NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Joint Security Summit Presentation Package

Presentations are posted with the written consent of the authors.
Joint SCWG/SWG/SITES Meeting
March 23, 2023

RELIABILITY | RESILIENCE | SECURITY




March 23, 2023

Sam Chanoski
Technical Relationship Manager

Idaho National Laboratory Energy Cybersecurity Programs Update

NERC RSTC Security Groups Summit

Idaho National Laboratory

INL/MIS-23-71834

INL's Position Nationally

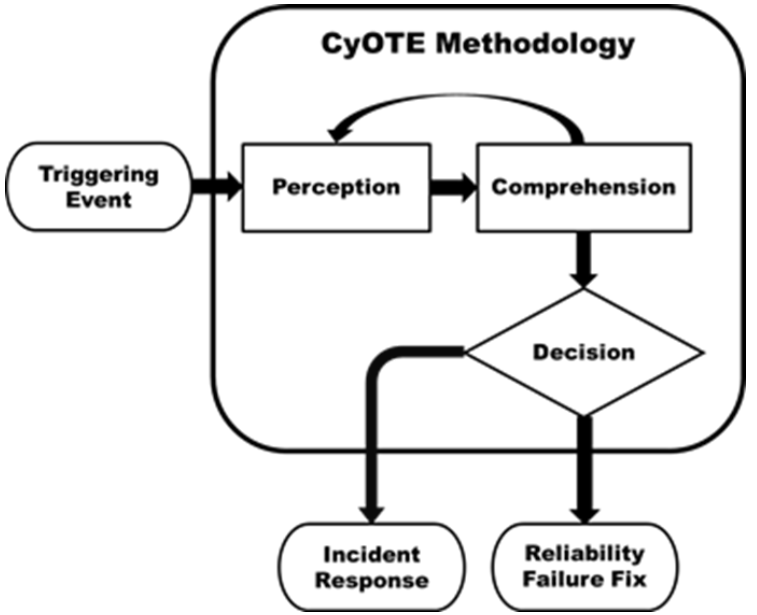
- Network of 17 DOE National Laboratories
- Center for National Security & Clean Energy
- Lead Laboratory for Nuclear Energy R&D
- Labs are Capability Machines
- Labs innovate to solve multi-disciplinary problems
- Do what others can't, won't, or shouldn't do

Cybersecurity for the Operational Technology Environment (CyOTE)

Cybersecurity for Operational Technology Environments (CyOTE™)

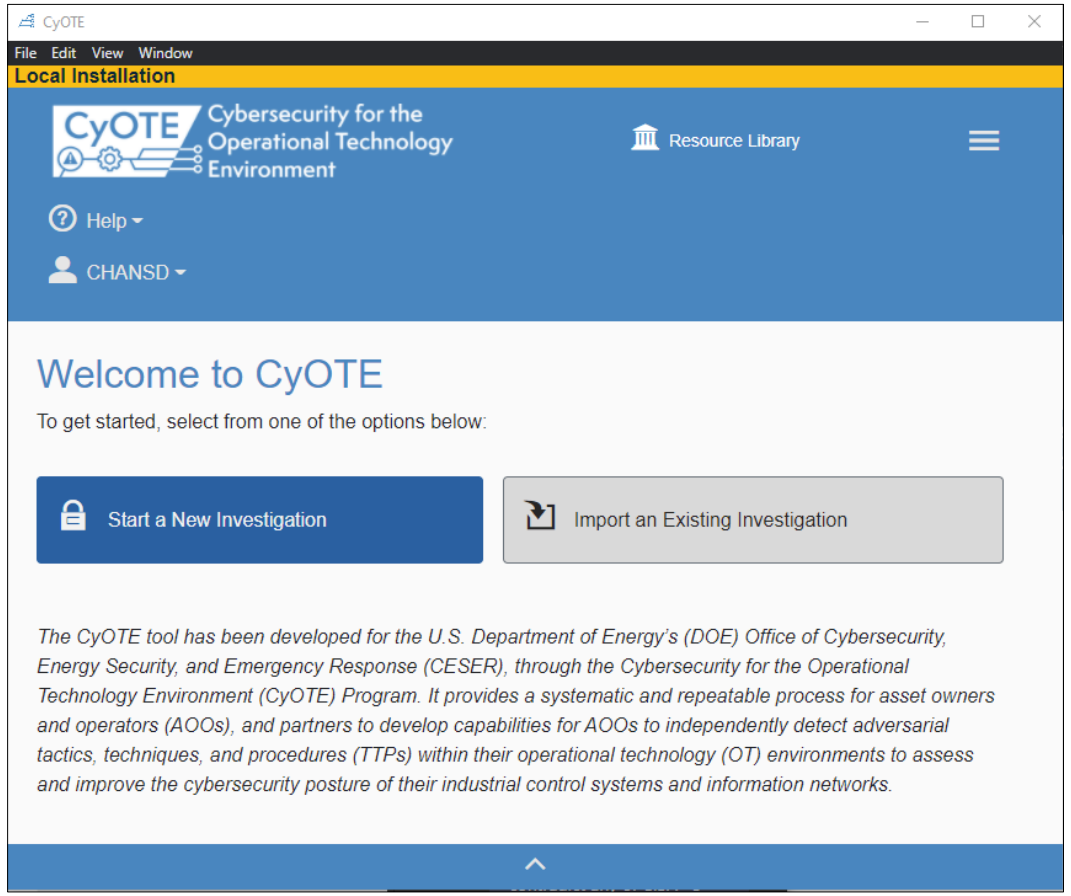
- Continuing to produce **Precursor Analysis Reports** identifying observables and artifacts correlated to adversary techniques
- Job aid **Application tool** in beta testing
  - Anticipate industry release in the next month
- **”Alexandria” library of observables** in development
  - Anticipate industry release in late 2023
- For more information: https://inl.gov/cyote/

CyOTE Cybersecurity for the Operational Technology Environment



CyOTE Application

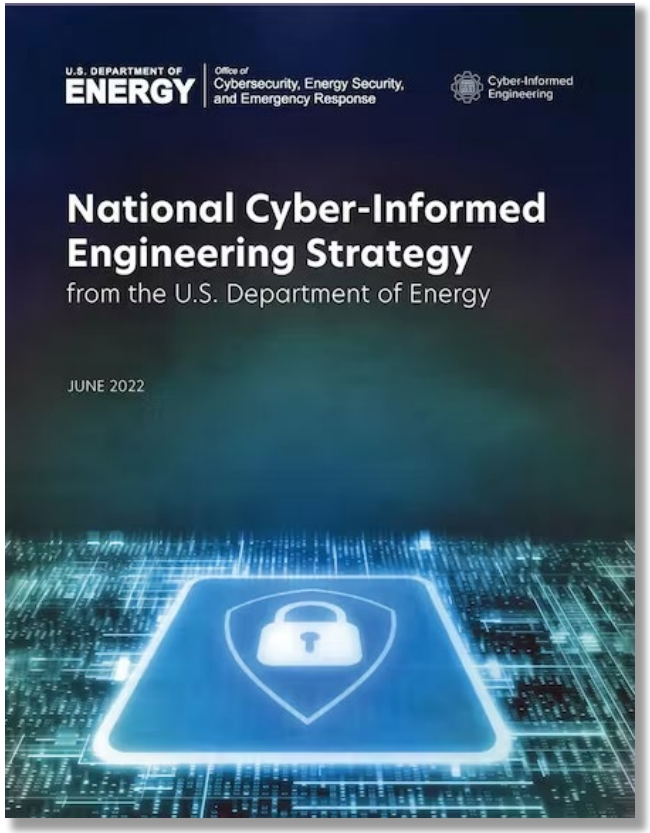
- Structured job aid to implement CyOTE methodology
  - Real-world investigation
  - Post-mortem review
  - Exercises
- Provides suggestions and produces documentation
- Similar look and feel to CSET



Cyber-Informed Engineering (CIE)

Cyber-Informed Engineering

- CIE uses **design decisions** and **engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to "engineer out" cyber risk** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to engender a **culture of security** aligned with the existing industry safety culture.
- For more information: https://inl.gov/cie/



Key Premises of the CIE Strategy

Today's risk landscape calls for systems that are engineered to continue operating critical functions while faced with increasingly severe and sophisticated cyber attacks from intelligent, determined adversaries.

While specialized IT and OT cybersecurity experts bring strong skills, **many engineers and technicians who design and operate control systems with digital components currently lack sufficient cybersecurity education** and training to adequately address the risk of cyber-enabled sabotage, exploitation, failure, and misuse in the design, development, and operational lifecycle.

Accelerating industry's adoption of a culture of cybersecurity by design—complementing industry's strong culture of safety—offers the ability to maintain secure design even as systems evolve and grow in functionality.

CIE offers an opportunity to reduce risk across the entire device or system lifecycle, starting from the earliest possible phase of design.

Early in the design phase is often the most optimal time to achieve low cost and effective cybersecurity, compared to solutions introduced late in the engineering lifecycle.

