

CIP LOW IMPACT FROM THE GROUND UP

August 19th, 2025

CIP Low Impact Workshop

RF Offices, Independence, OH



MEET THE PRESENTERS



David Sopata

Principal Reliability
Consultant, Entity
Engagement, RF



Ron Ross

Principal Reliability
Consultant, Entity
Engagement, RF



Lew Folkerth

Principal Reliability
Consultant, Entity
Engagement, RF



Chris Holmquest

Senior Reliability and
Security Advisor, Outreach
and Training, SERC

PART 1 8:15-10:00

INTRODUCTION TO NERC AND THE
RELIABILITY STANDARDS - LEW

INTRODUCTION TO THE LOW IMPACT
STANDARDS - CHRIS

OVERVIEW OF COMPLIANCE STEPS - DAVE

IDENTIFYING YOUR CIP SENIOR MANAGER
(CIP-003 R3, R4) - RON

PART 2 10:15- 12:00

IDENTIFYING BES ASSETS CONTAINING LOW
IMPACT BCS (CIP-002) - RON

GOVERNANCE AND POLICY (LOW IMPACT
ONLY) - CHRIS

PART 3 1:00-2:30

DEVELOPING YOUR LOW IMPACT CYBER
SECURITY PLANS - LEW/RON

PART 4 2:45-4:45

CIP-012 - DAVE

CIP-014 - CHRIS

FUTURE STATE - -10,-11,-12, CATEGORY 2 -
CHRIS

QUALITY EVIDENCE/RSAW/ERT - LEW

CLOUD - LEW

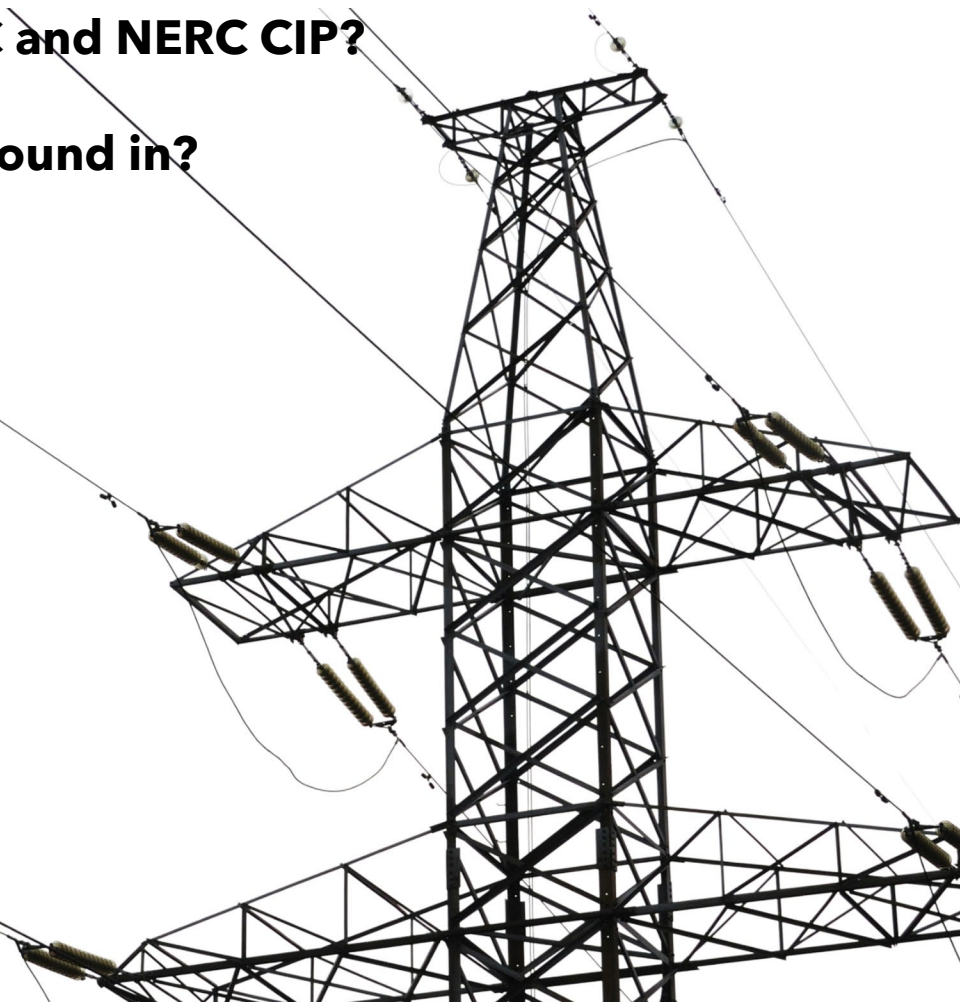
WRAP-UP - REFERENCES, WEBINARS



Slido Questions!!!

