North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Supplier Sharing Virtual Workshop

November 6, 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

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

Tom Galloway

NATF President and CEO

Opening Remarks

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

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

- Keynote Presentation

  Stephanie Johnson, Program Manager, Supply Chain Risk Management, Risk Management Tools & Technology, CESER, DOE

- National Strategy

  Frank Harrill, VP, Security, Schweitzer Engineering (SEL)
  Heath Knakmuhs, VP and Policy Counsel, US Chamber of Commerce

- Break (15 min)
- Considerations for International Suppliers

  Christopher Fitzhugh, Industrial Cybersecurity Consultant, North America, Siemens Energy
  Michael Pyle, Director of Product Cyber Security, Energy Management Business, Schneider Electric

- Getting Ahead of Regulation

  Panel Discussion

Stephanie Johnson

DOE CESER

Keynote Presentation

Stephanie Johnson
Program Manager,
Supply Chain Risk Management,
Risk Management Tools & Technology,
CESER, DOE

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

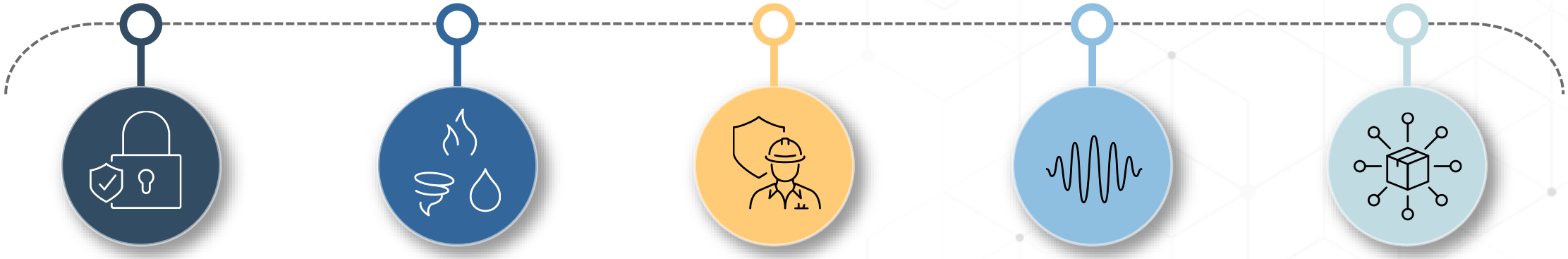
CESER Supply Chain Security Initiatives and Programs

September 6, 2023

CESER Mission

Strengthen the security and resilience of the U.S. energy sector from cyber, physical, and climate-based risks and disruptions.

Evolving Threats to Energy Infrastructure



What We Do

CESER advances the office's national security mission through:

Risk Assessment. Identifying, analyzing, and prioritizing risks to the energy sector.

Risk Mitigation. Developing policies, tools, and technologies and providing technical assistance to mitigate risks to the energy sector.

Sector Collaboration. Strengthening the security of U.S. energy systems through enhanced public and private sector collaboration.

Preparedness and Response. Facilitating energy sector preparedness, response, and restoration efforts in collaboration with other Federal agencies, the private sector, and state, local, tribal, and territorial communities and international partners.

Energy Supply. Mitigating the impacts of energy supply disruptions on American businesses and consumers.

CESER Divisions

Preparedness, Policy, and Risk Analysis

- Energy Security Policy and Partnerships
- Exercises, Training, Workforce Development
- Risk Analysis, Resilience, and Recovery

Risk Management Tools and Technologies

- All-Hazards Tools and Technologies
- Cyber Tools and Technologies

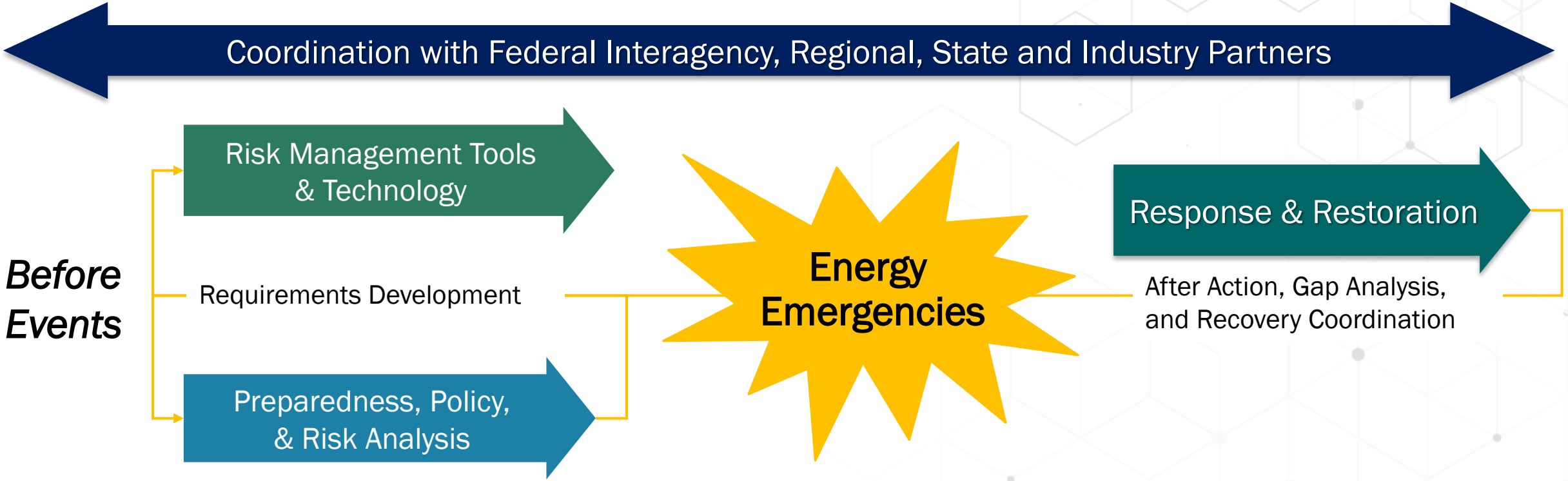
Response and Restoration

- All Hazards Situational Awareness and Analysis
- All Hazards Response Operations
- Response Preparedness and Support

Office of Petroleum Reserves

- Planning & Engineer Office
- Operations & Readiness
- Budget & Financial Management Technologies
- Management & Administration
- Reserve Lands Management
- SPR Project Management

How We Work: Energy Risk Management Timeline



DOE is the ***Sector Risk Management Agency*** for the energy sector and the federal coordinating agency for Emergency Support Function (ESF) #12 -- Energy

Energy Cyber Sense

Strategic Goal: Establish a national capability for enhancing the cybersecurity and cyber resilience of critical energy infrastructure, including the bulk power system, through conducting cyber vulnerability testing and forensic analysis, illuminating supply chain risks, applying classified threat intelligence, and engineering out cyber risk through improvements to digital component design, manufacturing, and procurement.

