Supports (20)			0
THRD-08	Have you established and do you maintain a security management program that validates the authenticity and origin of third-party hardware, firmware, and software including open source code?						48	Primary (48)			0
THRD-09	Do you have a process by which you will notify purchaser when production and/or operation of products and/or services changes to another supplier or location?						23	Primary (23)			0
THRD-10	Do you document country of source for all components of any product provided to your customers?						62, 63	Supports (23, 59)			0

Includes a scoring mechanism

Identifies the main criteria the question supports

Provides a consistent set of questions that support the NATF Criteria and help obtain granular information on a supplier's security risk performance

Energy Sector Supply Chain Risk Questionnaire



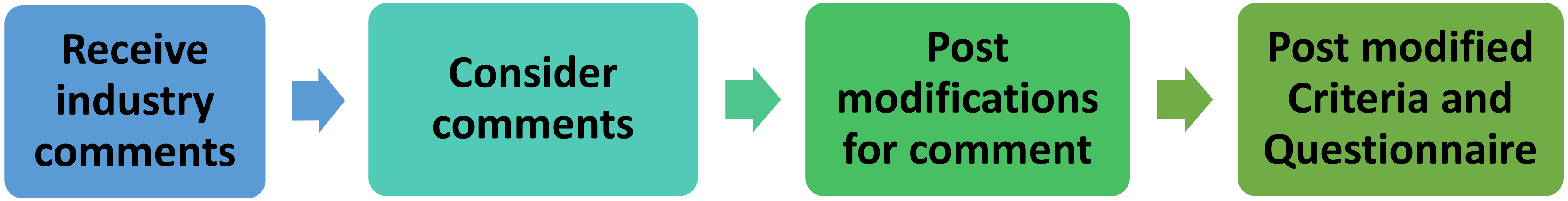
All-new framework mappings

Listed to the right of the scoring column

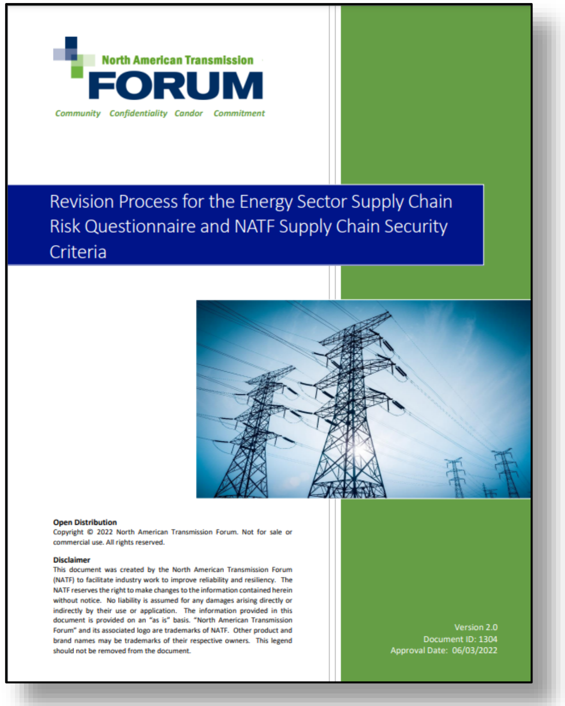
Version 5.0	Published 5/21/2024		Answer	Weight	Score										
Guidance	NATF Criteria	Primary or Supporting for NATF Criteria	Category Score		0	CIP-013-2	CIP-005-7	CIP-010-4	NIST SP 800-161r1	NIST SP 800-53r5	NIST SP 800-171r2	Cybersecurity Framework Version 1.1	62443-1-1:2009 62443-2-1:2010 62443-2-3:2015 62443-2-4:2017 62443-3-1:2009 62443-3-2:2020 62443-3-3:2013 62443-4-1:2018 62443-4-2:2019	ISO/IEC 27001:2022	2017 Trust Services Criteria
Ensure that all elements of THRD-01 are clearly stated in your response.		Supports (39)			0				SR-6	SR-6		ID.SC-4		A.1.5.21 A.1.5.23	CC9.2
Robust answers from the supplier improve the quality and efficiency of the security assessment process.															
		Supports (39			0				SC-8	SR-8		ID.SC-3		A.1.5.20	CC9.2
	2	Primary (2)			0				MP-4	MP-4	3.8.1	PR.AC-2	2-1 4.3.3.3.2	A.1.7.8	CC6.4
		Supports (48)			0	R1.2.5		R1.1.6				PR.DS-6	3-3 SR 3.4 4-1 SM-6	A.1.5.19	CC9.2
		Supports (49, 58)			0	R1.2.5		R1.1.6	SI-2 SI-7	SI-2 SI-7	3.11.2	PR.DS-6 PR.DS-8	3-3 SR 3.3 3-3 SR 3.4 4-1 SM-9 4-1 SM-12	A.1.8.8	CC7.1
	59	Primary (59) Supports (20)			0	R1.2.5			PE-16	PE-16		PR.DS-3	2-1 4.3.3.3.9 2-4 SP.02.01	A.1.7.9 A.1.7.10	PI1.4
	48	Primary (48)			0	R1.2.5		R1.1.6	SR-4	SR-4		PR.DS-6 PR.DS-8	3-3 SR 3.4 4-1 SM-3 4-1 SM-9	A.1.5.19	CC9.2
	23	Primary (23)			0									A.1.5.22	CC2.3

Revision Process for Criteria and Questionnaire

- Provides an annual cycle for industry to modify the Criteria and Questionnaire
  - Based on industry-wide input
  - Includes review to maintain ERO endorsement of the NATF CIP-013 Implementation Guidance documents



Receive industry comments → Consider comments → Post modifications for comment → Post modified Criteria and Questionnaire



North American Transmission FORUM

Community Confidentiality Candor Commitment

Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Supply Chain Security Criteria

Open Distribution

Copyright © 2022 North American Transmission Forum. Not for sale or commercial use. All rights reserved.

Disclaimer

This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve reliability and resiliency. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

Version 2.0
Document ID: 1304
Approval Date: 06/03/2022

Prior versions are also posted for tracking ease

ERO Endorsed Implementation Guidance: Supply Chain Risk Management Plans

- Describes how to use the NATF Supply Chain Security Assessment Model to develop supply chain cyber security risk management plans
  - Focus is on security
  - Incorporates by reference the NATF model, criteria, questionnaire, and associated revision process
  - Provides assurance of alignment between security and compliance
- Addresses the six risk areas identified in CIP-013, Requirement R1, Part 1.2

North American Transmission FORUM

Community Confidentiality Candor Commitment

ERO Enterprise Endorsed Implementation Guidance

NATF CIP-013 Implementation Guidance:
Supply Chain Risk Management Plans

Open Distribution

Copyright © 2022 North American Transmission Forum. Not for sale or commercial use. All rights reserved.