CIE and Technology Readiness Levels

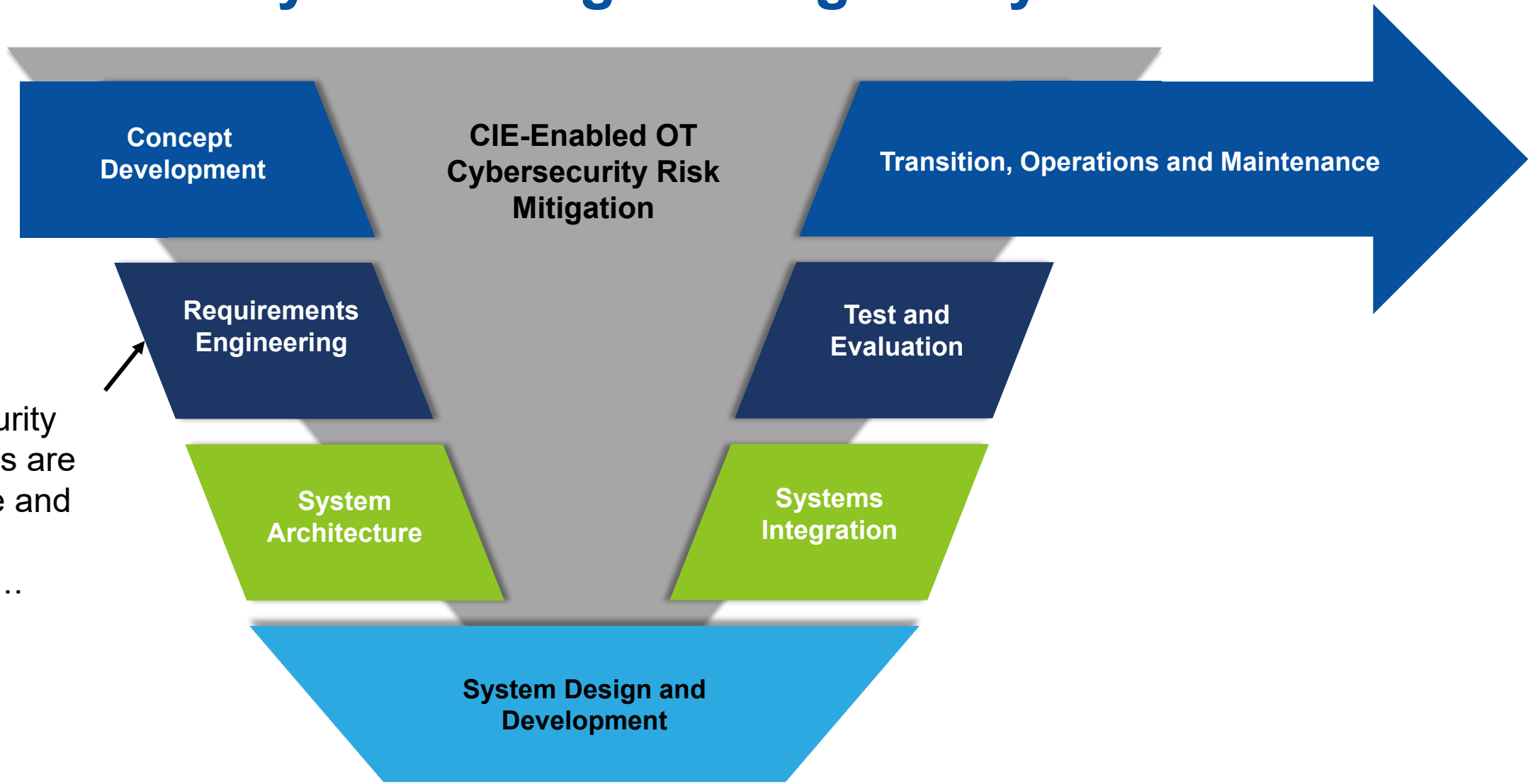
Traditional OT Cybersecurity risk mitigations are usually applied here…

CIE and Technology Readiness Levels

Traditional OT Cybersecurity risk mitigations are usually applied here…

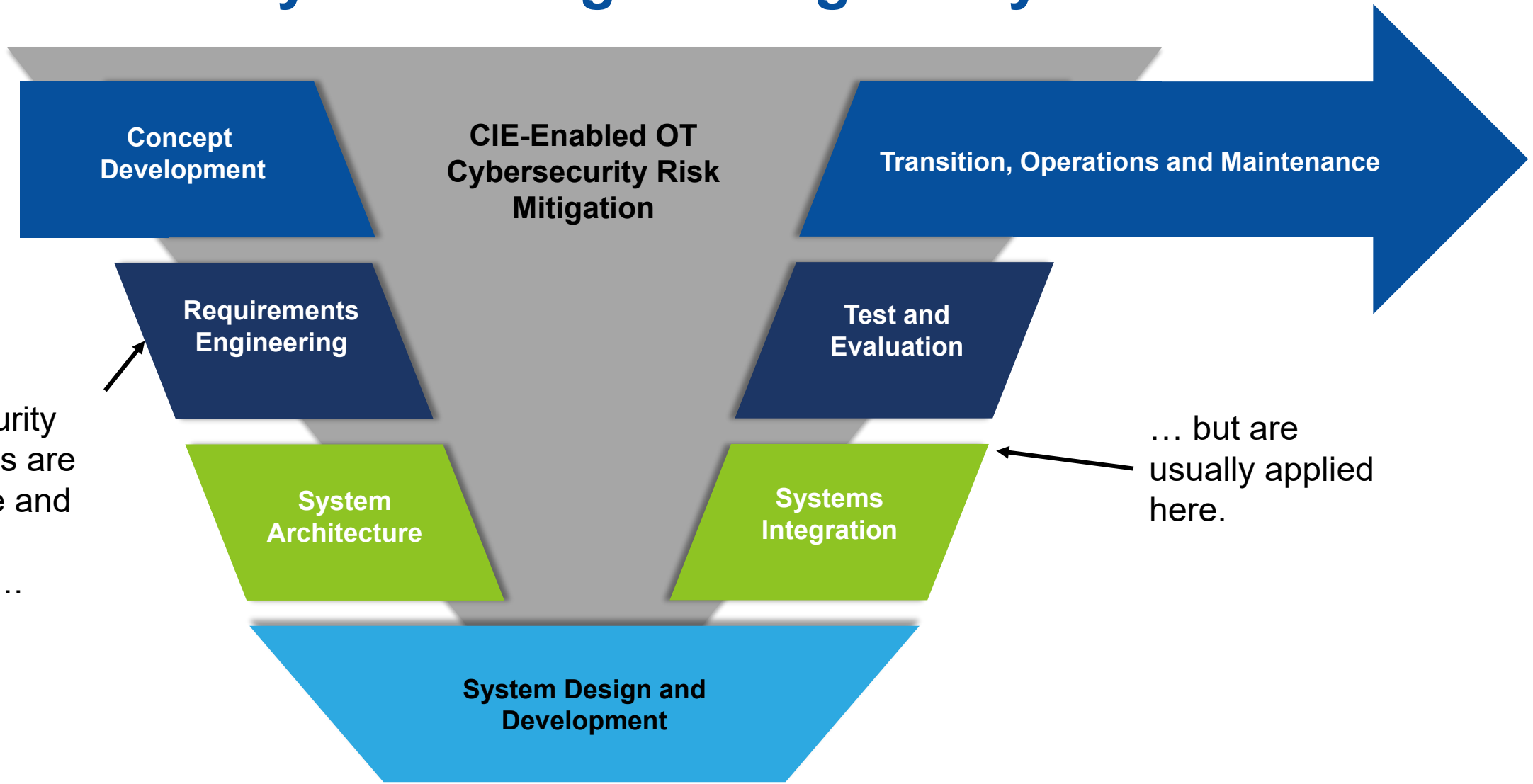
… but are more effective and efficient when applied here.

CIE and the Systems Engineering Lifecycle



OT Cybersecurity risk mitigations are more effective and efficient when applied here….

CIE and the Systems Engineering Lifecycle



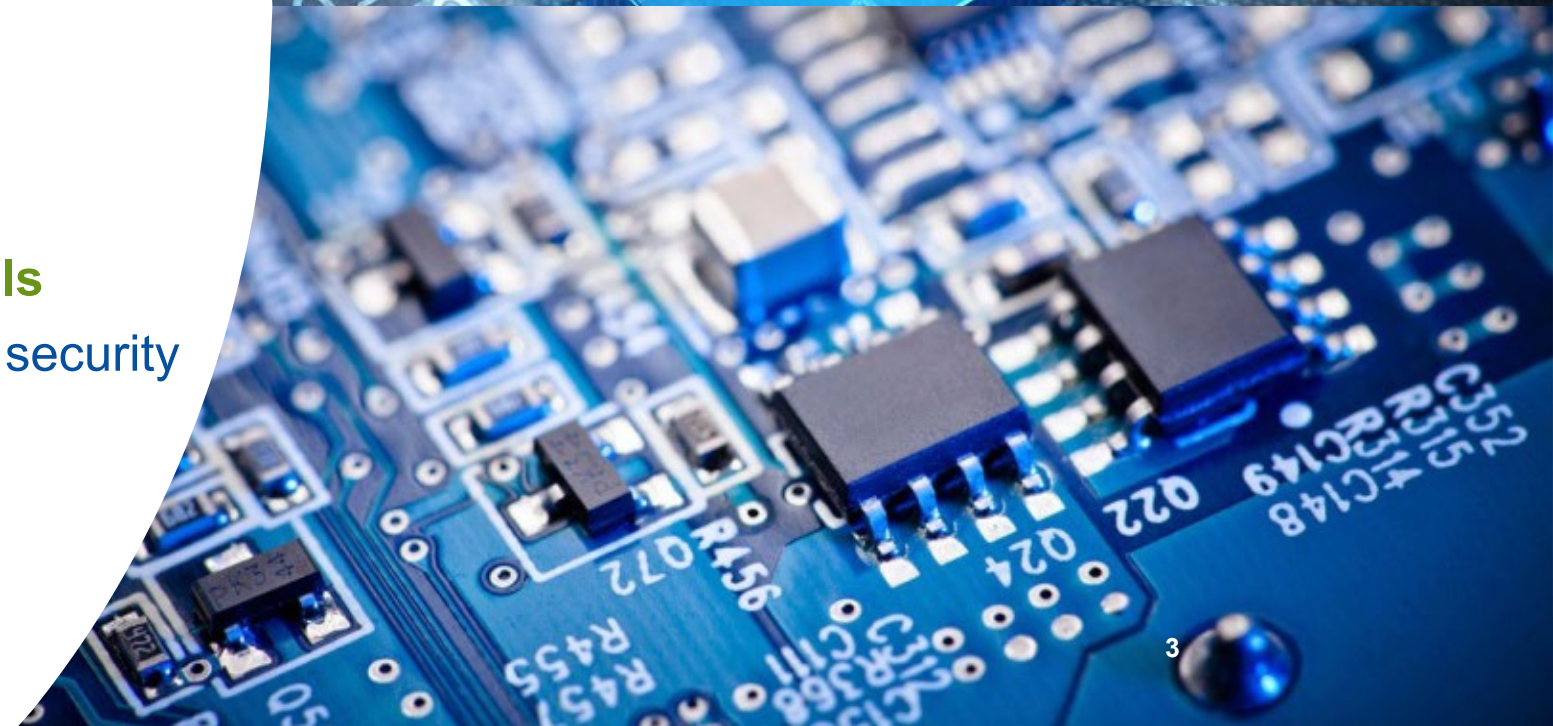
OT Cybersecurity risk mitigations are more effective and efficient when applied here….