- **What is your Role within the Organization?**
- **How "New" are you to NERC and NERC CIP?**
- **What is your primary background in?**

Join at
slido.com
#2071 9698
Passcode:
tzy1n4



PART 1 8:15-10:00


INTRODUCTION TO NERC AND THE RELIABILITY STANDARDS - LEW

INTRODUCTION TO THE LOW IMPACT
STANDARDS - CHRIS

OVERVIEW OF COMPLIANCE STEPS - DAVE

IDENTIFYING YOUR CIP SENIOR MANAGER
(CIP-003 R3, R4) - RON

INTRODUCTION TO NERC AND THE RELIABILITY STANDARDS

- 
- Guiding entities through NERC CIP Standards for low impact BES Cyber Systems.
 - Emphasis on practical advice and discussion—not binding interpretations.
 - We cannot tell you how to be compliant.



1965
Northeast
Blackout

Electric Utilities

Regional
Reliability
Councils

1968

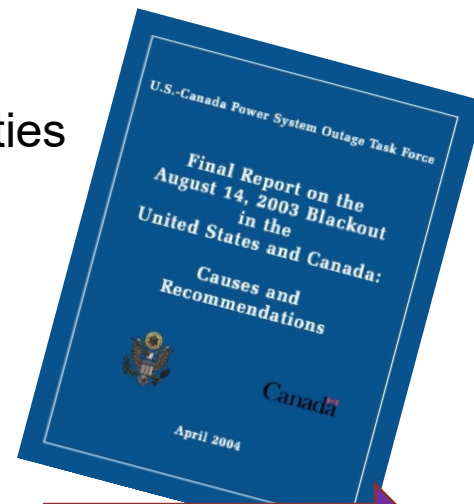
Voluntary
Reliability
Standards

Canadian
Participation
Recognized

Electric Utilities

Regional
Reliability
Councils

1981



2003
Blackout

National Electric Reliability Council

NERC

North American Electric Reliability Council

NERC

1965-2003

Energy
Policy Act
of 2005



Federal Energy Regulatory Commission (FERC)

2007 Electric Reliability Organization (ERO)



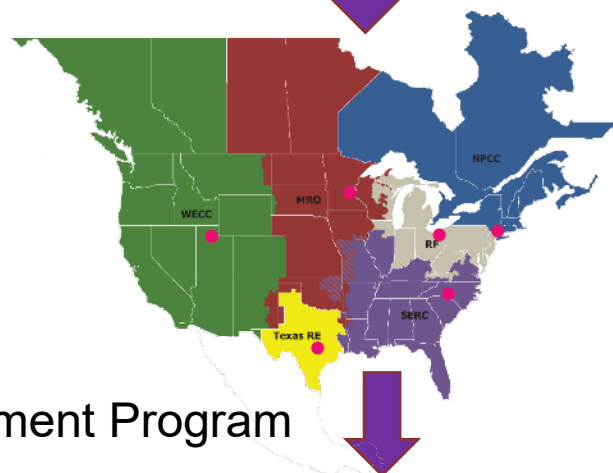
North American Electric Reliability Corporation

NERC

Regional Delegation Agreements



Regional
Entities



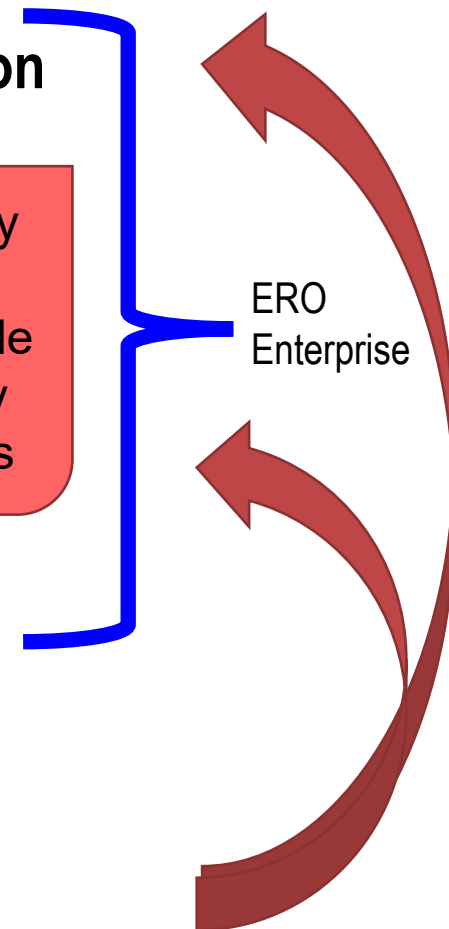
Compliance Monitoring and Enforcement Program