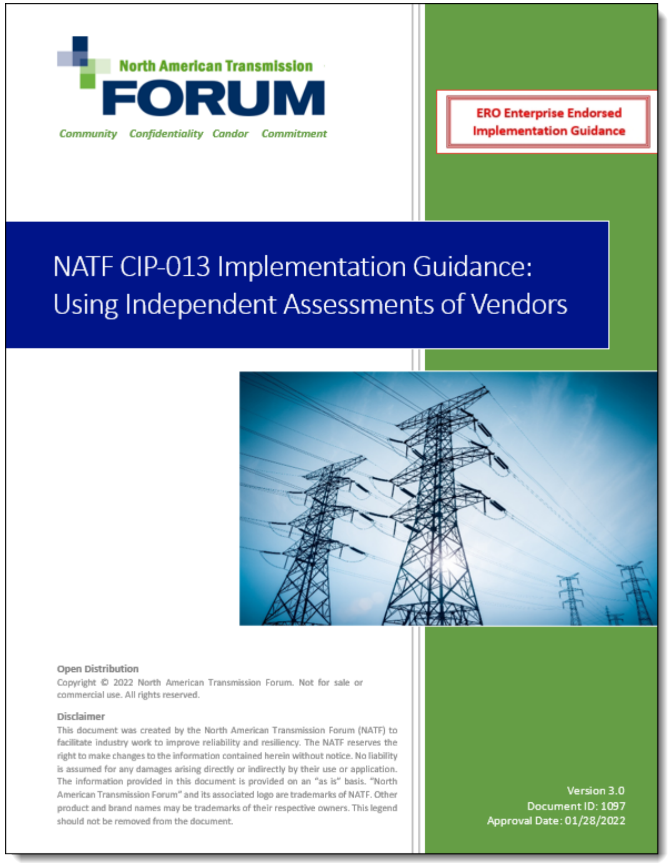
Disclaimer

This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve reliability and resiliency. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

Version 1.0
Document ID: 1605
Approval Date: 01/28/2022

ERO Endorsed Implementation Guidance: Using Independent Assessments of Vendors

- Describes how to leverage the work of others
  - CIP-013 R1: How to incorporate reliance on independent assessments into supply chain risk management plans
  - CIP-013 R2: How to document use of independent assessments when implementing supply chain risk management plan
- Incorporates by reference the NATF model, criteria, questionnaire, and associated revision process



North American Transmission FORUM

Community Confidentiality Candor Commitment

ERO Enterprise Endorsed Implementation Guidance

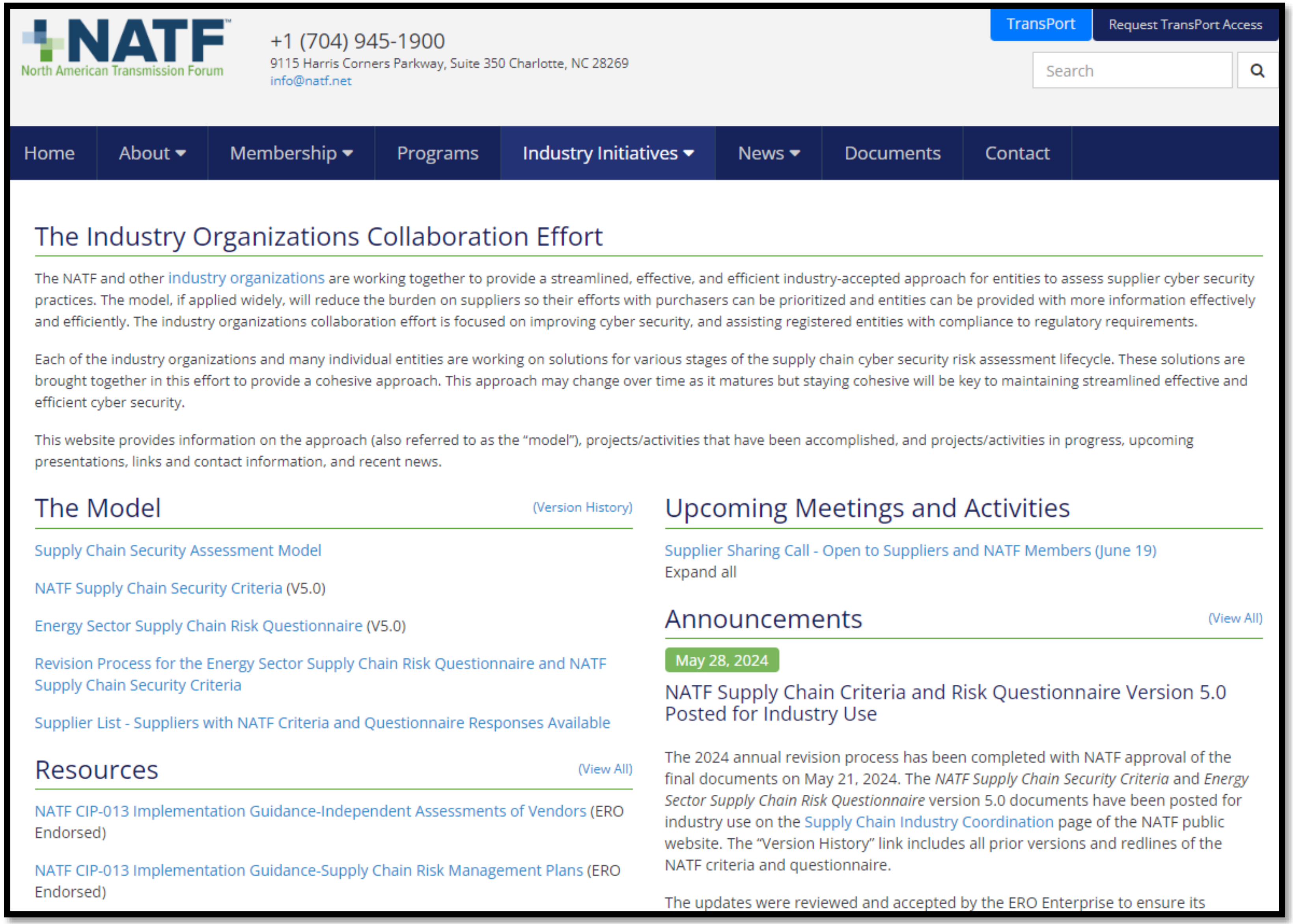
NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors

Open Distribution
Copyright © 2022 North American Transmission Forum. Not for sale or commercial use. All rights reserved.

Disclaimer
This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve reliability and resiliency. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

Version 3.0
Document ID: 1097
Approval Date: 01/28/2022

Where to find NATF supply chain resources



+1 (704) 945-1900
9115 Harris Corners Parkway, Suite 350 Charlotte, NC 28269
info@natf.net

The Industry Organizations Collaboration Effort

The NATF and other industry organizations are working together to provide a streamlined, effective, and efficient industry-accepted approach for entities to assess supplier cyber security practices. The model, if applied widely, will reduce the burden on suppliers so their efforts with purchasers can be prioritized and entities can be provided with more information effectively and efficiently. The industry organizations collaboration effort is focused on improving cyber security, and assisting registered entities with compliance to regulatory requirements.