… but are usually applied here.

Principles of CIE

- **Consequence-focused design**
- Engineered Controls
- Secure information architecture
- Design Simplification
- Resilient layered defenses
- Active defense

- Interdependency evaluation
- Digital asset awareness
- **Cyber-secure supply chain controls**
- Planned resilience with no assumed security
- Engineering information control
- Security culture



Consequence-Focused Design

- What must happen?
- What must not happen?
- What governs my risk appetite?

Cyber-Secure Supply Chain

- 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

CIE Community of Practice and Working Groups

Cyber-Informed Engineering COP

Started Jan. 2023
Quarterly

Multi-stakeholder team to aid the translation of CIE into technical requirements that can inform guidance, practices, and standards development

CIE Education WG

Monthly started Feb. 2023
Chair: Marc Sachs, Auburn University

Develop curricula and materials that integrate CIE principles into engineering degree programs

CIE Development & Tools WG

Monthly started Feb. 2023
Chair: Ginger Wright, Idaho National Lab

Develop CIE implementation guidance and an open-source library of resources

CIE Standards WG

(Coming Soon; start date TBD)
Chair: TBD

Support integration of CIE into engineering and cybersecurity standards

Supply Chain Security

Cyber Testing for Resilient Industrial Control Systems (CyTRICS)

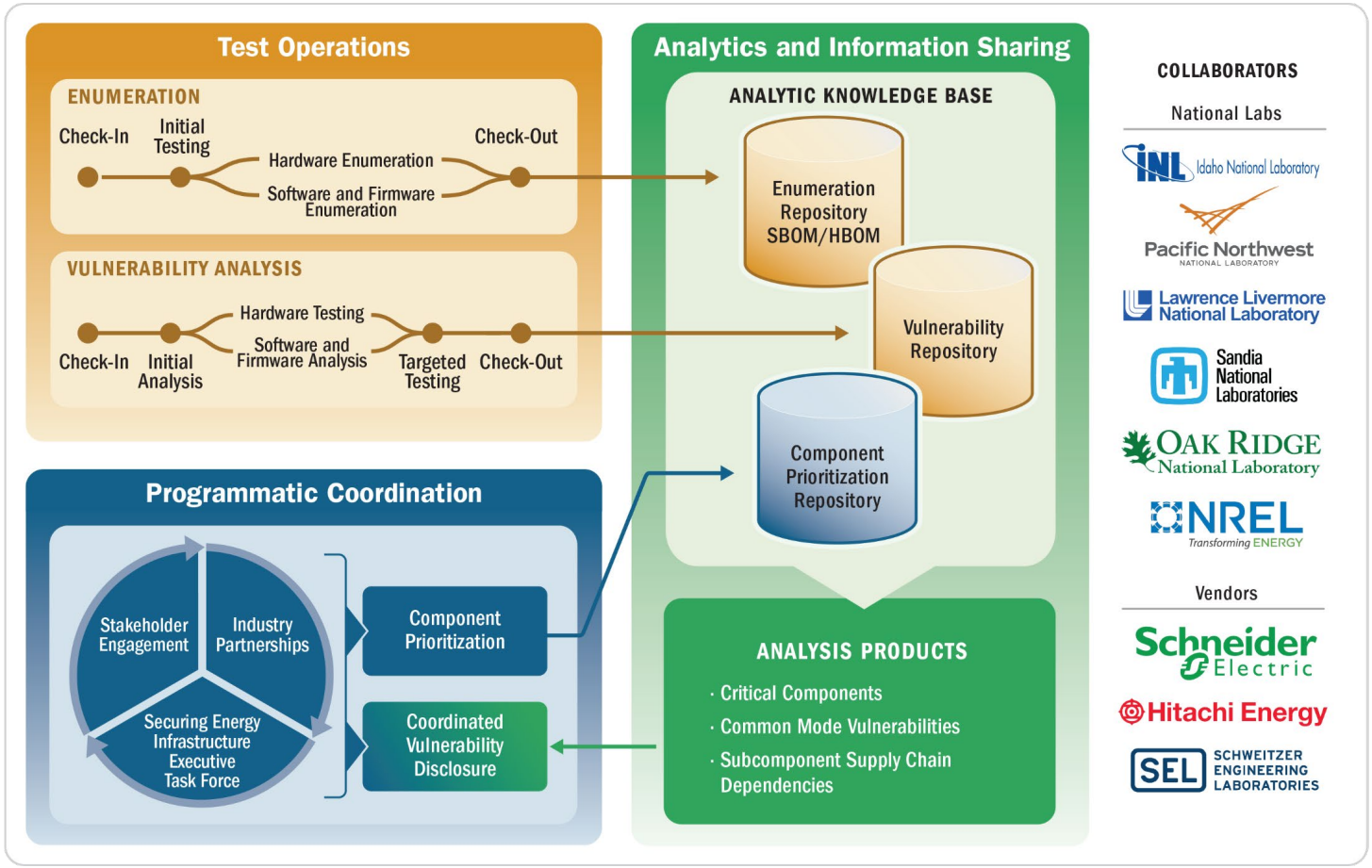
- Work with manufacturers and asset owners to discover, mitigate, and ultimately engineer out cyber vulnerabilities in digital components in energy sector critical supply chains
- Synergies with **Energy Cyber Sense Program** (IIJA, Section 40122)
- **SBOM Proof of Concept** for Energy Sector
- For more information: https://inl.gov/cytrics/

CyTRICS Program Overview

Standardized Repository and Reporting

Standardized Testing Process

Prioritization Methodology

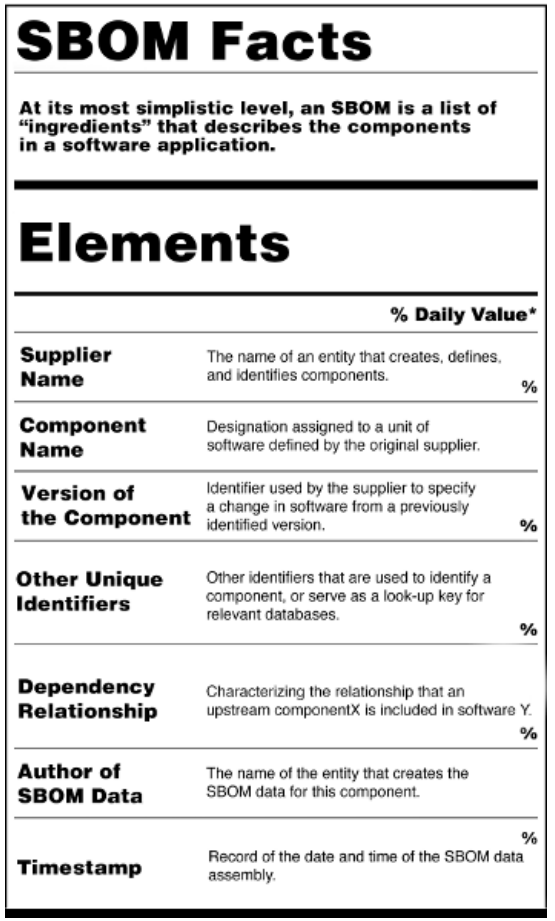


Multi-Laboratory Cooperation

Vendor Agreements

Energy Sector Software Bill of Materials Proof of Concept (SBOM POC)

- Started at NTIA, now a partnership between DOE CESER and DHS CISA
  - Broad and open participation
- S4x23 SBOM challenge: Five participants, three artifacts, three tasks
  - No “one tool to rule them all”
  - Firmware-based device enumeration is far less mature than software enumeration
  - VEX
  - Significant maturation year over year
- For more information: https://sbom.inl.gov/



SBOM Facts

At its most simplistic level, an SBOM is a list of “ingredients” that describes the components in a software application.

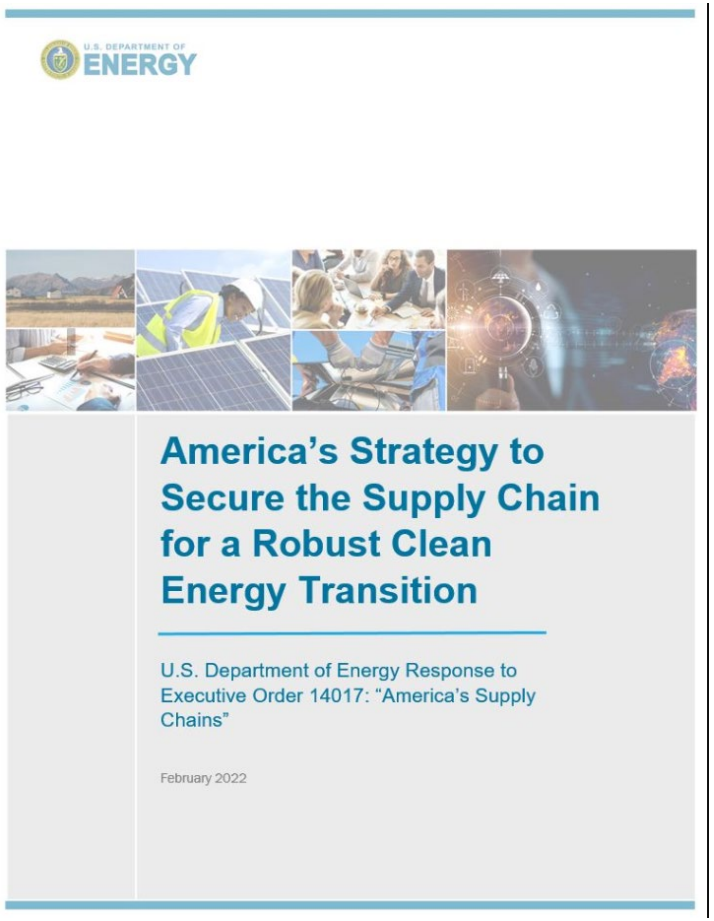
Elements

		% Daily Value*
Supplier Name	The name of an entity that creates, defines, and identifies components.	%
Component Name	Designation assigned to a unit of software defined by the original supplier.	
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.	%
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.	%
Dependency Relationship	Characterizing the relationship that an upstream componentX is included in software Y.	%
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.	
Timestamp	Record of the date and time of the SBOM data assembly.	%

https://soos.io/sbom-101-what-is-an-sbom-why-are-they-important

EO 14017 and Energy Cyber Sense

- Executive Order 14017 directives to strengthen the resilience of America's supply chains
  - DOE strategy, 13 topical reports
- Bipartisan Infrastructure Law Section 40122 requires DOE to "establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system, and for other purposes."
  - Testing
  - Vulnerability reporting and tracking
  - Technical assistance
  - Guidance