Electric Utilities

Mandatory
and
Enforceable
Reliability
Standards

ERO
Enterprise



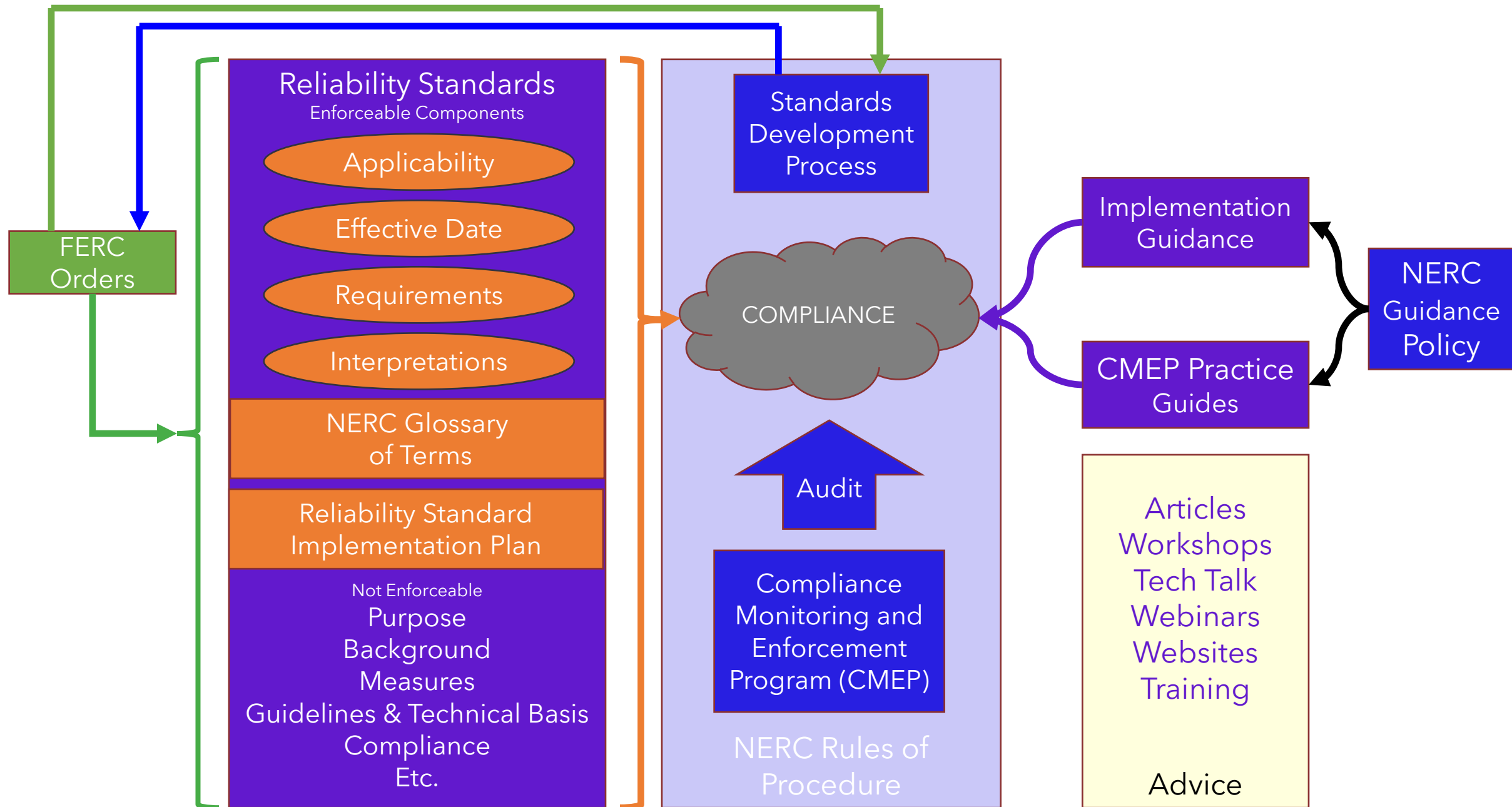
Present

STANDARD FAMILIES

Topic Area	Acronym	Topic Area	Acronym
Resource and Demand Balancing	BAL	Modeling, Data, and Analysis	MOD
Critical Infrastructure Protection	CIP	Nuclear	NUC
Communications	COM	Personnel Performance, Training, and Qualifications	PER
Emergency Preparedness and Operations	EOP	Protection and Control	PRC
Facilities Design, Connections and Maintenance	FAC	Transmission Operations	TOP
Interchange Scheduling and Coordination	INT	Transmission Planning	TPL
Interconnection Reliability Operations and Coordination	IRO	Voltage and Reactive	VAR