Each of the industry organizations and many individual entities are working on solutions for various stages of the supply chain cyber security risk assessment lifecycle. These solutions are brought together in this effort to provide a cohesive approach. This approach may change over time as it matures but staying cohesive will be key to maintaining streamlined effective and efficient cyber security.

This website provides information on the approach (also referred to as the "model"), projects/activities that have been accomplished, and projects/activities in progress, upcoming presentations, links and contact information, and recent news.

The Model

(Version History)

Supply Chain Security Assessment Model

NATF Supply Chain Security Criteria (V5.0)

Energy Sector Supply Chain Risk Questionnaire (V5.0)

Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Supply Chain Security Criteria

Supplier List - Suppliers with NATF Criteria and Questionnaire Responses Available

Resources

(View All)

NATF CIP-013 Implementation Guidance-Independent Assessments of Vendors (ERO Endorsed)

NATF CIP-013 Implementation Guidance-Supply Chain Risk Management Plans (ERO Endorsed)

Upcoming Meetings and Activities

Supplier Sharing Call - Open to Suppliers and NATF Members (June 19)
Expand all

Announcements

(View All)

May 28, 2024

NATF Supply Chain Criteria and Risk Questionnaire Version 5.0 Posted for Industry Use

The 2024 annual revision process has been completed with NATF approval of the final documents on May 21, 2024. The *NATF Supply Chain Security Criteria* and *Energy Sector Supply Chain Risk Questionnaire* version 5.0 documents have been posted for industry use on the Supply Chain Industry Coordination page of the NATF public website. The "Version History" link includes all prior versions and redlines of the NATF criteria and questionnaire.

The updates were reviewed and accepted by the ERO Enterprise to ensure its

https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

Obtaining Assurance with Certifications

Andre Ristaino, ISA

International Society of Automation

ISASecure®

Automation and Control Systems Certifications For COTS Products, Service Providers and, Operating Sites

Based on ISA/IEC 62443

www.isasecure.org

29 May 2024

Elevating OT cybersecurity from an art, to a science, to an engineering discipline.

Andre Ristaino

ISA Managing Director, Conformance Programs and Consortia
aristaino@isa.org PH: +1 919-323-7660

- Mr. Ristaino directs ISA's consortiums and alliances, including, ISA Security Compliance Institute, ISA Wireless Compliance Institute, ISAGCA, ICS4ICS; 150 combined companies with over $1.25 trillion of turnover.

- Prior to ISA, Mr. Ristaino held positions at NEMA, Renaissance Worldwide and, Deloitte's Advanced Manufacturing Technology Group where he was a recognized leader in system lifecycle methodologies.

- Mr. Ristaino earned a BS in Business Management from the University of Maryland, College Park and an MS in Applied Computing from the American University in Washington DC with a focus on expert systems and artificial intelligence.

aristaino@isa.org

ISASecure®

ISA Automation Cybersecurity Leadership

ISASecure

ISASecure - ISA/IEC 62443 cybersecurity certification of COTS products, supplier development processes and automation at asset owner operating sites. Established 2007. **45+ companies** www.isasecure.org

ISA GLOBAL CYBERSECURITY ALLIANCE

ISAGCA - Bridge the gap between ISA/IEC 62443 standards and market adoption. Lead cybersecurity culture transformation. **60+ companies** https://isagca.org

ICS4ICS Incident Command System for Industrial Control Systems

ICS4ICS – Incident Command System for Industrial Control Systems (ICS4ICS) credentials incident leaders & trains teams for responding to cyber attacks on automation in critical infrastructure. Collaborates with FEMA and CISA; stood up under ISAGCA. **1,400 volunteers; over 850 companies** www.ics4ics.org

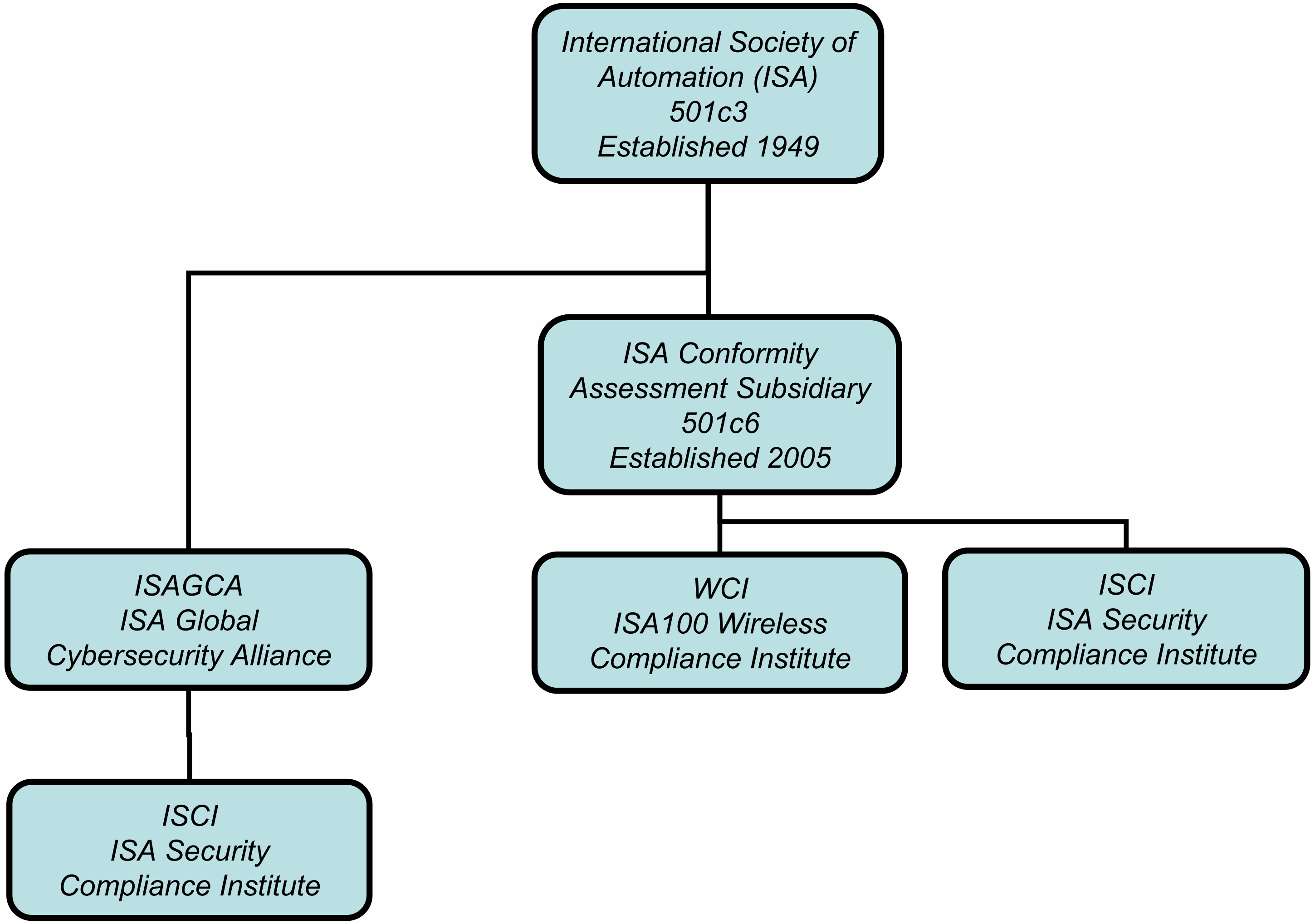
ISA99 Committee

ISA99 Committee – The ISA99 Standards committee is the origin of the ISA/IEC 62443 Standards. ISA99 Working groups draft and approve the ISA/IEC 62443 standards for submission to ANSI and IEC for approval as international standards. **Over 1,500 volunteers** www.isa.org/ISA99