- Established pursuant to the requirements of Section 40122 of the *Bipartisan Infrastructure Law* (BIL), signed November 15, 2021.
- Expanded beyond requirements in statute to serve as the governing entity for CESER's entire portfolio of digital supply chain initiatives and programs in FY23.
- Voluntary program targeting strategic partnerships with members of the Energy Sector Industrial Base (ESIB)
    - The ESIB is defined as the "complex network of industries and stakeholders that spans from extractive industries, manufacturing industries, energy conversion and delivery industries, end of life and waste management industries, and service industries to include providers of digital goods and services."

Energy Cyber Sense

Four Pillars of Excellence:

Understand Criticality and Provenance

This pillar aims to improve the understanding of impacts from discovered vulnerabilities and illuminate supply chain dependencies within the Energy Sector Industrial Base (ESIB).

Test and Establish Supply Chain Transparency

This pillar aims to enable best-in-class testing, automation of testing, and other tools to scale benefits across the ESIB and illuminate digital supply chain risks for effective decision support in key use cases.

Aid in Application of Standards, Norms, and Best Practices

This pillar aims to promote excellence in security standards, norms, and best practices across the ESIB. This effort goes beyond supporting domestic and international standards setting bodies (e.g., NIST and IEEE) to promote a unity of effort in cybersecurity best practices, lessons learned, and other norms for ICS/OT systems in energy and other critical infrastructure sectors. This pillar includes standardization of reporting and vulnerability disclosure processes.

Improve Technology and System Designs (Both Legacy & New)

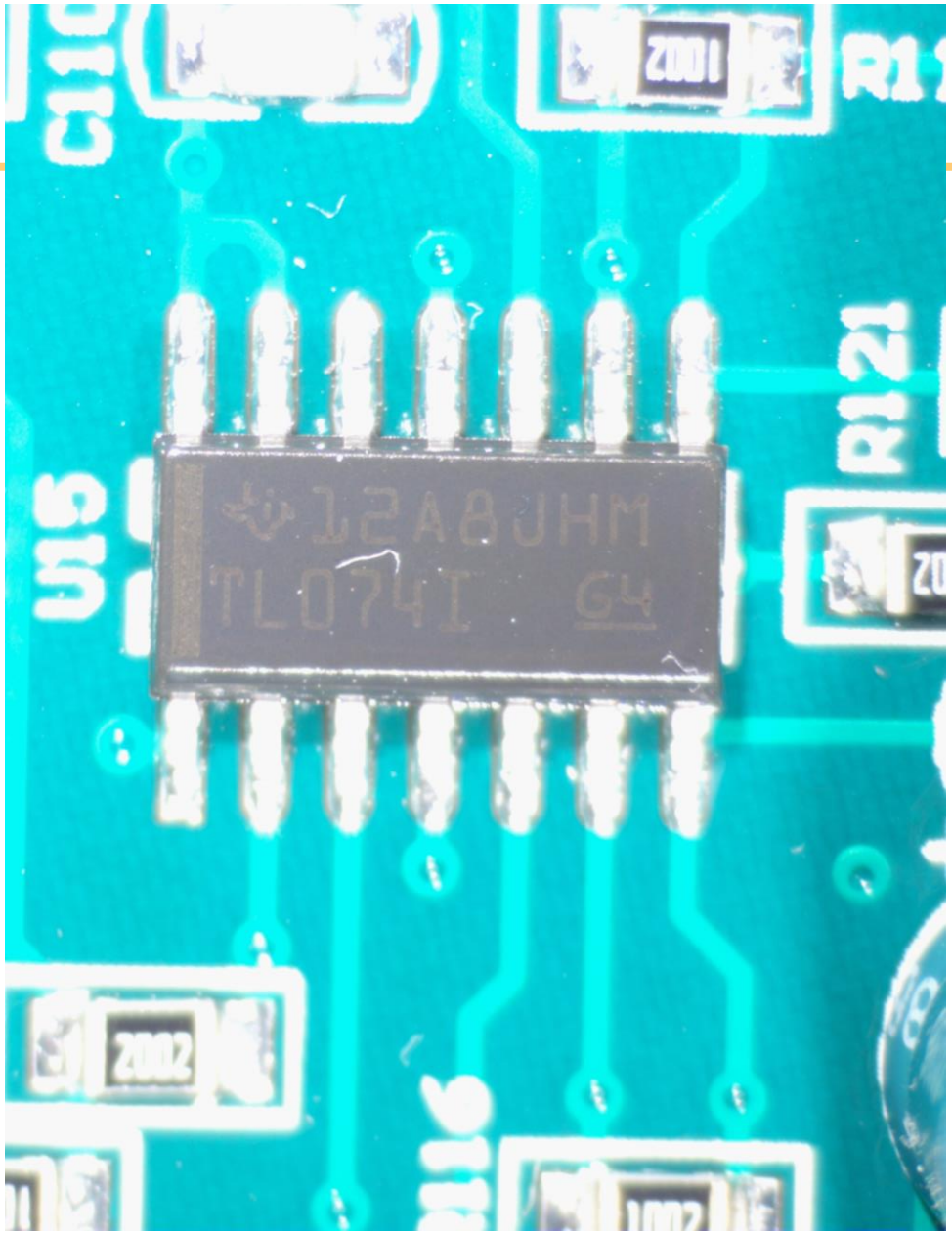
This pillar aims to provide technical assistance to asset owners, manufacturers, system integrators, services providers, and other stakeholders in the ESIB to improve the secure design of technology and systems within ICS/OT.