Operations & Planning (O&P or 693) Standards

CIP (706) Standards



Reliability Standards Document Relationships

NERC CIP STANDARDS (THE SECURITY PROTECTIONS)

CIP-002: Cyber Asset and Cyber System Categorization

CIP-003: Security Management Controls

CIP-004: Personnel and Training

CIP-005: Electronic Security Perimeters

CIP-006: Physical Security of Cyber Systems

CIP-007: Systems Security Management

CIP-008: Incident Reporting and Response Planning

CIP-009: Recovery Plans for Cyber Assets and Systems

CIP-010: Configuration Management and Vulnerability Assessments

CIP-011: Information Protection

CIP-012: Communications between Control Centers

CIP-013: Supply Chain Risk Management

CIP-014: Physical Security (Critical substations and associated Control Centers)

CIP-015: Internal Network Security Monitoring

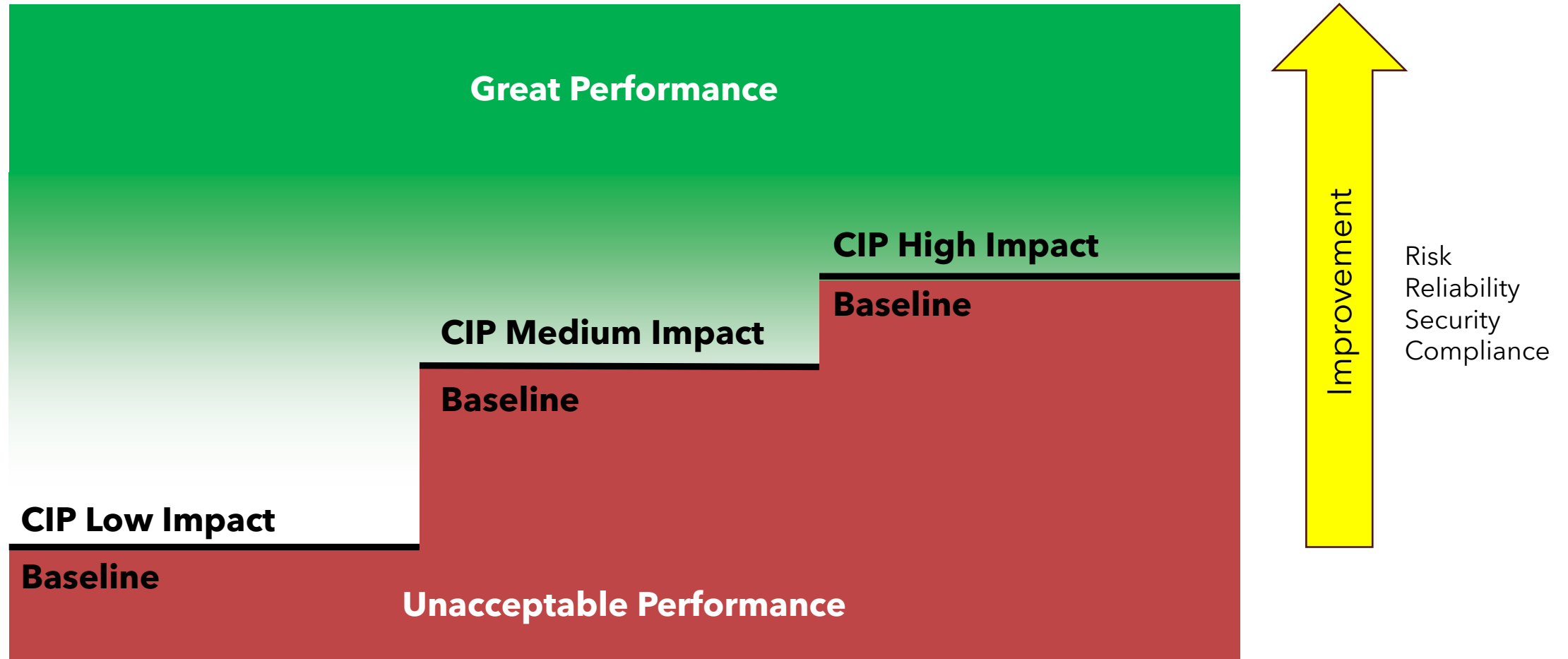


They are the only “**mandatory and enforceable**” cyber security standards and are the only explicitly OT cyber security standards publicly available.