ISA Education

ISA Education & Training – Education and training in all industrial automation and control systems topics, including cybersecurity. **Over 4,000 students in 2023**. https://www.isa.org/training

ISA Conformity Assessment Program



International Society of Automation (ISA)
501c3
Established 1949

ISA Conformity Assessment Subsidiary
501c6
Established 2005

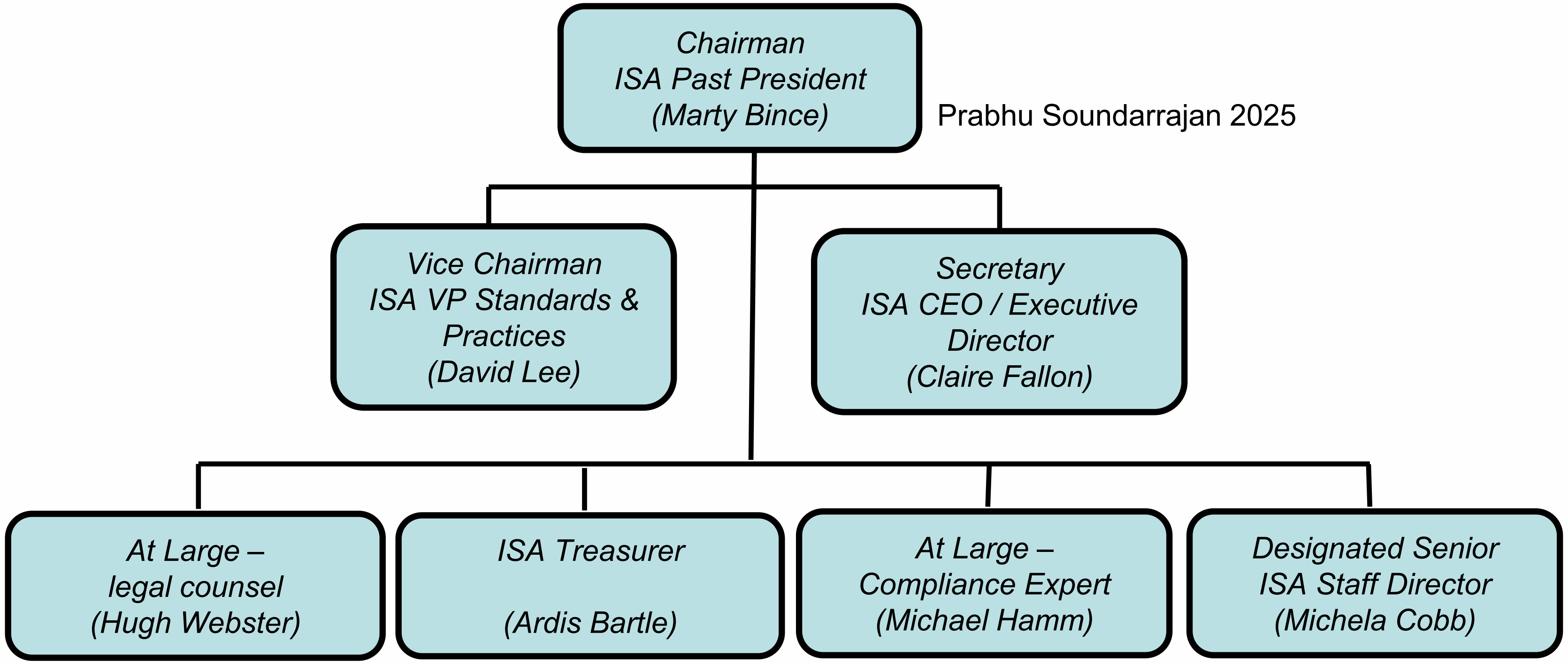
ISAGCA
ISA Global Cybersecurity Alliance

WCI
ISA100 Wireless Compliance Institute

ISCI
ISA Security Compliance Institute

ISCI
ISA Security Compliance Institute

2024 ISA Conformity Assessment Board



Chairman
ISA Past President
(Marty Bince)

Prabhu Soundarrajan 2025

Vice Chairman
ISA VP Standards & Practices
(David Lee)

Secretary
ISA CEO / Executive Director
(Claire Fallon)

At Large –
legal counsel
(Hugh Webster)

ISA Treasurer

(Ardis Bartle)

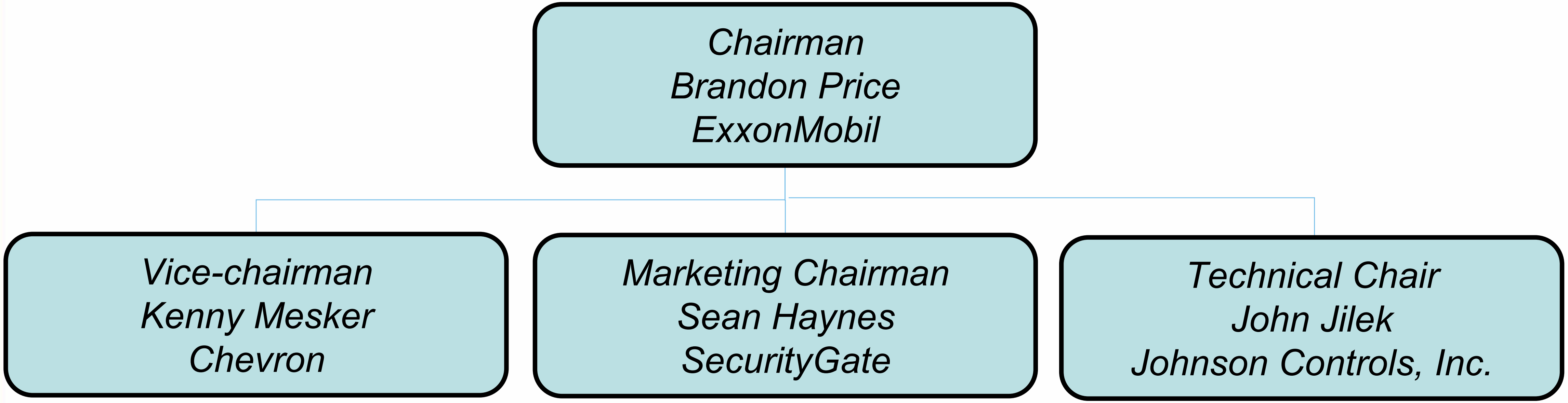
At Large –
Compliance Expert
(Michael Hamm)

Designated Senior
ISA Staff Director
(Michela Cobb)

All board positions are voting.