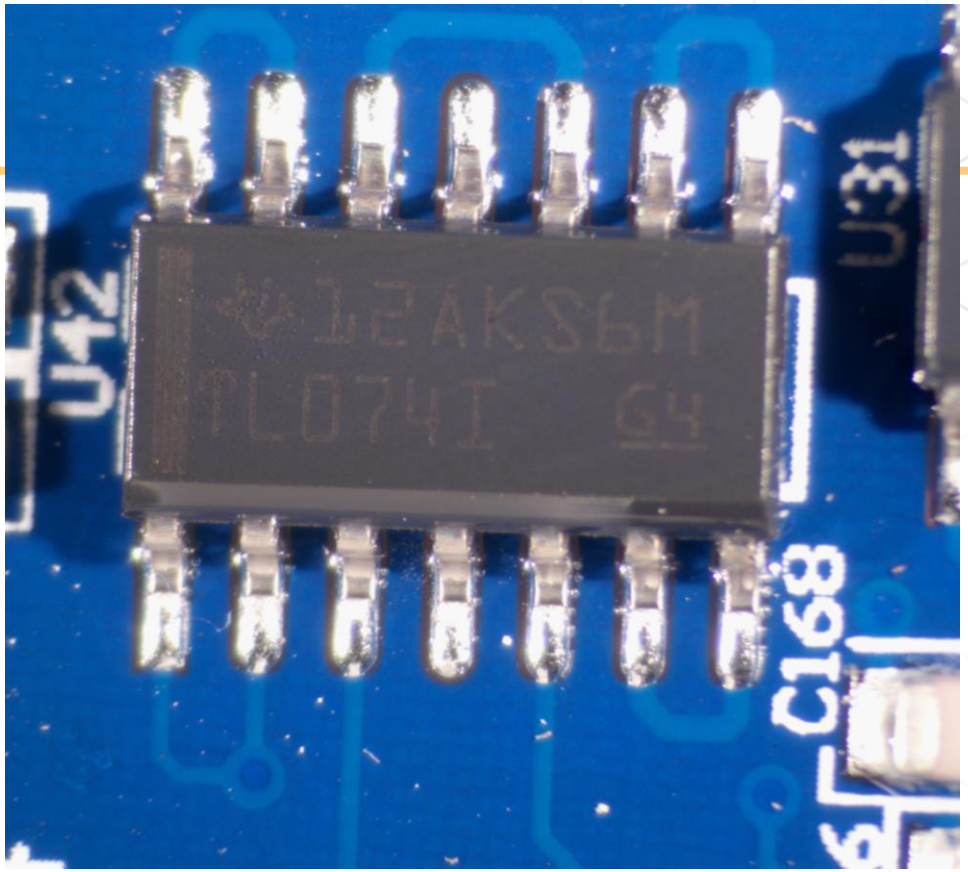
Collaborations with WETO/SETO/OE

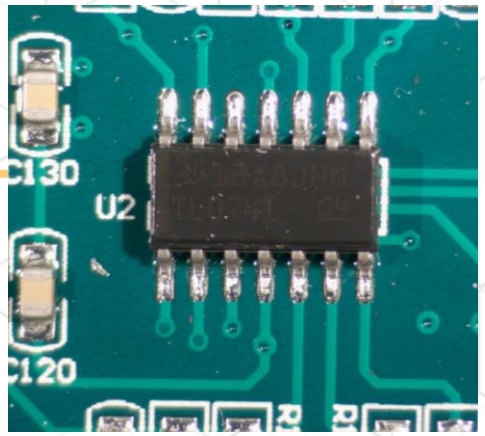
- Goal: Understand critical components used within Energy infrastructure.
- Energy Cyber Sense is collaborating with the following Applied Energy Offices to
  - Wind Energy Technology Office (WETO)
  - Solar Energy Technology Office (SETO)
  - Office of Electricity (OE)
- Research objectives
  - Develop a Hardware Bill of Materials (HBOM)
    - What are the most common components?
    - Are there similarities between similar devices made by different manufacturers?
  - Are there any issues or known vulnerabilities on these components?

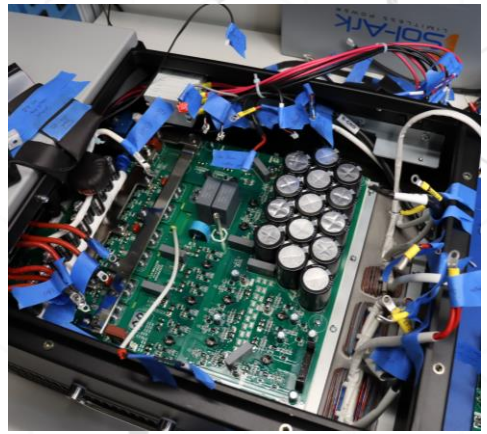
Energy Cyber Sense Collaboration with Solar Energy Technology Office (SETO)

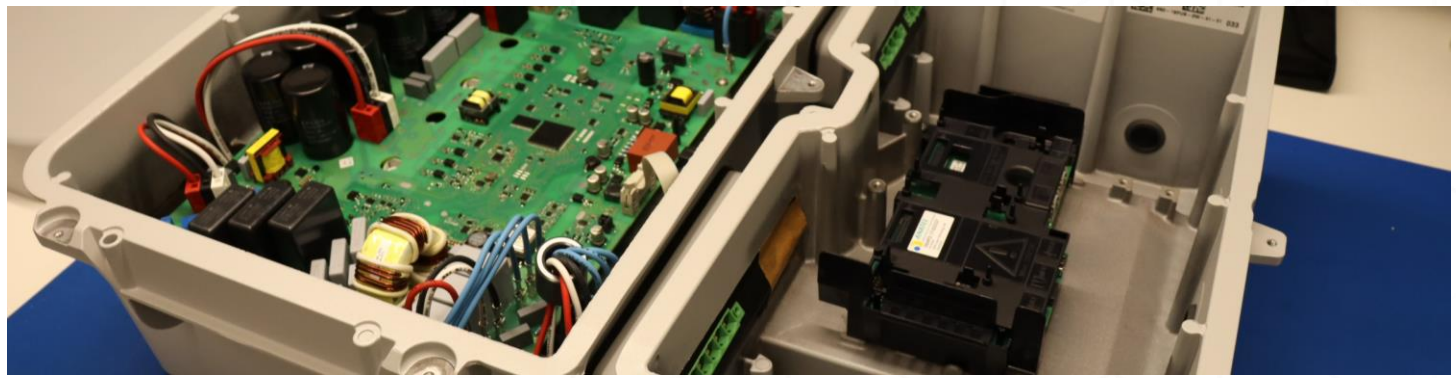
- DOE CESER sponsored program, focused on supply chain security within the Energy sector
  - SETO is specifically focused on solar devices.
- Gain awareness of the supply chain, what are the most common components being used in these systems?
- Develop a hardware bill of materials (HBOM), this includes photos of the system, components, relationships of the components, details on each of the components, datasheets on the components, etc.
  - Build a repository, allowing further research.
  - Example use case: Component matching, have we seen this component before?