Questions and Discussion

Sam Chanoski
Technical Relationship Manager | Cybercore Integration Center
samuel.chanoski@inl.gov | 404-904-2480
Idaho National Laboratory | Atlanta, GA

Idaho National Laboratory

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FERC Order Directing Internal Network Security Monitoring (INSM)

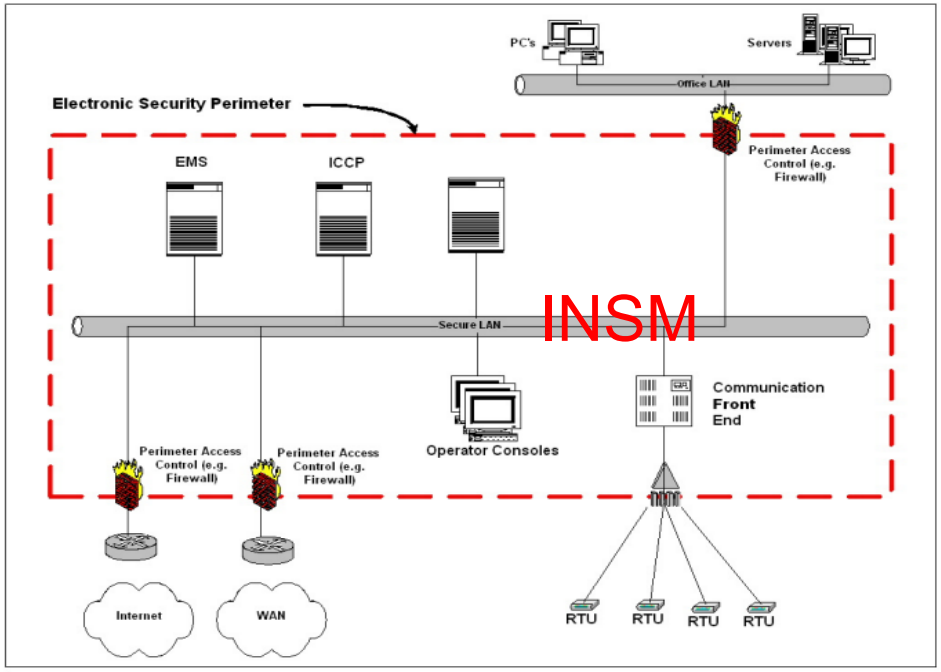
Michaelson Buchanan, Senior CIP Compliance Assurance Advisor
March 2023 Security Group Summit

RELIABILITY | RESILIENCE | SECURITY



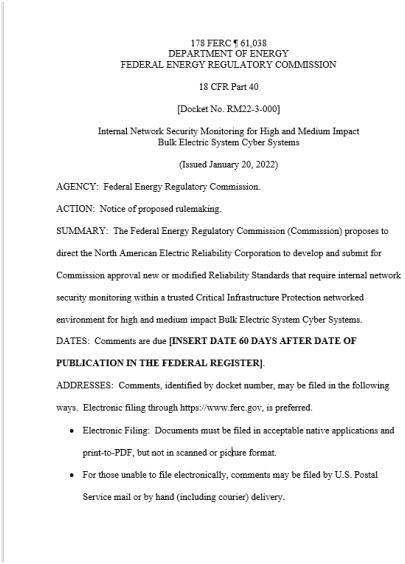

What is Internal Network Security Monitoring?

- INSM is a subset of network security monitoring that is applied within a “trust zone”
- Enables continuing visibility of communications between networked devices within a trust zone and detection of malicious activity that has circumvented perimeter controls



Notice of Proposed Rulemaking

- Commission issued INSM NOPR January 2022
- CIP networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack
- NOPR Proposed requiring INSM within a trusted CIP networked environment for high and medium impact BES Cyber Systems



178 FERC ¶ 61,038
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM22-3-000]

Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems

(Issued January 20, 2022)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to direct the North American Electric Reliability Corporation to develop and submit for Commission approval new or modified Reliability Standards that require internal network security monitoring within a trusted Critical Infrastructure Protection networked environment for high and medium impact Bulk Electric System Cyber Systems.

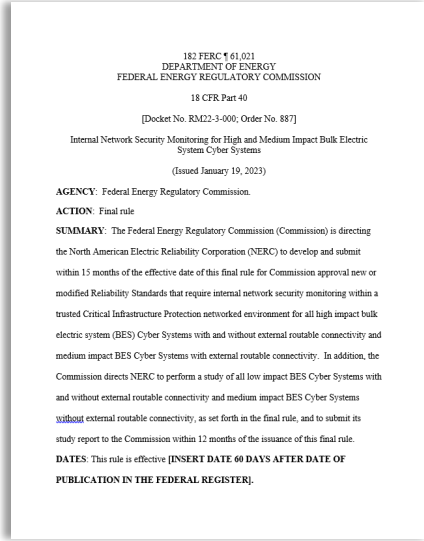
DATES: Comments are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Comments, identified by docket number, may be filed in the following ways. Electronic filing through https://www.ferc.gov, is preferred.

- Electronic Filing: Documents must be filed in acceptable native applications and print-to-PDF, but not in scanned or picture format.
- For those unable to file electronically, comments may be filed by U.S. Postal Service mail or by hand (including courier) delivery.

What does FERC Order 887 Require ?

- Two basic parts to the order:
  - Modify CIP Reliability Standards to require INSM for High Impact BES Cyber Systems with/without External Routable Connectivity (ERC) and Medium Impact BES Cyber Systems (BCS) with ERC
  - Submit a report that studies the feasibility of implementing INSM at all locations with low impact BCS and medium impact locations without ERC
    - Unmitigated risk of not implementing INSM
    - Challenges and solutions
- 15 months to complete Reliability Standards modifications
- 12 months to complete the feasibility study



182 FERC ¶ 61,021
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM22-3-000; Order No. 887]

Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems

(Issued January 19, 2023)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule

SUMMARY: The Federal Energy Regulatory Commission (Commission) is directing the North American Electric Reliability Corporation (NERC) to develop and submit within 15 months of the effective date of this final rule for Commission approval new or modified Reliability Standards that require internal network security monitoring within a trusted Critical Infrastructure Protection networked environment for all high impact bulk electric system (BES) Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity. In addition, the Commission directs NERC to perform a study of all low impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems without external routable connectivity, as set forth in the final rule, and to submit its study report to the Commission within 12 months of the issuance of this final rule.

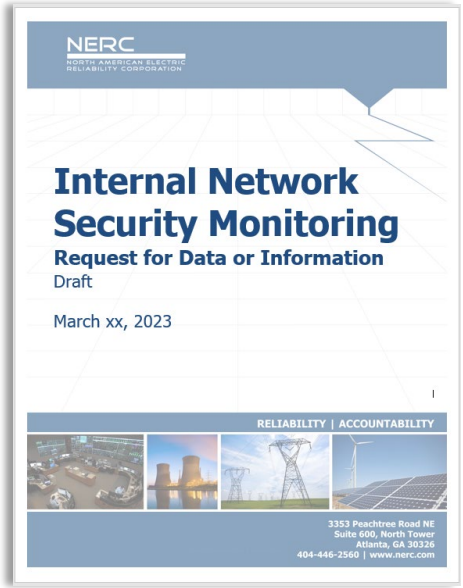
DATES: This rule is effective **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

CIP Reliability Standard Modifications

- New or modified Standards must be forward looking and objective based
- New or modified Standards must address three security objectives require entities to:
  - Develop baselines of their network traffic inside their CIP-networked environment
  - Monitor for and detect unauthorized activity, connections, devices, and software inside the CIP networked environment
  - Identify anomalous activity to a high level of confidence by:
    - Logging sufficient network traffic
    - Maintaining logs of network traffic
    - Implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices

INSM Feasibility Study

- Feasibility study must include:
  - Unmitigated risk of not implementing INSM
  - Challenges and solutions
- Order requires the collection of certain information in connection with the feasibility study
- Data request must include:
  - Count of Medium Impact locations with ERC
  - Count of Low Impact locations with ERC
  - Count of Low Impact locations without ERC
- Data requests will also include questions as necessary to identify risks, implementation challenges and potential solutions



INSM Feasibility Study- Data Request

- 21 day comment period, 60 days to respond
- Collection method
- Data Request Questions:
  - *Counts as required by FERC Order
  - *Network configurations for medium w/o ERC and low impact locations containing medium impact w/o ERC and low impact BES Cyber Systems
  - *Required - Rate technological and logistical challenges (e.g. Network redesign, compliance)
  - *Estimate low impact locations with IDS/IDP
  - Optional – Recommend alternative solutions to address risk
  - Optional – Existing INSM solutions deployed