ISA ASCI Managing Director is non-voting. (Andre Ristaino)

ISA Security Compliance Institute Governing Board



Chairman
Brandon Price
ExxonMobil

Vice-chairman
Kenny Mesker
Chevron

Marketing Chairman
Sean Haynes
SecurityGate

Technical Chair
John Jilek
Johnson Controls, Inc.

Governing Board Companies

Chevron
Honeywell
Yokogawa

ExxonMobil
Johnson Controls, Inc.
Schneider Electric

Carrier Global
Saudi Aramco
Trane Technologies
GSK

ISA99 Committee Liaison

ISASecure Supporter Members

Chevron

ExxonMobil

أرامكو السعودية
Saudi Aramco

YPF

aws

FM Approvals®
Member of the FM Global Group

ARCADIS

GSK

SECURING THINGS
FOR SMART & SAFER SOCIETY

UL Solutions

ISA99
STANDARDS COMMITTEE

cyberprism.net

INTERSTATES

Schneider Electric

BYHON

cyberprism.net

SIEMENS
Ingenuity for life

HITACHI
Inspire the Next

Honeywell

ARMEXA

TAF Taiwan Accreditation Foundation

SecurityGate.io

Peloton
CYBER SECURITY

exida.com

KAIZEN CYBER LAB

YOKOGAWA

ISA

Secudea
Cybersecurity services for Industry

CSSC

SYNOPSYS®

SCC ccn 50 YRS ANS

ITRI
Industrial Technology Research Institute

WisePlant®

TÜVRheinland®
Precisely Right.

GE Digital

TRANE TECHNOLOGIES

KPMG

IACS CONSULTING

PROD JAB

TRUSTCB®

ZUONET

BEYOND security

Johnson Controls

BUREAU VERITAS 1828

DNV·GL

TÜV SÜD

Carrier

Singapore Accreditation Council

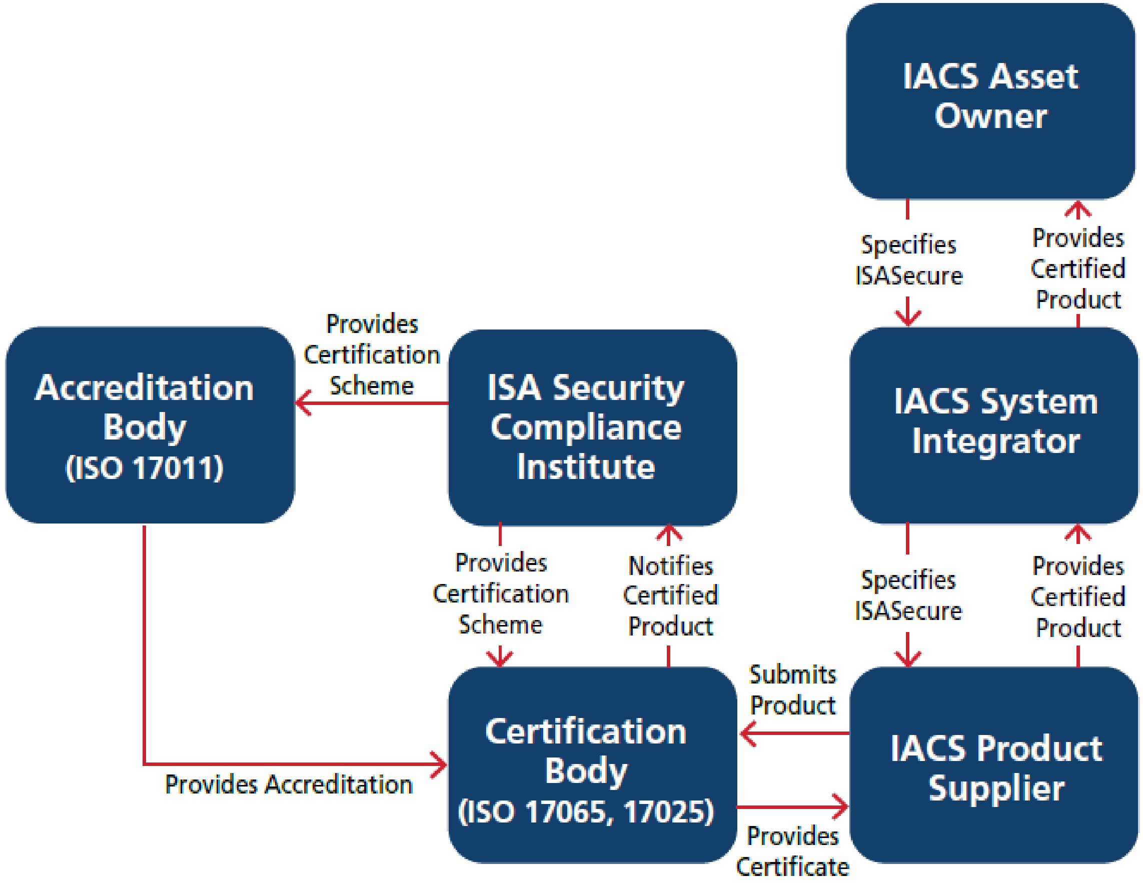
ANSI
ANSI Accredited Program
PRODUCT CERTIFICATION

ANAB
ACCREDITED
ISO/IEC 17021
MANAGEMENT SYSTEMS CERTIFICATION BODY

ilac-MRA

DAkkS
Deutsche Akkreditierungsstelle
D-PL-18345-01-00

ISO 17065 Conformance Scheme


IACS Asset Owner
Specifies ISASecure
Provides Certified Product
Accreditation Body (ISO 17011)
Provides Certification Scheme
ISA Security Compliance Institute
IACS System Integrator
Provides Certification Scheme
Notifies Certified Product
Specifies ISASecure
Provides Certified Product
Submits Product
Certification Body (ISO 17065, 17025)
IACS Product Supplier
Provides Accreditation
Provides Certificate

ISASecure® Accreditation Bodies and Certification Bodies

ISASecure ISO 17011 AB	Geographic Coverage
ANSI/ANAB	North America/Global
DAkkS	Germany/EU
Japan Accreditation Board	Japan
RvA Dutch Accreditation Council	Netherlands
Singapore Accreditation Council	Singapore
Standards Council of Canada	Canada
Taiwan Accreditation Foundation	Taiwan
A2LA	USA/Global
National Accreditation Board for Certification Bodies (NABCB)	India