U16
R121
TL074I


U42
U31
C168
TL074I


C130
U2
C120

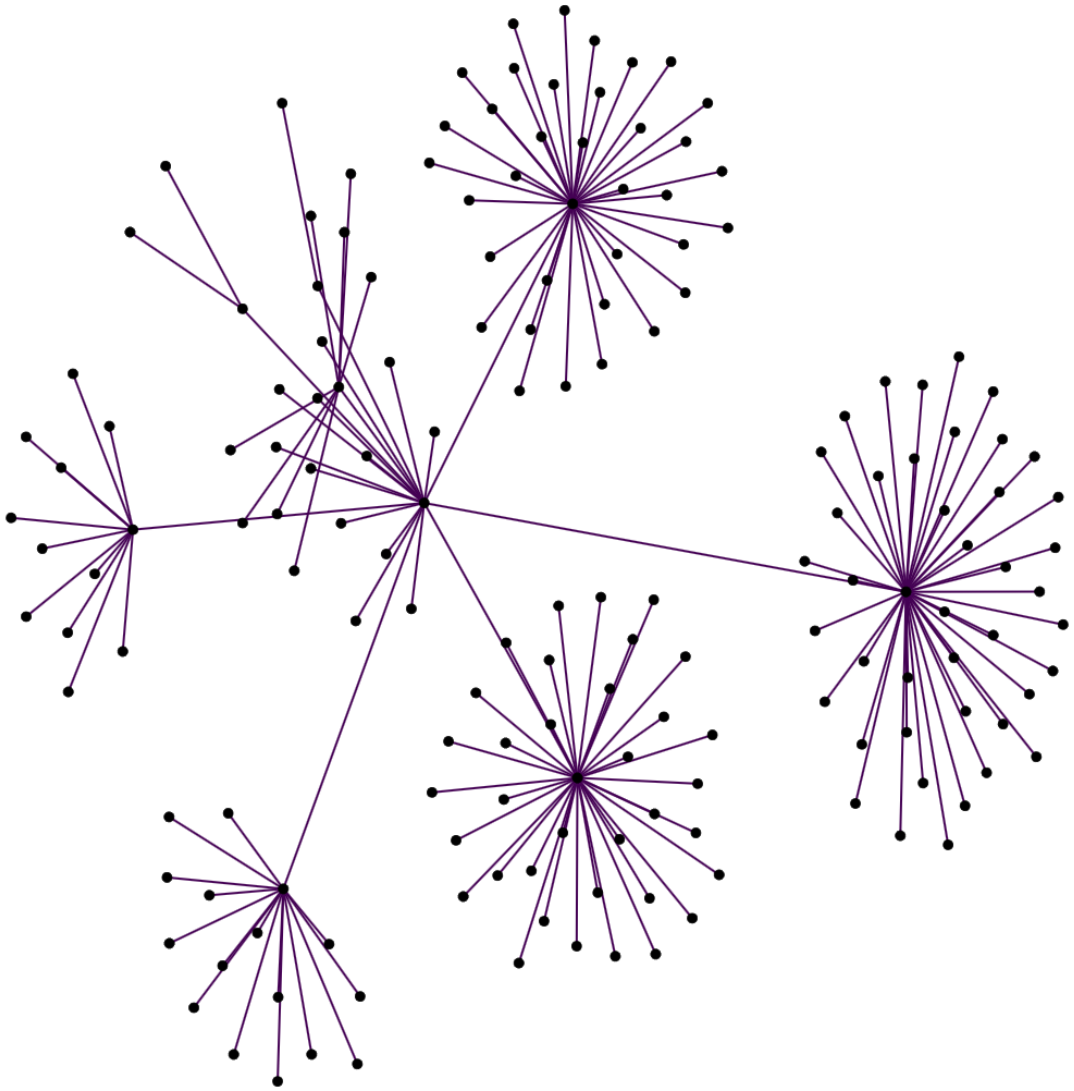




Energy Cyber Sense Collaboration with SETO

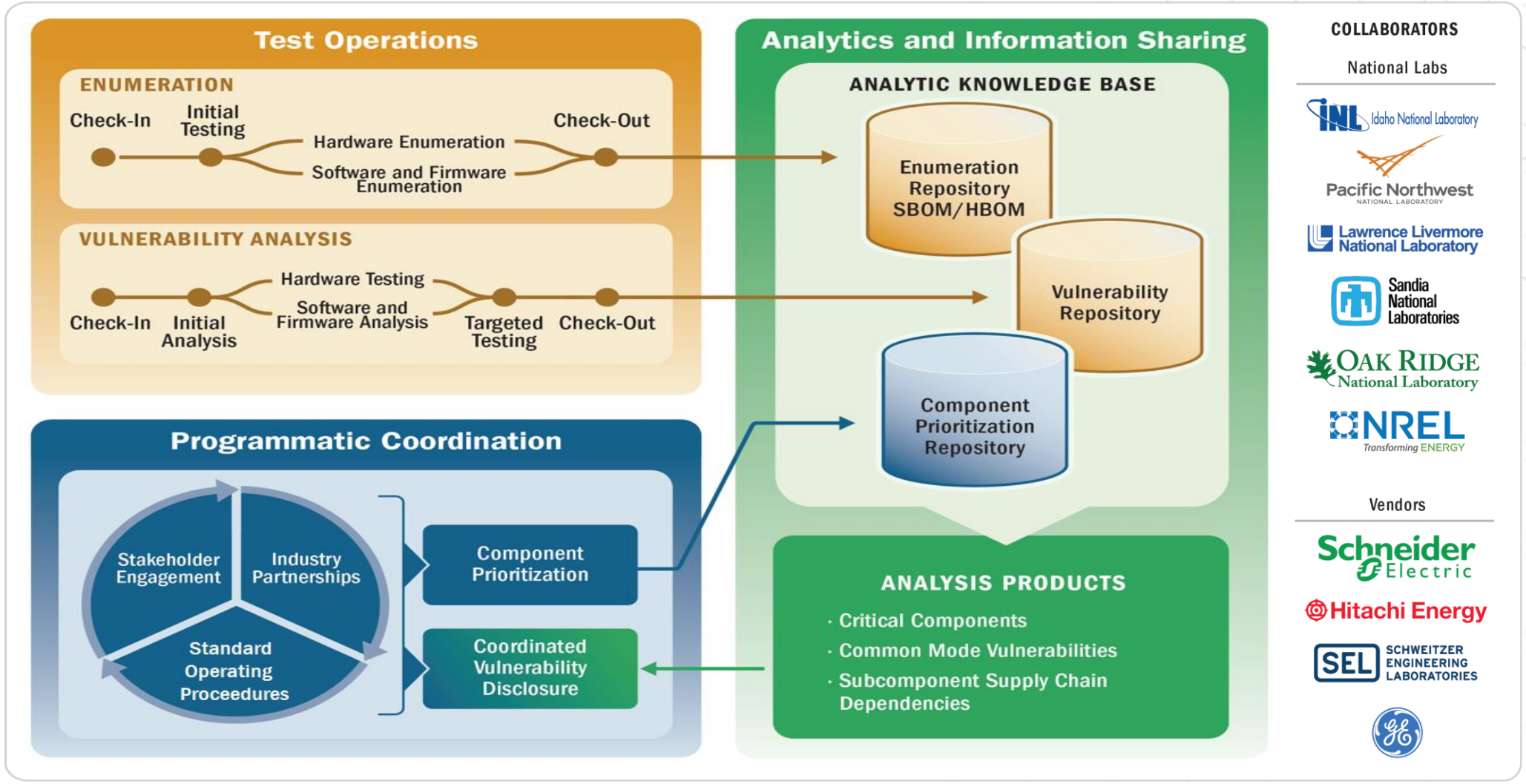
- Compare components on devices
  - E.g., compare solar inverter from one manufacturer to another.
  - What are the similarities and differences?
- Research each key component
  - Have we seen this component before?
  - look for known vulnerabilities / issues on individual components
  - Perform vulnerability matching.
- Develop a report
  - Observations and any findings.
  - Share with DOE CESER and SETO.