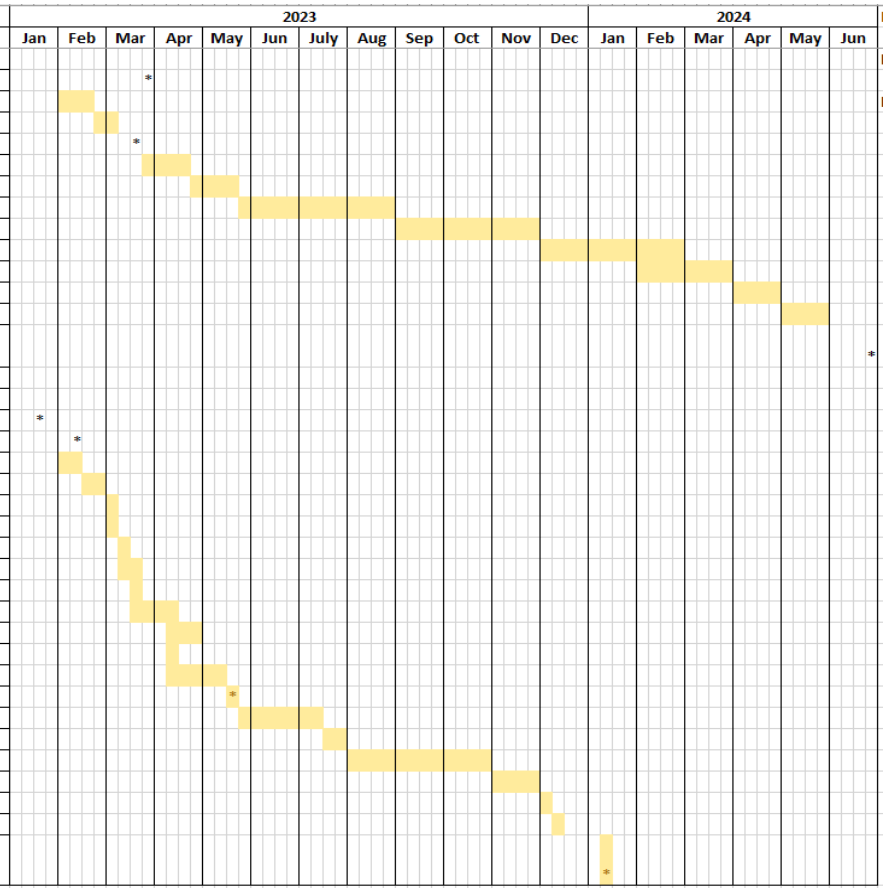
Current Activities/Project Risks

- Current Activities
  - FERC collaboration on data request draft
  - Reviewed data request with ERO participants
  - Standards Authorization Request (SAR) submitted and pending March approval by NERC Standards Committee
  - Final data request approved by FERC
  - Data request to be released for industry comment this week
- Project Risks / Challenges
  - Issuing a data request that is sufficient to complete the study
  - Mechanics of issuing and managing data request responses
  - Ensuring that the feasibility study considers all elements of risk

Resources and Timeline

- Resources
  - Core NERC team (Myself, Dan Goodlett, Larry Collier)
  - ERO Participants 1-2 from each region
- Timeline

Task	Date Due
INSM Standards Development	
Effective date (publication + 60 days)	3/31/23
Draft SAR	2/20/23
Review SAR	3/6/23
Standards Committee Approval	3/22/23
SAR Comment Period	4/21/23
drafting team nomination	5/19/23
Standards Development	8/31/23
Draft 1 ballot period	
Draft 2 ballot period	
Draft 3 ballot period	
Final ballot period	4/30/24
BoT approval	5/31/24
Submit standard to FERC (15 months from Effective Date)	6/28/24
INSM Feasibility Study	
INSM Feasibility Study Start Date (Issuance of Order)	1/19/23
BoT Approval for expedited proc	2/16/23
Develop Data Request	2/15/23
FERC Collaboration Period	2/22/23
ERO Review	3/7/23
Address ERO comments	3/9/23
Submit to FERC for 5 day preview	3/14/23
Prepare Comment Form	3/23/23
Industry Announcement & Comment form release	3/16/23
Data Request Industry comment period (21 Days)	4/13/23
Address Data Request comments	4/30/23
DR (Cover Letter) ready for BoT package	4/11/23
BoT Data Request Approval	5/11/23
Issue Data Request	5/17/23
Data Request Responses Due	7/17/23
Review DR Response and Develop Summary	8/3/23
Develop Feasibility Study	11/10/23
Review Feasibility Study	11/30/23
Report ready for BoT package	12/1/23
BoT Approval on Final Report	12/15/23
Submit INSM Study to FERC (12 months rom issuance of Order)	1/18/24



Questions?

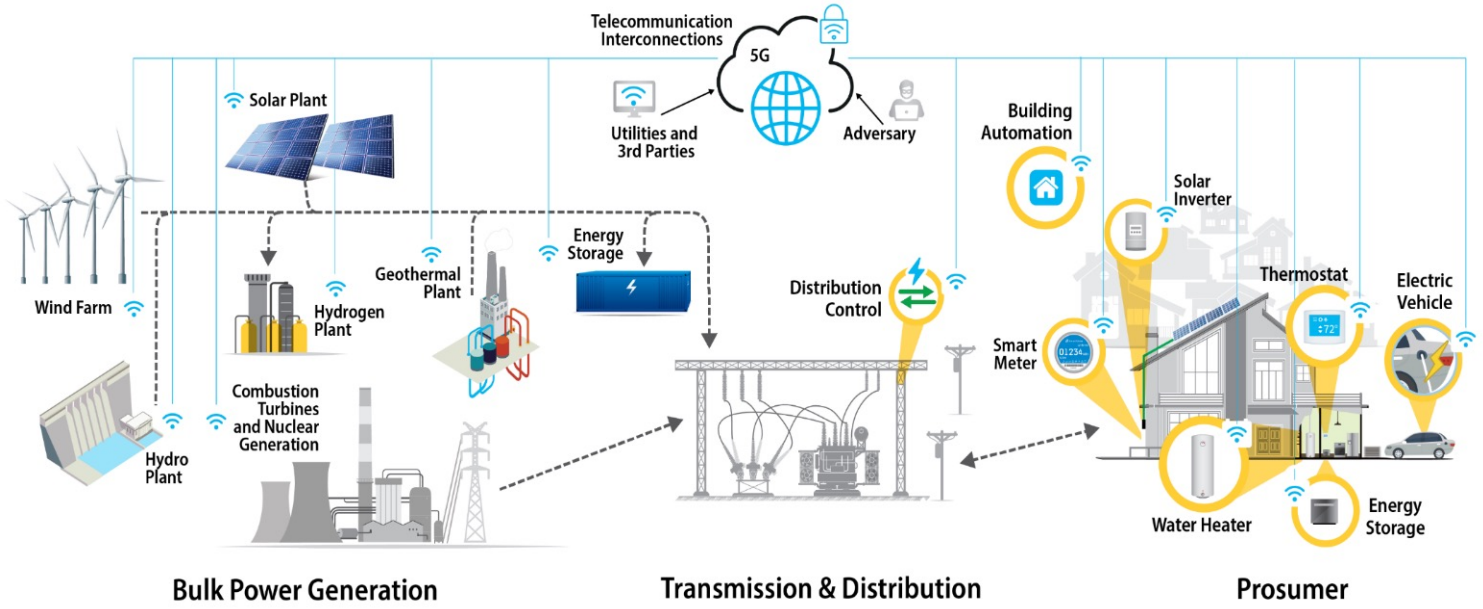
U.S. DEPARTMENT OF ENERGY

Office of
Cybersecurity, Energy Security, and Emergency Response

Report on Cybersecurity of Distribution Systems

The distribution of energy, communications, and risk in the year 2030

At the Edge of Energy Transformation



The power grid is changing to become more **distributed, intelligent, and complex**. As we adopt new technology for these emerging energy systems, cyber threats will evolve their capabilities to target and impact those energy systems. Action now is necessary to prepare for those threats.

Previous Studies

Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems, U.S. Government Accountability Office (2021)

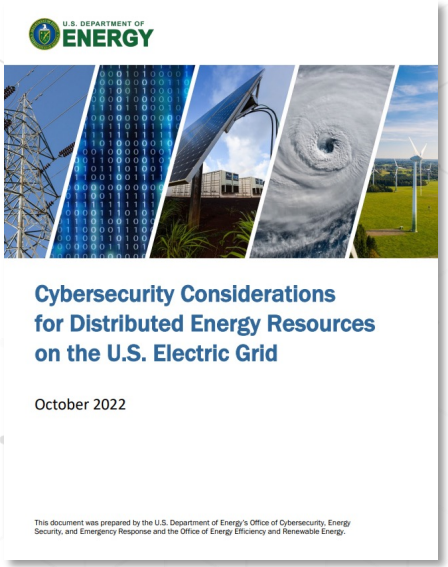
CESER Blueprint, U.S. Department of Energy (2021)

EERE Cybersecurity Multiyear Program Plan, United States Department of Energy (2021)

Roadmap for Wind Cybersecurity, United States Department of Energy (2020)

Certification Procedures for Data and Communications Security of Distributed Energy Resources, National Renewable Energy Laboratory (2019)

Roadmap for Photovoltaic Cyber Security, Sandia National Laboratories (2017)



Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid, United States Department of Energy (2022)

Report to Congress on Cybersecurity of Distribution Systems

In support of the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), **NREL is leading the Bipartisan Infrastructure Law Section 40121(c) *Report on Cybersecurity of Distribution Systems*.**

The report to Congress will assess:

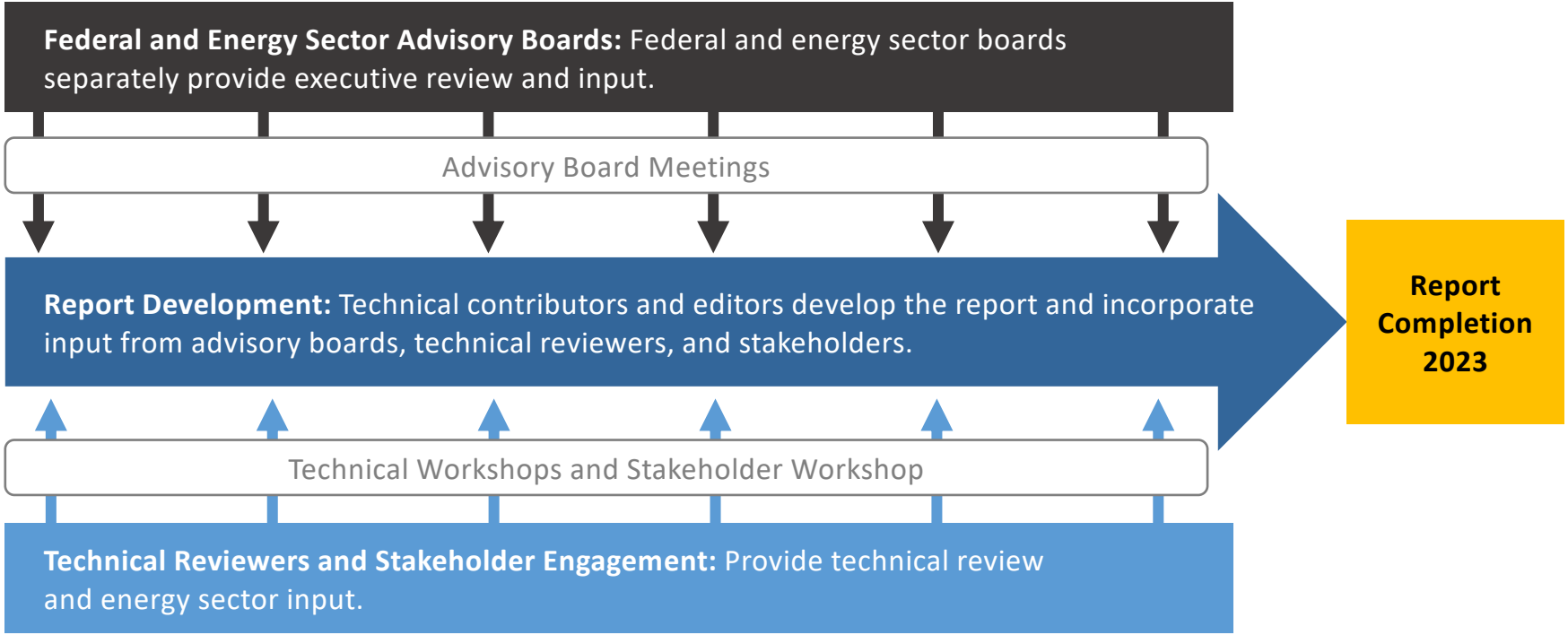
> "(1) priorities, policies, procedures, and actions for enhancing the physical security and cybersecurity of electricity distribution systems, including behind-the-meter generation, storage, and load management devices, to address threats to, and vulnerabilities of, electricity distribution systems; and
>
> (2) the implementation of the priorities, policies, procedures, and actions assessed under paragraph (1), including—
>
> (A) an estimate of potential costs and benefits of the implementation; and
>
> (B) an assessment of any public-private cost-sharing opportunities."

Team Objectives

In support of CESER's assigned "Report on Cybersecurity of Distribution Systems" from Sec. 40121(c) of the Infrastructure Investment and Jobs Act, the team will:

1. **Convene and gather input** from federal agencies, state regulatory authorities, and industry stakeholders
2. **Produce a report** on cybersecurity of distribution systems
3. **Support CESER in its briefings to leadership** with DOE and the U.S. Department of Homeland Security.

Project Development

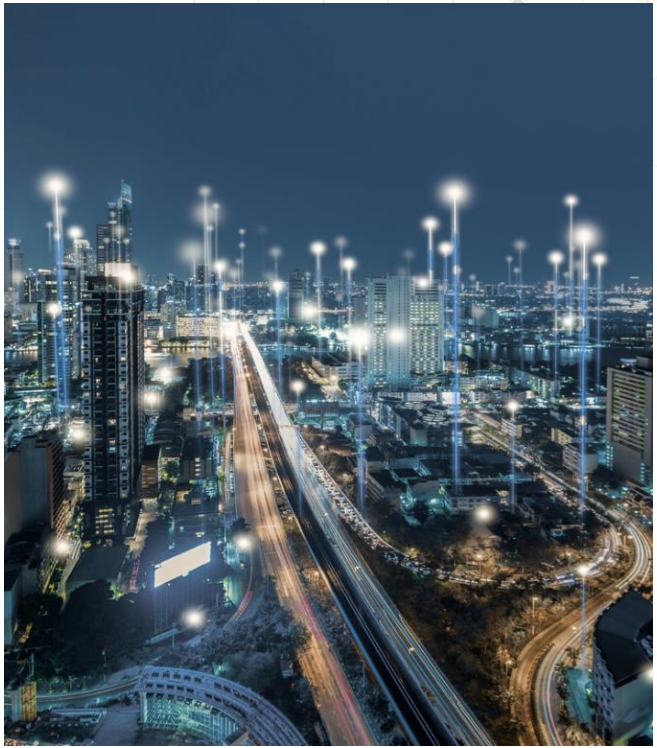


Scope of the Report

- **PRIMARY FOCUS:** Electrical distribution systems, with particular attention paid to future systems in 2030
- Aspects of cybersecurity that are unique to operational technology for distribution systems
- Physical security related to cyber assets.

Key Trends

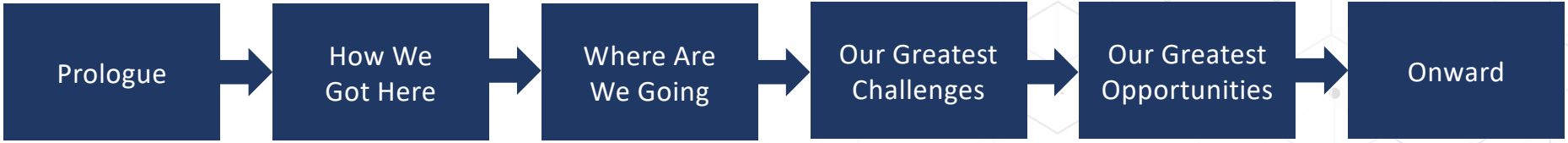
- Distribution system design and control, such as trends towards software-driven control and virtualization.
- Emerging technology such as virtual power plants, autonomous control strategies, advanced telecommunications, and microgrids.
- Interdependence of infrastructure sectors (e.g., water, transportation, energy, and communications).



Technical Contributors

PURPOSE Led by NREL, technical contributors are responsible for gathering relevant supporting material, performing analysis, authoring the report, incorporating feedback from the Federal Sponsor Committee and stakeholders, and revising content.

Current Narrative



Short anecdote illustrating the current state of the distribution system, the stakeholders, and the grand challenges we face

"A Distribution System": A history of the distribution system leading up to today and the current state of cybersecurity

"An Integration System": Where the distribution system is going, including trends and why cybersecurity is increasingly important to reliability

An analysis of our greatest cybersecurity challenges facing the electric distribution system

How we transform our challenges into opportunities in the form of policies, procedures, and actions

What the priorities based on costs/ benefits and identified public-private partnerships

Connect with Us!

energysrma@hq.doe.gov

Joseph.Quinn1@hq.doe.gov

Jonathan.White@nrel.gov

Jordan.Henry@nrel.gov

Software Supply Chain Cybersecurity of DERs

Ryan Cryar, Danish Saleem

NERC Reliability and Security Technical Committee Meeting

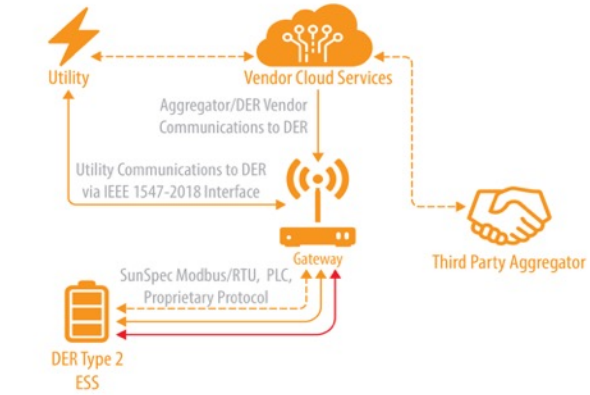
03/23/2022

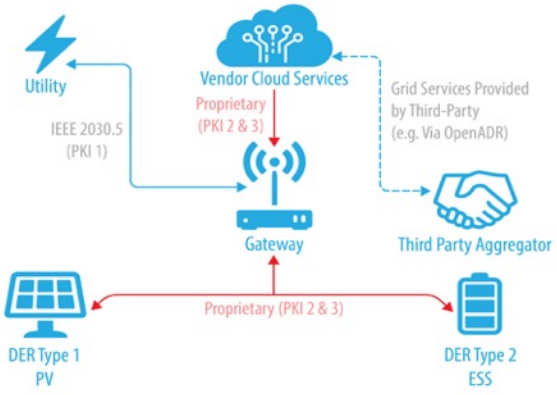
Why Care About DER Software Supply Chains?