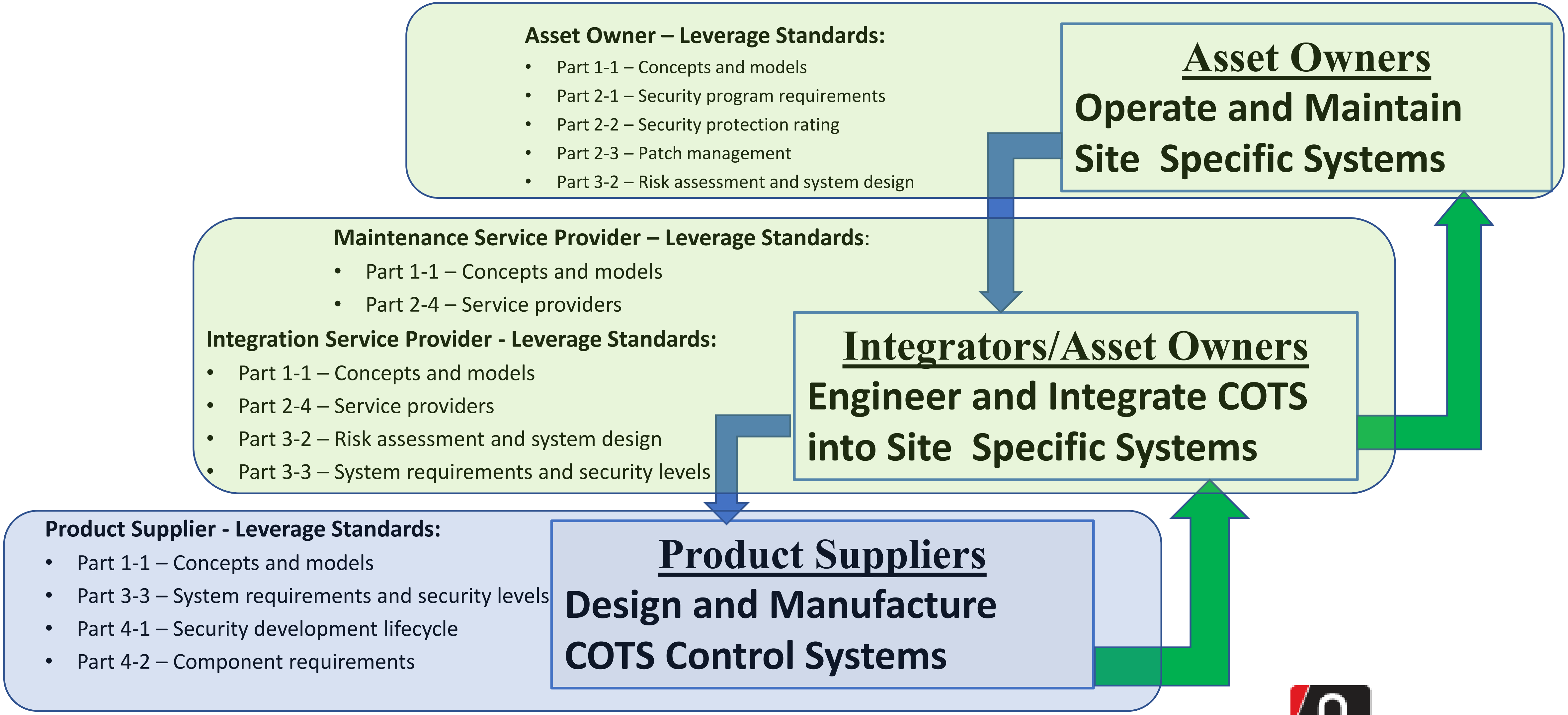
(Must be IAF Signatories for global MLA)

ISASecure CB ISO 17065/ISO 17025	Coverage
CSSC	Japan
Exida	USA / Global
TUV Rheinland	Germany / Global
FM Approvals	USA / Global
TUV SUD	Singapore / Global
BYHON	Italy / Global
Bureau Veritas	Taiwan / Global
Underwriters Labs (UL)	USA / Global
TrustCB	Netherlands / Global
DNV	India / Global
Ikerlan	Spain / Global
Kaizen Labs	India
AC&E	Italy/Global

ISASecure Global Product Certification Firsts

- 2010 - First global cybersecurity certification scheme for COTS automation and control systems (OT/CPS). Certifying off the shelf products since 2010.
- Meets ANAB FM 5116 “Suitability of Schemes” requirements, and IAF MD25 and EA-1/22 for EU suitability of schemes.
- 2010 - First OT COTS certification scheme requiring ISO 17065 accredited certification bodies, independently accredited by ISO 17011 Accreditation Bodies.
- 2011-First OT certification scheme to certify a safety system for nuclear sites (RTP Corp.).
- 2018–Only OT certification scheme to require ISA/IEC 62443-4-1 maturity level 3 to pass.
- 2022-First and only ISA/IEC 62443 OT certification scheme for IIoT devices and gateway.
- 2023-First and only OT certification scheme to implement market surveillance for product supplier incident response performance.
- 2023-Policies for certifying product families and for certifying OEM/relabeled products.

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

Currently Available Certifications

Future Availability

ISASecure®

ISASecure Certifications Currently Available

Certification Description	Certification Mark	Availability Date
IIOT Component Security Assurance (ICSA) ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2 plus 16 extensions	Certified IIOT Component ISASecure	Since Dec 2022
Component Security Assurance (CSA) ISA/IEC 62443 4-1 and ISA/IEC 62443 4-2	Certified Device ISASecure	Since Aug 2019
System Security Assurance (SSA) ISA/IEC 62443 3-3 and ISA/IEC 62443 4-2 ISA/IEC 62443-4-1	Certified System ISASecure	Since Oct 2018
Security Development Lifecycle Assurance (SDLA) ISA/IEC 62443 4-1	"An ISASecure Certified Development Organization"	Since July 2014

ISASecure Certification Expansion Roadmap

Certification Description	Certification Mark	Availability Date
IIOT System Security Assurance (ISSA) ISA/IEC 62443 4-1 and ISA/IEC 62443 3-3	Certified IIOT System ISA**Secure**	TBD
Automation and Control system Security Assurance (ACSSA) ISA/IEC 62443 2-1, 2-4, 3-2, 3-3	"ISASecure IEC 62443 Conformant Operating Site"	1H 2025

Phase I Study - IIOT Component Certification Based on the ISA/IEC 62443 Standards
https://gca.isa.org/iiot-component-certification-based-on-62443

Phase II Study - IIOT System Implementation and Certification Based on ISA/IEC 62443 Standards (includes cloud provider)- https://isasecure.org/learning-center