Example BOM (Flower Graph)



- A **bill of materials (BOM)** is a list of ingredients of what was found in a specific device/system.
- Typically, hardware and software are represented in separate HBOMs and SBOMs.
- This Flower Graph represents the relationships between the components and subcomponents relative to the system itself, i.e. the central point to which all other points are connected.

Cyber Testing for Resilient Industrial Control Systems (CyTRICS)



Cyber-Informed Engineering (CIE)

Cyber-Informed Engineering

CIE supports Energy Cyber Sense through the CIE Principle:

Cyber-Secure Supply Chain Controls

- Cyber security requirements must flow down to vendors, integrators, and third-party contractors
  - You are only as secure as your least secure vendor
- Procurement language must specify the exact requirements a vendor must comply with as part of the system design, build, integration, or support
- These requirements can raise procurement costs, but without them, caveat emptor
- Be aware of what a subcontractor leaves behind on your network
  - You don't know where subcontractor devices were before today
- Consider vendor tools such as calibration equipment or diagnostic equipment

- Cyber-Informed Engineering Implementation Guide: https://www.osti.gov/biblio/1995796

Cyber Labeling

Goal: Research what could go onto a Security Label

- Based upon research results, provide recommendations to FCC
- Focused on solar inverter and smart meter use cases

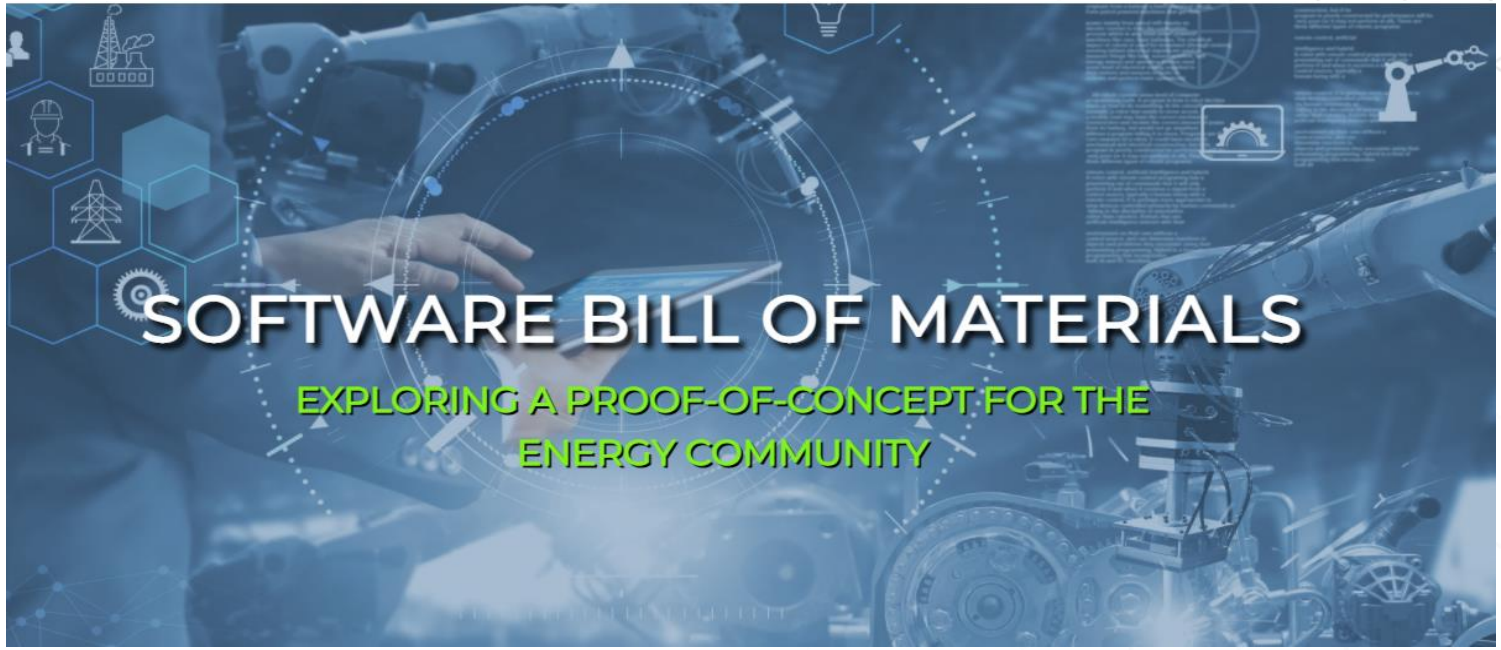
Areas of research:

- *Done:* What standards for labels already exist, what do they care about? International, national, state & local
- *Done:* Should the label be proscriptive (certification) or descriptive (information)?
- *Active:* How do we present information to multiple audiences? (Consumer vs. Utility vs. Integrator...)
- *Active:* What kind of information should be on a label? What purpose will the information serve?
- *Active:* How should that information be presented?
- *Active:* Physical components of label (QR-Code, short link, etc)
- *Additional research topics being identified…*

Add timeline here:

- Phase 1: Developing a label – EO November 2023
- Phase 2: Label Pilot – starts December 2023, finishing March 2024
- Final Research Results Report: July 2024

HBOM/SBOM Adoption by the Energy Sector



https://sbom.inl.gov/

Hardware Bill of Materials

- Driving automated capture and a standard format for Hardware Bill of Materials (HBOM) to exchange with vendors and asset owners

Software Bill of Materials

- Developing tools, technologies, and use cases to catalyze Software Bill of Material (SBOM) adoption by vendors and asset owners

Thank You!

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

Energy Cyber Sense and DOE Programs

The BIL outlines eight requirements for the Program, all of which are supported by existing DOE programs and initiatives. Background on these existing DOE programs and iniatives can be found below, as well as in the Energy Cyber Sense Strategic Plan.

		DOE Supporting Programs and Initiatives							
	Energy Cyber Sense Legislative Requirements	ETAC	CyTRICS	CIE	EO 14017	BOM Pilots	CyManII	CECA	WEST WORLD
1	Establish a testing process under the program to test the cybersecurity of products and technologies intended for use in the energy sector, including products relating to industrial control systems and operational technologies, such as supervisory control and data acquisition systems		✓		✓	✓	✓	✓	✓
2	For products and technologies tested under the program, establish and maintain cybersecurity vulnerability reporting processes and a related database that are integrated with Federal vulnerability coordination processes	✓	✓				✓		✓
3	Provide technical assistance to electric utilities, product manufacturers, and other energy sector stakeholders to develop solutions to mitigate identified cybersecurity vulnerabilities in products and technologies tested under the program	✓	✓	✓			✓	✓	✓
4	Biennially review products and technologies tested under the program for cybersecurity vulnerabilities and provide analysis with respect to how those products and technologies respond to and mitigate cyber threats		✓			✓			
5	Develop guidance that is informed by analysis and testing results under the program for electric utilities and other components of the energy sector for the procurement of products and technologies	✓		✓	✓			✓	✓
6	Provide reasonable notice to, and solicit comments from, the public prior to establishing or revising the testing process under the program		✓						✓
7	Oversee the testing of products and technologies under the program		✓				✓		
8	Consider incentives to encourage the use of analysis and results of testing under the program in the design of products and technologies for use in the energy sector					✓	✓		