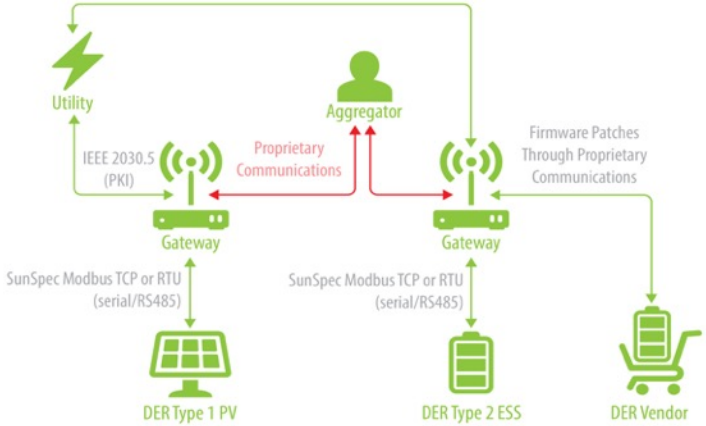
How DERs are increasingly consequential to grid reliability and why the DER supply chain problem is unique

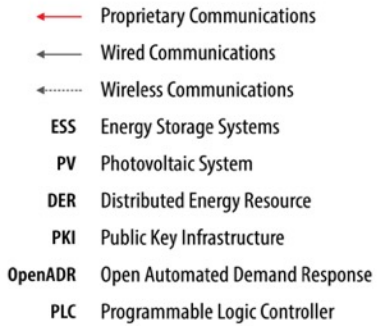
The Impact of DERs

- DERs increasingly supporting grid operating services
- More stakeholders exchanging more information
- Perimeter security becoming more tenuous
- Less tractable supply chains









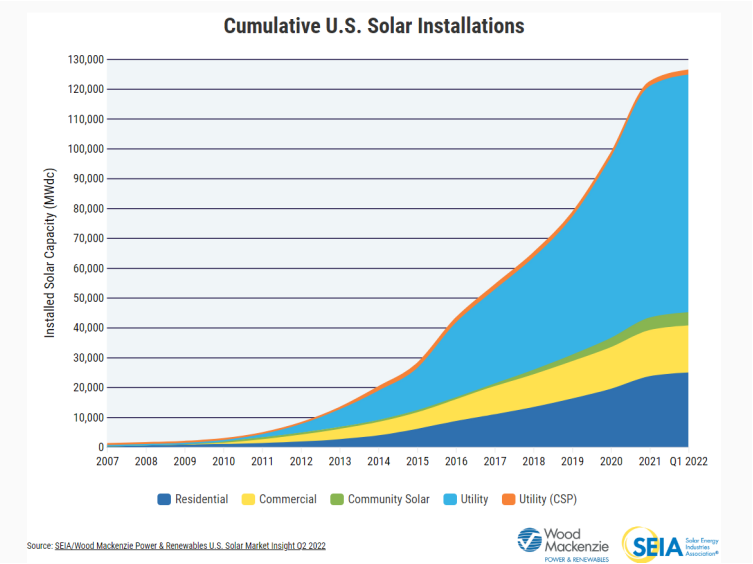
Graphic by NREL

Renewable Generation is Growing Rapidly

Solar data snapshot (June 2022)

Installed Solar Capacity	126 GWdc
Number of Solar Systems	3.5 million
Distributed PV (including rooftop and community solar)	~40%
Price decline in last 10 years	60%
Annual Growth in last 10 years	33%
Fraction of Electricity Generation	4%
Fraction of Electricity Generation in 2035* (projected)	40%

** DOE SETO "Solar Futures Study," September 2021*



What are the DER supply chain risks?

Software supply chain is an increasingly intractable attack vector for sector stakeholders to manage.

How do we quantify the risk?

Who owns the risk?

How to we manage the risk?

How are the risks unique?

What is the shared responsibility?

Software Supply Chain Challenges

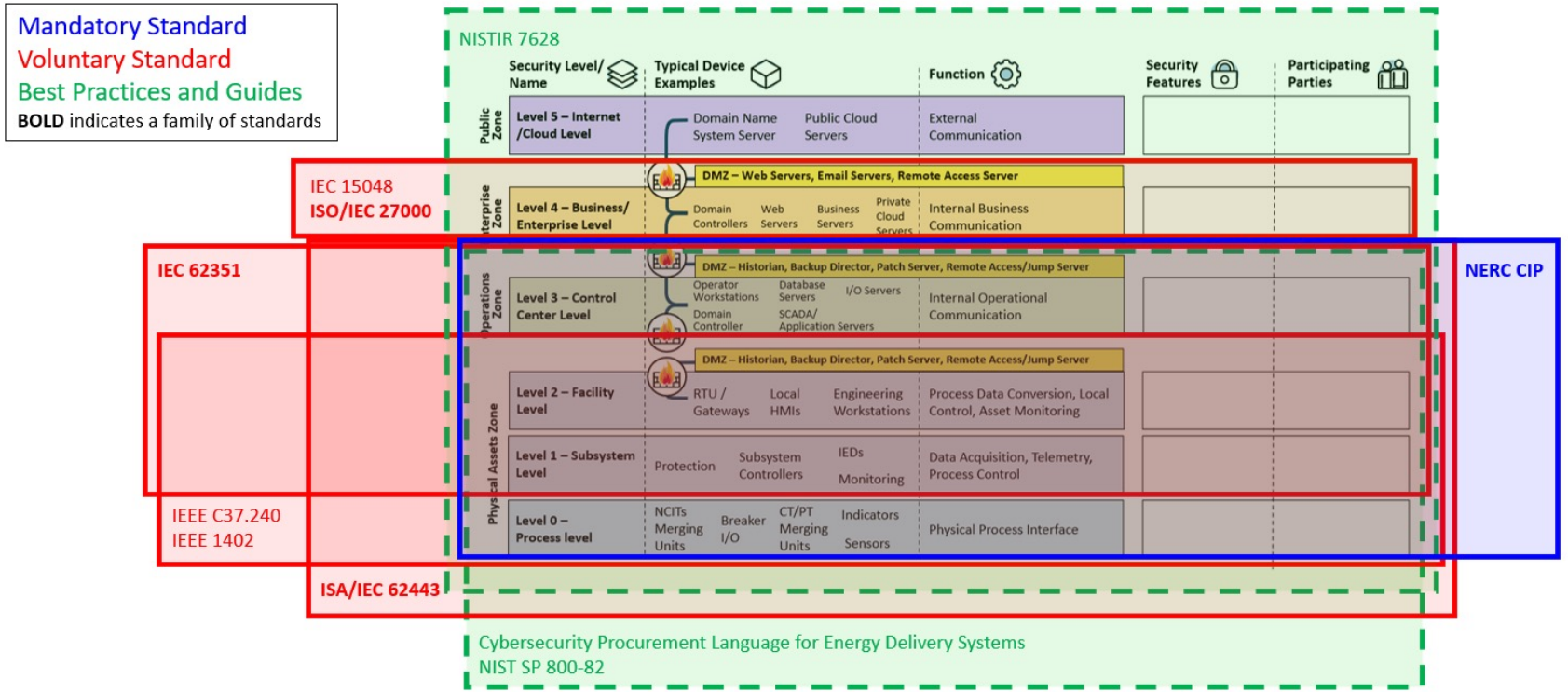
- **Open-source** software is a growing area in energy systems software development
- **Vulnerabilities** in downstream dependencies pose risks to systems using bloated, aging software packages
- **Risk management** of the vulnerabilities require deep analysis and reducing dependencies on the vulnerable package

CyTRICS and **CECA** evaluating software supply chain risks.

The Role of Standards and Certifications

The gaps in standards, certifications, and best practice guides for DER software supply chain

Cacophony of Standards



"Reference Architectures as a Means of Influencing Electric Energy Operational Technology/Industrial Control Systems Security Outcomes" - SEI ETF

Cybersecurity Certification Standard

- The requirements will provide a single unified approach for testing and certification of DERs *in advance* of deployment.
- The certification will be applicable to generation and energy storage technologies.
- UL and NREL are actively developing the outline of investigation.
- We will welcome participation from industry.

A national or international cybersecurity certification standard can aid industry stakeholders to evaluate and validate the cybersecurity posture of their DER or IBR devices before they are connected to the electric grid.

https://www.nrel.gov/security-resilience/cybersecurity-standards.html

PRESS RELEASE

UL and NREL Announce Cybersecurity Testing Recommendations for Distributed Energy Resources and Inverter Based Resources

UL and the National Renewable Energy Laboratory will complete an Outline of Investigation as a precursor to the first cybersecurity certification standard for distributed energy resources.

Home > News > UL and NREL Announce Cybersecurity Testing Recommendations for Distributed Energy Resources and Inverter Based Resources

March 7, 2022

NORTHBROOK, Illinois – March 7, 2022 – UL, a global safety science leader, has released a report, co-authored with the U.S. Department of Energy's (DOE's) National Renewable Energy Laboratory (NREL), titled "Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources." The report includes recommendations that enable distributed energy resources (DER) and inverter based resources (IBRs) to maintain a strong cybersecurity posture.

With support from DOE's Solar Energy Technologies Office, UL will continue working with NREL on developing requirements to support cybersecurity certification standards for DERs and IBRs. NREL and UL are currently working on an Outline of Investigation for a standard that will apply to energy storage and generation technologies on the distribution grid, including photovoltaic inverters, electric vehicle chargers, wind turbines, fuel cells and other resources essential to advancing grid operations. These new requirements will prioritize cybersecurity enhancements for power systems dealing with high penetration inverter-based resources, including those interfacing with bulk power systems for periods of instantaneous high wind, solar and hybrid/storage generation. It will also help ensure cybersecurity is designed into new IBR and DER systems.

"Currently, there are no cybersecurity certification requirements to which manufacturers and vendors can certify their DER and IBR devices against an established and widely adopted cybersecurity certification program. The development of these new cybersecurity certification requirements will provide a single unified approach that can be taken as a reference for performing the testing and certification of DERs before being deployed and while in the field," said Kenneth Boyce, senior director for Principal Engineering, Industrial, group at UL. "Drafting comprehensive certification requirements with peer review requires effective leadership and stakeholder participation. We are pleased to be working with NREL in this effort to bring additional performance-based security to electrical grid infrastructure."