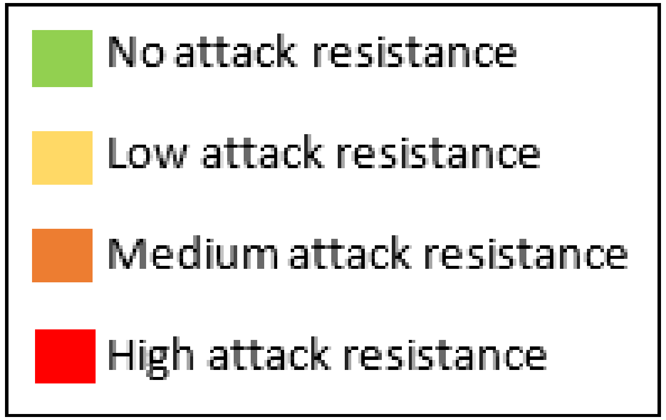
ISA**Secure**®

Development **Process** versus **Product** Certifications

Certification Type	**Recertification Criteria**	**Measure**
Organization's Development **Process** ISA/IEC 62443-4-1 Addresses the supplier's SDL, design, testing, incident response, patch/release, supply chain	**Time** Driven / Periodic Every 3 Years	**Process Maturity Level** ML-1,ML-2, ML-3, ML-4
Component and System **Products** ISA/IEC 62443 4-2 and ISA/IEC 62443-3-3 Addresses the specific product characteristics such as security capabilities/security level, free of known vulnerabilities, robust against network attacks	**Event** Driven Product **Upgrades** as defined int the 62443 standard (typically major version releases)	**Security Capability Level** SL-1, SL-2, SL-3, SL-4

ISASecure®

ISA/IEC 62443 Component and System Security Levels

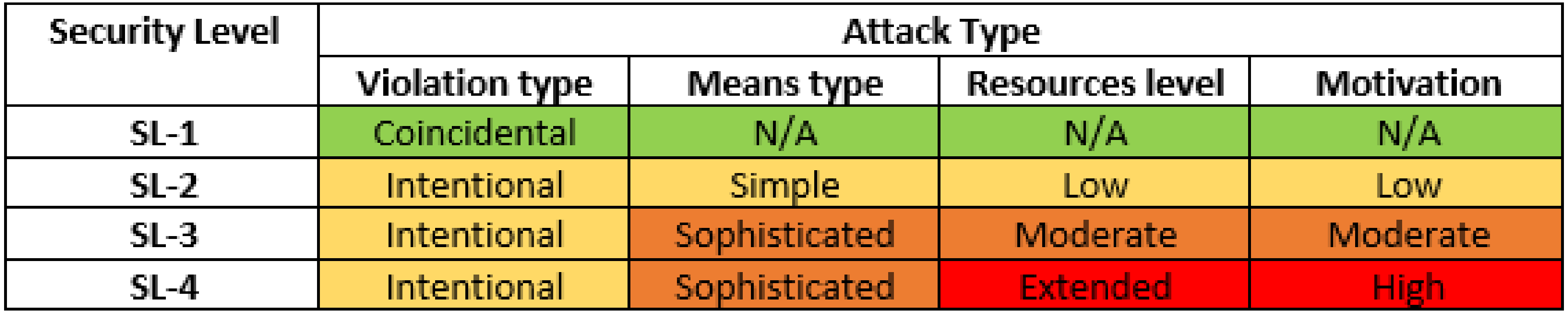


🟩 No attack resistance

🟨 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

- ISCI is now recommending that suppliers certify to level 2 or higher. ISCI SL-1 certifications still ensures that the supplier’s SDLA is at maturity level 3 or higher.
- OPAF (Open Process Automation Forum) standardized on level 2 or higher for their OPA Specification.

ISASecure®

ISA/IEC 62443-4-1 (development process)
Security Development Lifecycle Assurance (SDLA)

1) Define **scope** of evaluation (companywide, division, product line, geographic location, other)

2) Organization must have a formal, **defined SDL** (System Development Lifecycle) methodology

3) Products in the certified organization **must be under configuration control**

4) Product supplier's SDL must include all of the requirements in the **eight practice areas** defined in the ISA/IEC 62443 standard. (this is what the auditor evaluates)

5) **Recertification** is **time-driven** (process) every 36 months after initial certification.

6) ISASecure requires **maturity level 3** or better to pass. While the standard provides 'informative' definitions for 4 levels of process maturity, it is improper to publish them on a certificate. So, while we do not publish the maturity level on the certificate, all ISASecure certifications conform to the level 3 definition or better.

ISASecure®

Eight Practice Areas in ISA/IEC 62443-4-1 (SDLA)

One through Four

Practice 1 Security Management (SM) The purpose of the security management practice is to ensure that the security-related activities are adequately planned, documented and executed throughout the product’s lifecycle

Practice 2 Specification of Security Requirements (SR) The processes specified by this practice are used to document the security capabilities that are required for a product along with the expected product security context

Practice 3 Secure by Design (SD) The processes specified by this practice are used to ensure that the product is secure by design including defense in depth

Practice 4 Secure Implementation (SI) The processes specified by this practice are used to ensure that the product features are implemented securely

Eight Practice Areas in ISA/IEC 62443-4-1 (SDLA)

Five through Eight

Practice 5 Security Verification and Validation Testing (SVV) The processes specified by this practice are used to document the security testing required to ensure that all of the security requirements have been met for the product and that the security of the product is maintained when it is used in its product security context

Practice 6 Security Defect Management (DM) The processes specified by this practice are used for handling security-related issues of a product that has been configured to employ its defense in depth strategy (Practice 3) within the product security context (Practice 2)

Practice 7 Security Update Management (SUM) The processes specified by this practice are used to ensure security updates associated with the product are tested for regressions and made available to product users in a timely manner

Practice 8 Security Guidelines (SG) The processes specified by this practice are used to provide documentation that describes how to integrate, configure, and maintain the defense in depth strategy of the product in accordance with its product security context

ISASecure®

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 one approach** for meeting the inventory requirements for software. 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)

An ISASecure specification with these requirements can be downloaded for free using the following link:

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

ISA/IEC 62443-4-2 Component Security Assurance (CSA)

1) Product must be under configuration control and managed within the organization’s certified SDL methodology.

2) Product development artifacts are audited to confirm that the product is properly using the organization’s SDL certified to 62443-4-1. This includes audits of testing.

3) Products are VIT (vulnerability identification test) tested with Tenable Nessus Scanner to confirm no known vulnerabilities exist.

4) Product is evaluated to confirm that it conforms to all of the security capabilities defined in the 4-2 standard for the target security level (1-4)

5) **Recertification** is **event driven** by any product version release that is considered to be an ‘upgrade’ as defined by the 4-2 standard.

6) ISASecure recommends **security level 2** or better but will certify to any level requested by the supplier.

ISA/IEC 62443-4-2 **IIoT** Component Security Assurance (ICSA)

1) Same requirements and rules as the CSA certification with the following adaptations to account for IIoT characteristics.
   a) Four requirements from ISA/IEC 62443-4-2 are dropped and sixteen new requirements are added for things like secure boot, no zones and conduits, etc.

   b) Allows only two security capability levels beginning with SL-3+ and then SL-4. SL-1 and SL-2 are insufficient for IIOT devices and gateways.

2) **Recertification** is **event driven** by any product version release that is considered to be an ‘upgrade’ as defined by the 4-2 standard.

ISA/IEC 62443-3-3 System Security Assurance (SSA)

1) Product must be under configuration control and managed within the organization’s certified SDL methodology.