BIL-funded Development Activities

- Automated SBOM/HBOM generation capabilities
  - Sandia National Laboratory developing **CopyCat-2** for automating the generation of HBOMs
  - Lawrence Livermore National Laboratory developing **Longclaw** for automating the generation of SBOMs
- Central data repository
  - Pacific Northwest National Laboratory has deployed the **Energy Cyber Sense central data repository**, enabling querying of enumeration data across all BOMs received to identify common mode vulnerabilities
- Advanced analytics capabilities
  - Includes capabilities like **retrospective analysis**, **cross-component analysis**, and **system-level impact analysis**

CyTRICS Test Process

	Enumeration	Vulnerability Analysis
Check-in	**Establish a baseline condition for system and configurations.**	**Establish a baseline condition for system and configurations.**
Initial	Enumeration of interfaces and services. Also, a minimal evaluation of the security and operational constraints of the system before a time-consuming, in-depth analysis.	Perform tests to understand the security model of a system, enumerate interfaces, identify services, evaluate security controls, and identify vulnerabilities.
Hardware	Physical analysis of hardware components that enables component identification. Note: this step is not performed for software-only enumeration.	Extract firmware, access in-circuit debug ports, and analyze hardware security features. Different levels of disassembly and removal will be performed as defined in the test plan.
Software/Firmware	Component identification of libraries, operating systems, and dependencies, including third-party libraries, operating systems, and utilities within the software and firmware.	Discover and analyze functionality to identify relevant weaknesses in the security of the system.
Targeted		Execute tests designed to further explore potential weaknesses or issues discovered within the analysis phase. This might require further realism, including full-scale operation of the system. Mitigations for identified vulnerabilities as well as specific counterfeit detection activities can be developed during this step.
Checkout	**Documentation of the final state of the system, including any changes in system functionality or capability based on the tests performed.**	**Documentation of the final state of the system, including any changes in system functionality or capability based on the tests performed.**

CyTRICS™ Impact-Based Prioritization

Impact	Prevalence	Technical Characteristics	Maintainability	Overriding Considerations
Operational Impact	Ubiquity	Network Enablement	Continuing Support	Intelligence
Safety Impact	Deployment Scale	Complexity	Deployability	National Security
Environmental Impact	Remaining Period of Use	Scope of Control		Strategic Considerations

North American Transmission FORUM

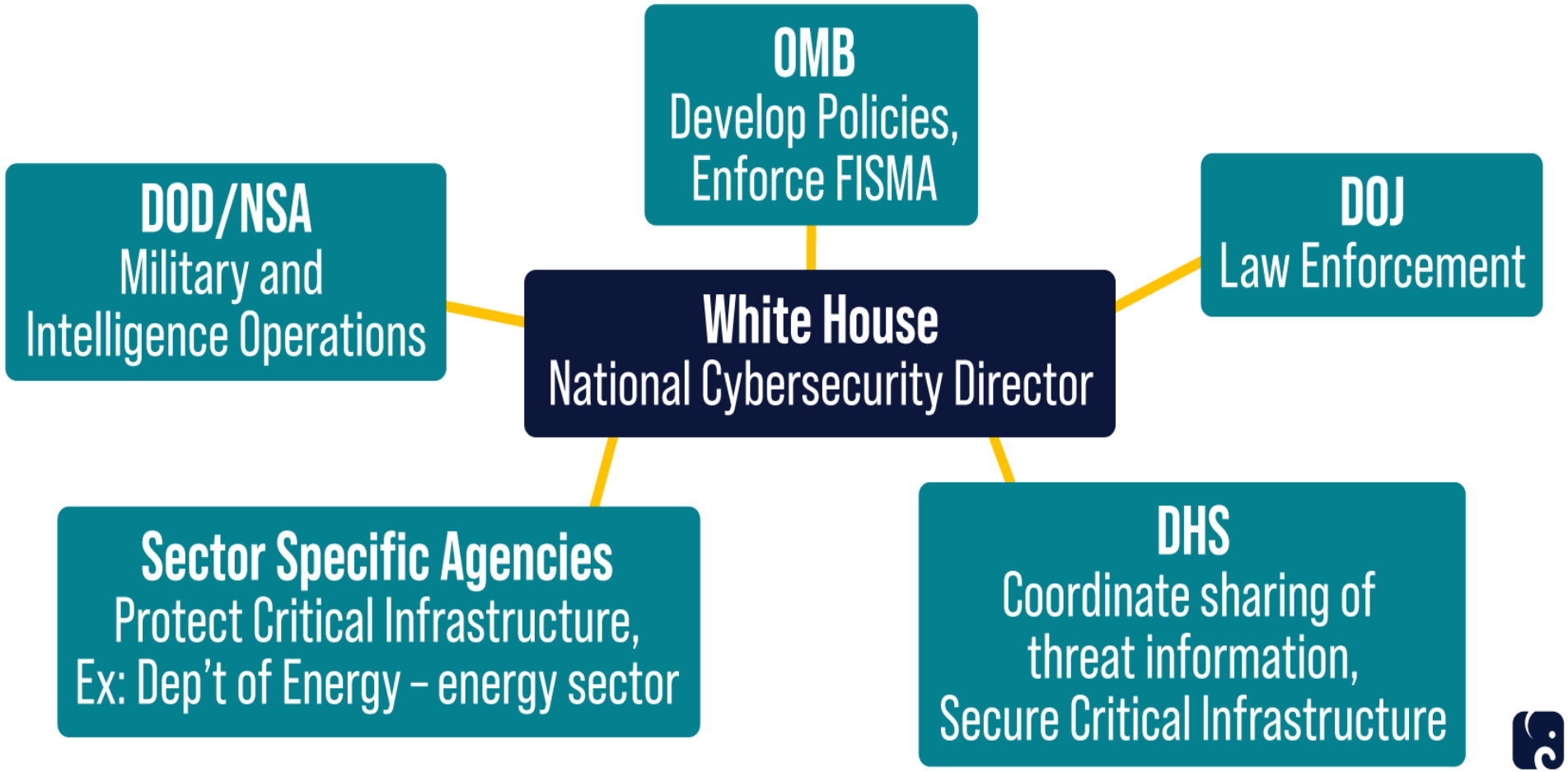
Community *Confidentiality* *Candor* *Commitment*

National Strategy

Frank Harrill
VP, Security, Schweitzer Engineering (SEL)
and
Heath Knakmuhs
VP and Policy Counsel, US Chamber of Commerce