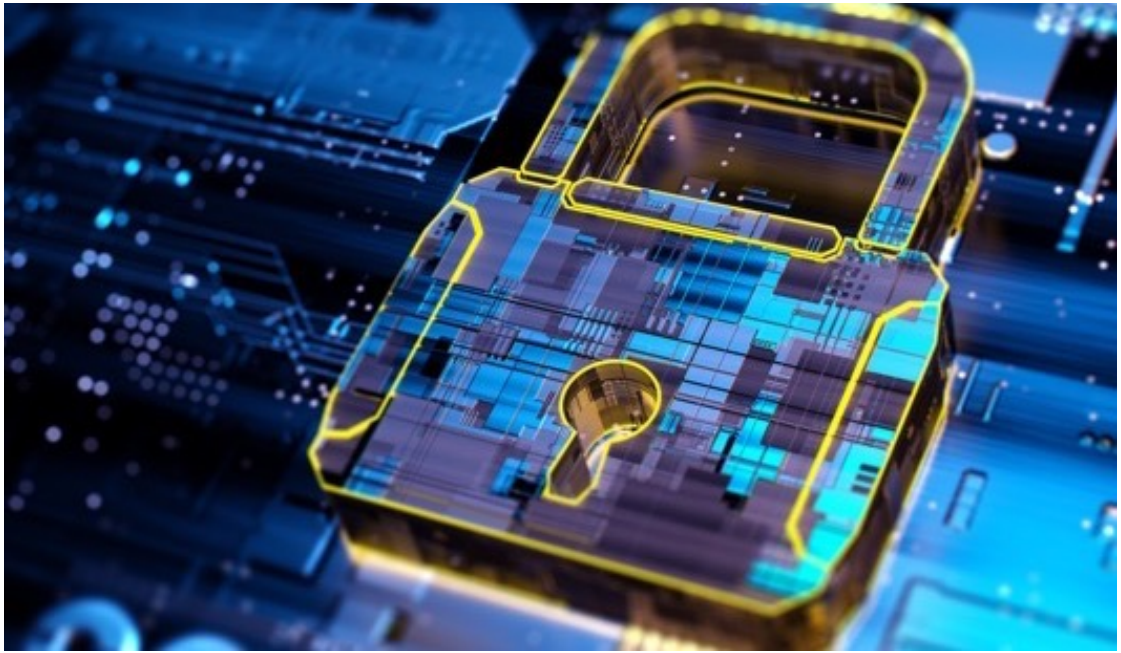


Photo from iStock, 1185245180

Benefits of a Cybersecurity Certification Standard

- Ensures DER devices have all five pillars of cybersecurity: confidentiality, integrity, availability, authentication and non-repudiation
- Supports federal and state mandates
- Incentivizes security by design in new DER systems
- Creates an environment where the baseline security posture of the DER industry will be elevated

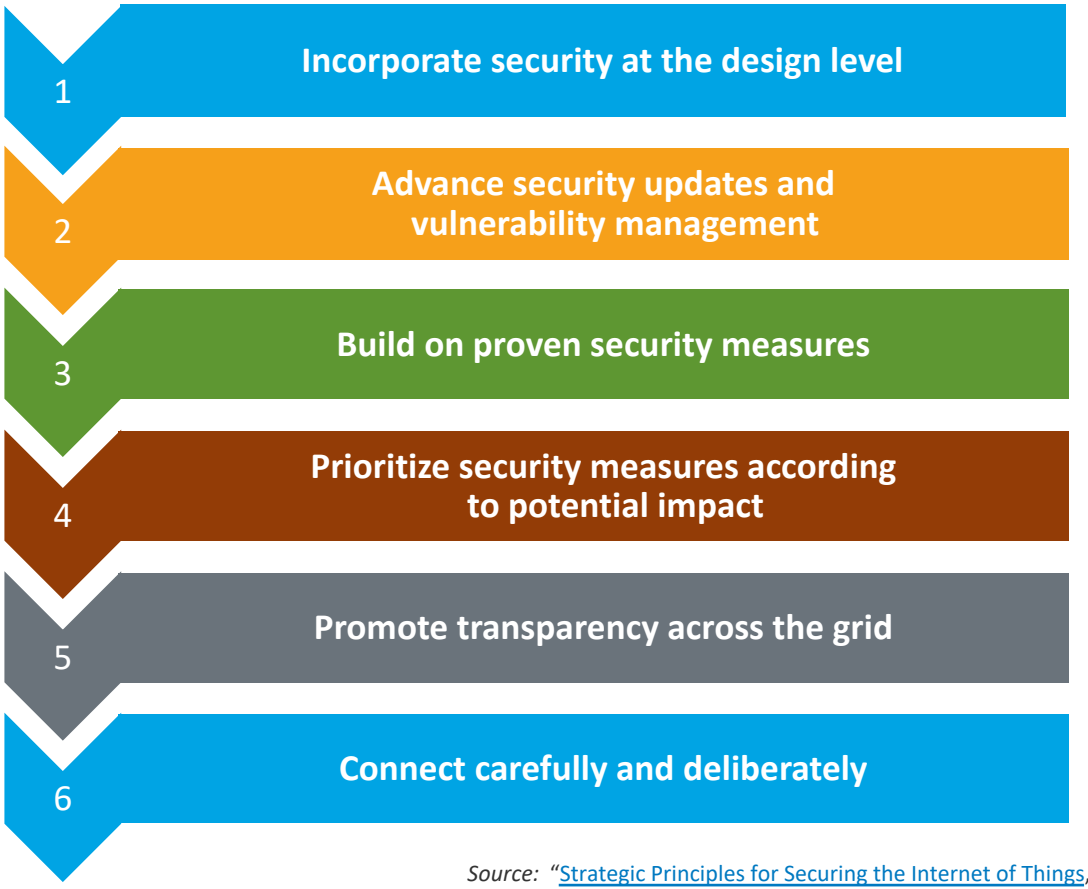
Where Do We Go From Here?

A focus on cyber resilience

Get The Basics Right

Implement **security-by-design** and practice basic **cyber hygiene**

- Change DER default passwords
- Know what's on your network (devices and connections)
- Whenever possible, enable MFA
- Install critical updates, i.e., authentication, TLS 1.2 or higher, etc.
- Monitor both consumer devices and vendor-managed devices
- If possible, add code-signing and roll-back firmware
- Use vendors who include cyber features
- Promote a cyber aware workforce and culture
- Have (and practice) an incident response plan



Source: "Strategic Principles for Securing the Internet of Things," U.S. Department of Homeland Security (2016)

Road Map of Next Steps

- Establishing “Security by Design” through frameworks and standardization
- Further partnership between industry and government entities
- Establishing open-source software guidance for energy systems
- Testing ecosystems for supply chain
- Prioritize based on system risks
- More focus on response and recovery from supply chain compromise

Thank You!

Let’s Work together!

Danish.Saleem@nrel.gov

Ryan.Cryar@nrel.gov

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Physical Security Insights

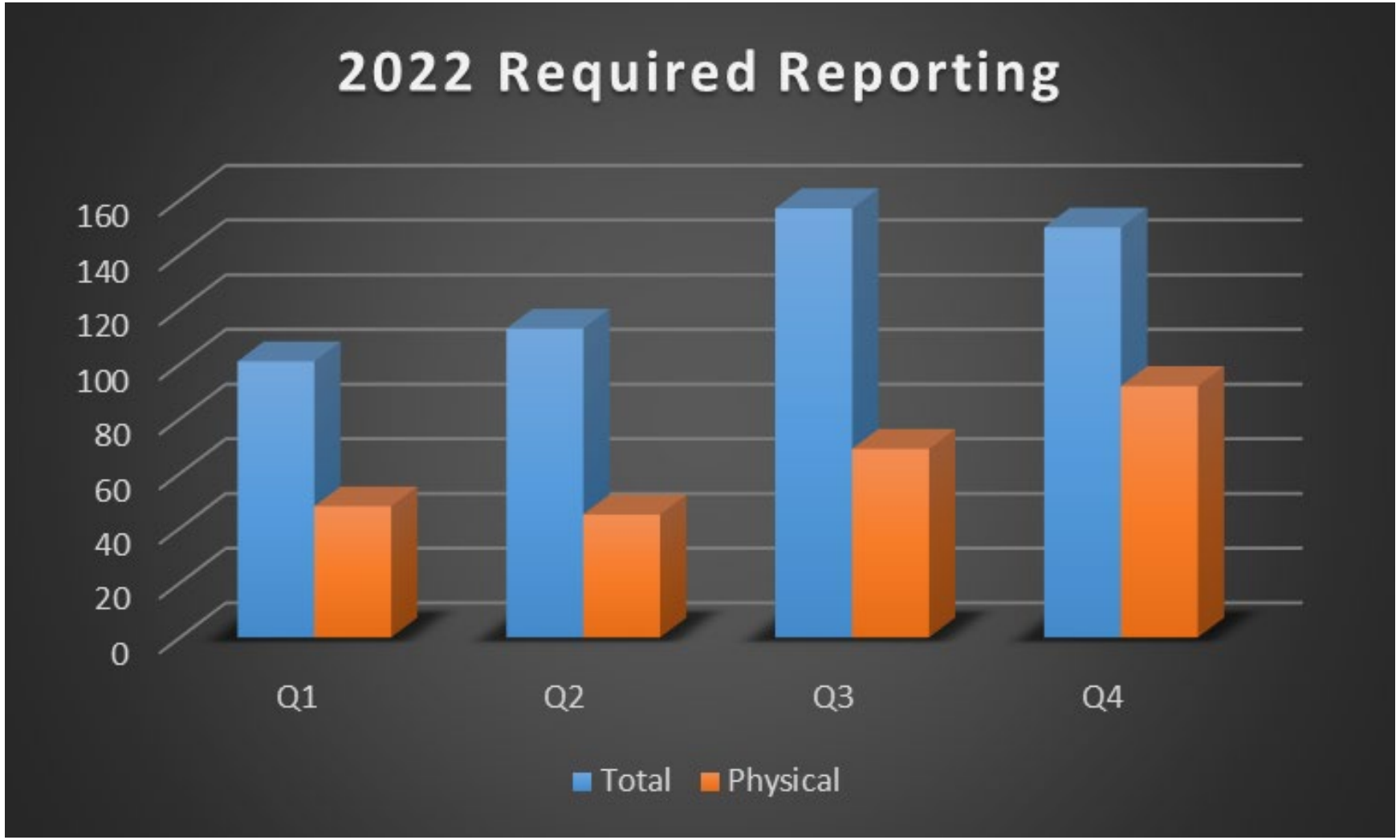
NERC Bulk Power System Awareness (BPSA)

Tony Burt, BPSA Physical Security Analyst
Security Group Summit
March 23, 2023

RELIABILITY | RESILIENCE | SECURITY




2022 Required Reporting



Questions and Answers