2) Product development artifacts are audited to confirm that the product is properly using the organization’s SDL certified to 62443-4-1. This includes audits of testing.

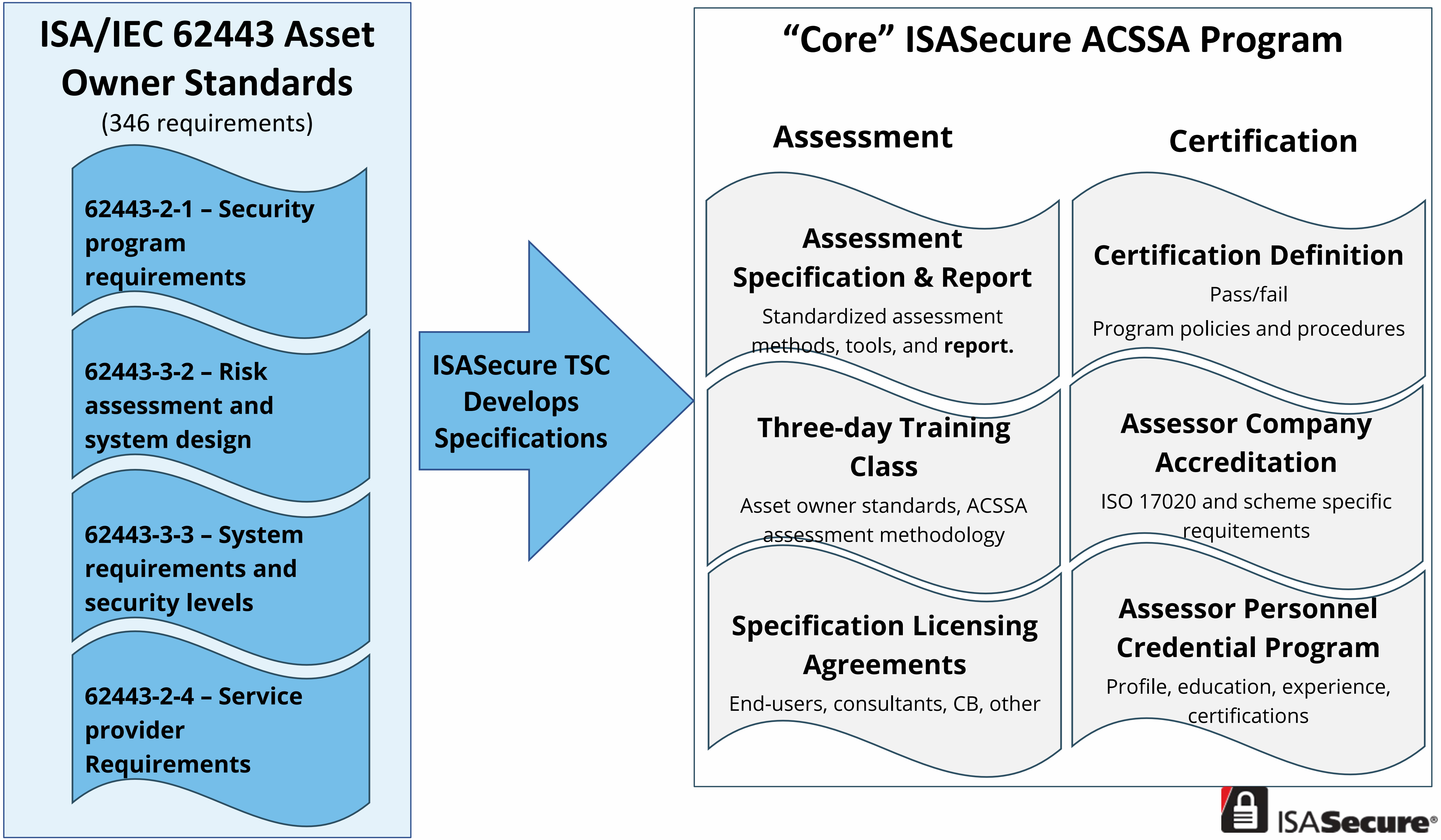
3) Products are VIT (vulnerability identification test) tested with Tenable Nessus Scanner to confirm no known vulnerabilities exist.

4) Product is evaluated to confirm that it conforms to all of the security capabilities defined in the 62443-3-3 standard for the target security level (1-4)

5) **Recertification** is **event driven** by any product version release that is considered to be an ‘upgrade’ as defined by the 62443-3-3 standard.

6) ISASecure recommends **security level 2** or better but will certify to any level requested by the supplier.

Asset Owner Operating Site Assessment/Certification



ISA/IEC 62443 Asset Owner Standards

(346 requirements)

62443-2-1 – Security program requirements

62443-3-2 – Risk assessment and system design

62443-3-3 – System requirements and security levels

62443-2-4 – Service provider Requirements

ISASecure TSC Develops Specifications

"Core" ISASecure ACSSA Program

Assessment

Assessment Specification & Report

Standardized assessment methods, tools, and **report.**

Three-day Training Class

Asset owner standards, ACSSA assessment methodology

Specification Licensing Agreements

End-users, consultants, CB, other

Certification

Certification Definition

Pass/fail

Program policies and procedures

Assessor Company Accreditation

ISO 17020 and scheme specific requitements

Assessor Personnel Credential Program

Profile, education, experience, certifications

Planned Milestone Dates for Phase One

- **Q3 2024 – ACSSA assessment specifications complete**
- **Q4 2024 – ACSSA program definition, policies/procedures, CB accreditation specifications**
- **Q4 2024 – Assessor Training class complete (3-day class)**
- **Q1 2025 – ACSSA available for asset owners, consultants, certification bodies**

Cybersecurity Resources at ISA

ISASecure product certifications – https://www.isasecure.org/en-US/

ISASecure ACSSA program details https://isasecure.org/isasecure-site-assessment-0

ISA Global Cybersecurity Alliance - https://isagca.org/

ISAGCA Blogs (tons of great info and free downloads) - https://gca.isa.org/blog

ISA/IEC 62443 Training - https://www.isa.org/training-and-certification/isa-training

OT cybersecurity incident command system for industrial control systems.
www.ics4ics.org

Andre Ristaino, ISA Managing Director, Consortia and Conformity Assessment
aristaino@isa.org O: +1 919-990-9222 M: +1 919-323-7660

Elevating OT cybersecurity from an art, to a science, to an engineering discipline

ISASecure®

Questions?

Key Takeaways

- Convergence for efficiency—the NATF continues to work towards bringing industry and suppliers together
- Leverage third-party assessments and certifications
- Endorsed by the ERO- https://www.nerc.com/pa/comp/guidance
- Available at no cost (it’s FREE)

Thank you for attending!

supplychain@natf.net

lunderwood@natf.net

dearley@natf.net

vagnew@natf.net

Questions?

Comments?

North American Transmission Forum

9115 Harris Corners Pkwy, Suite 350
Charlotte, NC 28269

(704) 945-1900
info@natf.net