A National Strategy to Support Cybersecurity

Key Cybersecurity Players



And…

Executive Order on Improving the Nation's Cybersecurity

Released: May 2021

- Removing barriers to sharing threat information
- Modernizing federal government cybersecurity
- Enhancing software supply chain security
- Establishing a cyber safety review board
- Standardizing federal response playbooks
- Improving detection on federal government networks
- Improving federal investigative and remediation capabilities
- National security systems

National Cybersecurity Strategy

Released: March 2023

1. Defending Critical Infrastructure
2. Disrupting and Dismantling Threat Actors
3. Shaping Market Forces and Driving Security and Resilience
4. Investing in a Resilient Future
5. Forging International Partnerships to Pursue Shared Goals

Key Industry Request … *Harmonization*

ONCD RFI Issued August 16, 2023 Comments due October 31, 2023

“Opportunities for and obstacles to harmonizing cybersecurity regulations”

Per Strategic Objective 1.1 of the National Cybersecurity Strategy

1. Fragmented Regulatory Landscape
    a. Compliance Burden
    b. Inefficiency
    c. Inadequate Coverage

2. Outcome Focused, Risk-Based, Consensus Standards are Critical for Driving Regulatory Cohesion

3. Key Harmonization Wins (NIST Cyber Framework; ISA-62443)

Key Industry Request … *Harmonization*

ONCD RFI Issued August 16, 2023 Comments due October 31, 2023

“Opportunities for and obstacles to harmonizing cybersecurity regulations”

Per Strategic Objective 1.1 of the National Cybersecurity Strategy

4. International Cooperation is Critical
   - *Cohesive global cyber framework*
   - *Avoid digital sovereignty requirements*

5. Challenges Create Barriers
   - *Sovereignty concerns; differing priorities; regulator personalization; mitigation of emerging risks; time commitment*

6. White House Should Establish Regulatory Harmonization Office

National Cybersecurity Strategy Implementation Plan

Released: July 2023

- Prevent abuse of U.S. based infrastructure (Q4 2025)
- Shift liability for insecure software products and safe harbor liability framework (Q2 FY24)
  - SBOMs and database of end-of-life components; emphasis on coordinated disclosure (Q2 FY25)
- Prioritize investments to accelerate the adoption of memory safe programming languages (Q1 FY24)

Update to OMB Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

Original Released: September 2022, updated June 2023

- Secure development attestation from suppliers required for software developed after 09/14/2022 three months after attestation common form is approved by OMB
- CISA released draft Secure Software Self-Attestation Common Form during April 2023
- Requirements drawn from NIST SP 800-218, Secure Software Development Framework” (SSDF)

Compliance with the NIST SSDF

- Development and production environments are segmented, activities within them are logged and audited, protected by MFA, encryption, and other layers of defense
- Source code and component supply chains are curated based on risk, including provenance information
- Automated tools are used to check for security vulnerabilities
- A system is in place to ensure these processes operate consistently and that vulnerabilities are disclosed in a timely manner

Joint Secure by Design and Default Guidance

Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing

Comment period ends 12/04/2023

- Software Bill of Material (SBOM) development, maintenance, and provision requirement
- Actual or potential security incident reporting requirement within eight hours of discovery
  - Malware uploaded within eight hours
  - Incident data preservation for 18 months
- FBI and CISA must be granted full access to relevant incident systems and data
- Security incident reporting harmonization, AIS participation, IPv6

Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems

Comment period ends 12/04/2023

- Federal information systems FIPS 199 assessment requirement
- Cross references incident reporting in the cyber threat and incident reporting and information sharing FAR
- Requirement to maintain an operational technology list with physical locations

Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

Released: 10/30/2023

- Invoked the Defense Production Act
- NIST directed to create standards to ensure systems are reasonably safe and secure before public release
- Requires non-public testing of certain AI systems to ensure they cannot be used to produce biological or nuclear weapons
- Requires foreign customer disclosure
- Immigration changes to attract and retain AI talent
- Recommends watermarking of content
- Government website: https://ai.gov/

Information Sharing Opportunities

- E-ISAC and other Information Sharing and Analysis Centers
- Homeland Security Information Network (HSIN)
- National Cyber Awareness System (NCAS)
- CISA Automated Indicator Sharing (AIS)
- NSA Cyber Collaboration Center
- FBI Infragard

Move beyond compliance

Develop a risk-based security management system using a recognized standard.

- CIS Critical Security Controls
- NIST Cybersecurity Framework
- ISO 27001
- IEC 62443

Questions?

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

BREAK

Return at 3:15

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Considerations for International Suppliers

Christopher Fitzhugh
Industrial Cybersecurity Consultant, North America, Siemens Energy
and
Michael Pyle
Director of Product Cyber Security, Energy Management Business, Schneider Electric

Dealing With Cybersecurity Regulations

Current situation

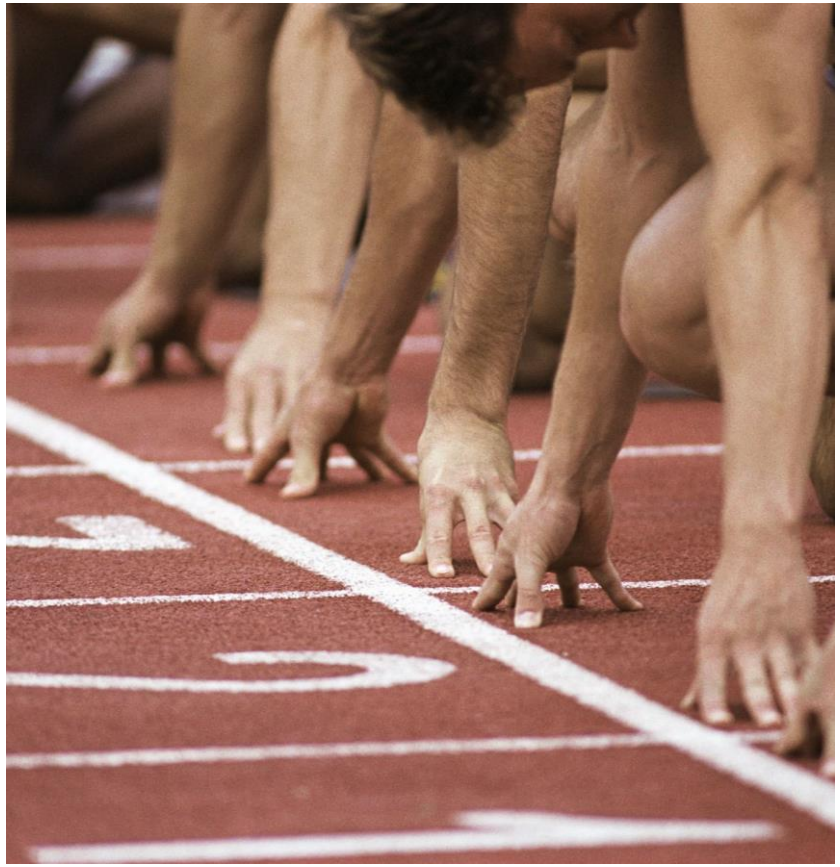
- Law makers are seeing the need for cybersecurity and data privacy regulations to address the growing demand to “digitize” our world
- As a result, new regulations addressing cybersecurity and data privacy are popping up in different regions and countries across the globe.
- Each regulation might have its own spin on requirements
- Compliance with these regulations will be mandatory to do business in their respective regions or countries

Challenges

- Complex and Ambiguous regulations
- Compliance with multiple regulations and even market segment requirements across the world
- Rapidly evolving technology and threats
- Evolving regulations as law makers react to the changing threat landscape
  - According to a report by KPMG, Regulators are looking to strengthen data risk management, especially in areas such as governance incident reporting, vulnerability management, and identity/access management. [1]
- Lack of skilled, knowledgeable resources
- Third party risks, both from vulnerabilities and to compliance
- Older devices that can’t be brought into compliance

Preparation

- Understand the requirements
  - Inventory the regulations applicable to your business
  - Ask questions of the regulators
  - Provide feedback to regulators when and where possible
  - Can we self-declare compliance, or must we be certified?
- Prioritize regulations based on potential impact to your business
- Develop a strategy and plan on how to meet the requirements
- Train your staff; if possible, bring on experienced resources to assist
- Implement, monitor and maintain security controls for your organization



Example: Global Security & Privacy Regulation Heatmap

*Final text expected **

2022 | 2023 | 2024

Impact to Business

HIGH

- **Privacy** — **Indonesia** Personal Data Protection Law
- **Trade controls** — **China** Restricted and Prohibited Technologies for Export
- **Trade controls** — **China** Micron ban
- **Trade controls** — **India** IT hardware import restrictions
- **Cybersecurity** — **India** draft IoT Security and Privacy standards
- **Cybersecurity** — **US** NIST Cybersecurity Framework 2.0
- **Cybersecurity** — **EU** Cloud Service Certification Scheme
- **Cybersecurity** — **China** Measures of Security Assessment for Data Export
- **Cybersecurity** — **EU** NIS 2
- **Data** — **EU** Data Act
- **Cybersecurity** — **US** National Cyber Strategy Implementation Plan
- **Privacy** — **China** Draft Provisions on Regulating and Promoting Cross Border Data Flows
- **Cybersecurity** — **EU** Cyber Resilience Act
- **Cybersecurity** — **US** FAR Rule Cyber Threat Sharing & Incident Reporting
- **Cybersecurity** — **US** Cyber Maturity Model Certification
- **Cybersecurity** — **US** FAR Rule Standardizing Contract Requirements
- **Cybersecurity** — **EU** Managed Security Providers Certification Schemes
- **Privacy** — **Saudi** Personal Data Protection Law Implementing Regulations
- **Privacy** — **Saudi** Personal Data Transfer Regulations
- **AI** — **EU** AI Act
- **Cybersecurity** — **US** CISA regulation from CIRCIA

MEDIUM

- **Cybersecurity** — **Australia** Critical Infrastructure Protection Act
- **Cybersecurity** — **Australia** Critical Infrastructure Protection Act
- **Cybersecurity** — **EU** Machinery Regulation
- **Trade Control** — **US** AI Chips Export Controls
- **Cybersecurity** — **Indonesia** Cybersecurity Bill (pending draft)
- **Cybersecurity** — **U.S.** Voluntary Consumer IoT Cyber Label
- **Cybersecurity** — **EU** Product Liability Directive
- **Privacy** — **UAE** Federal Personal Data Protection Law
- **Cybersecurity** — **US** NDAA 2023 Semi Supply Chain
- **Cybersecurity** — **India** CERT-in Incident Reporting Rules
- **Privacy** — **India** Digital Personal Data Protection Act
- **Data Centers** — **Saudi Arabia** Draft Data Centers Regulation
- **Cybersecurity** — **U.S.** FASCSA Interim Rule
- **AI** — **EU** AI Liability Directive
- **Trade Control** — **US** Commerce ICTS Prohibition Rule
- **Privacy** — **EU-US** Data Privacy Framework (Schrems III)
- **Cybersecurity** — **US** TSA Pipeline Cyber Directive Update
- **Privacy** — **US** State-level privacy laws
- **Trade Control** — **US** Outbound Investment EO
- **Cybersecurity** — **Singapore** Cybersecurity Act amendments
- **Cybersecurity** — **U.S.** DOE IIoT Label for Smart Meters & Inverters

LOW

- **Competition** — **EU** Digital Services Act
- **Cybersecurity** — **Indonesia** Protection of VII Regulation
- **Trade controls** — **US** NDAA Printed Circuit Boards
- **Cybersecurity & Data** — **EU** Digitalization of the Energy Action Plan
- **Trade controls** — **China** gallium and germanium export restrictions
- **AI** — **China** Interim Measures on Generative AI
- **Cybersecurity** — **US** SEC Cyber Incident Reporting Final Rule
- **Foreign Policy** — **China** Foreign Relations Law
- **Digital** — **India** Digital India Bill
- **Privacy** — **Argentina** Personal Data Protection Bill
- **Data** — **Brazil** Draft Reg for Int'l Data Transfers
- **Cybersecurity** — **Canada** C-26 Act Respecting Cyber Security
- **AI** — **Canada** C-27 AI & Data Act

Action

- Identify and **implement** international standards such as ISA/IEC 62443 and ISO 2700x that are most relevant to your markets and types of products
  - Many regulations have their basis in international standards
  - They will get you close and give you a solid foundation to build on to become compliant
- Map regulations, guidance, and frameworks to the standards
  - Leverage work already done such as CISA's Cyber Resilience Review
- Address your product development environments; Establish a secure development process, strong DevSecOps workflow, train in secure coding practices and secure system architecture
- Get your supply chain in order; establish SLAs and Terms and Conditions required from your suppliers for your company to be compliant with the regulations

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Getting Ahead of Regulation

Panel Discussion

Panelists

- Jennifer Couch, Manager, Transmission EMS Compliance, Southern Company
- Christopher Fitzhugh, Industrial Cybersecurity Consultant, North America, Siemens Energy
- Frank Harrill, VP, Security, Schweitzer Engineering (SEL)
- Mike Pyle, Director of Product Cyber Security, Energy Management Business, Schneider Electric
- *Moderated by Heath Knakmuhs, VP and Policy Counsel, US Chamber of Commerce*

Frank Harrill

VP, Security, SEL

Closing Remarks

Frank Harrill
VP, Security Schweitzer Engineering (SEL)

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Thank you for attending!

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

Links from the webinar chat:

https://www.cisa.gov/sites/default/files/2023-10/Software-Identification-Ecosystem-Option-Analysis-508c.pdf

https://www.cisa.gov/sites/default/files/2023-11/When-to-Issue-a-VEX-508c.pdf

https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/

https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112