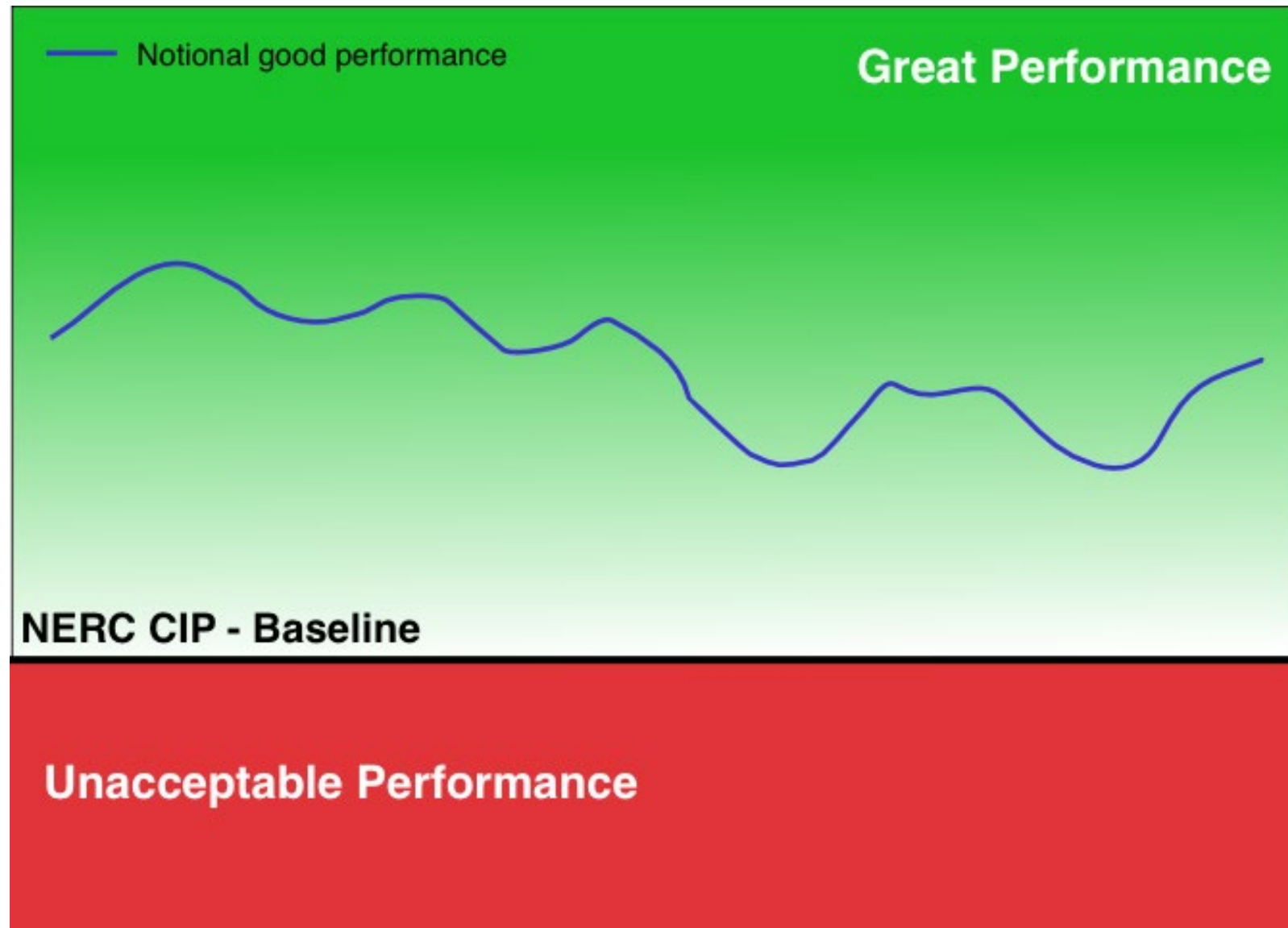
The NERC CIP Standards establish a **minimum-security framework** that must be implemented for all applicable Bulk Electric System Cyber Assets.

FOUNDATIONAL VS. ASPIRATIONAL

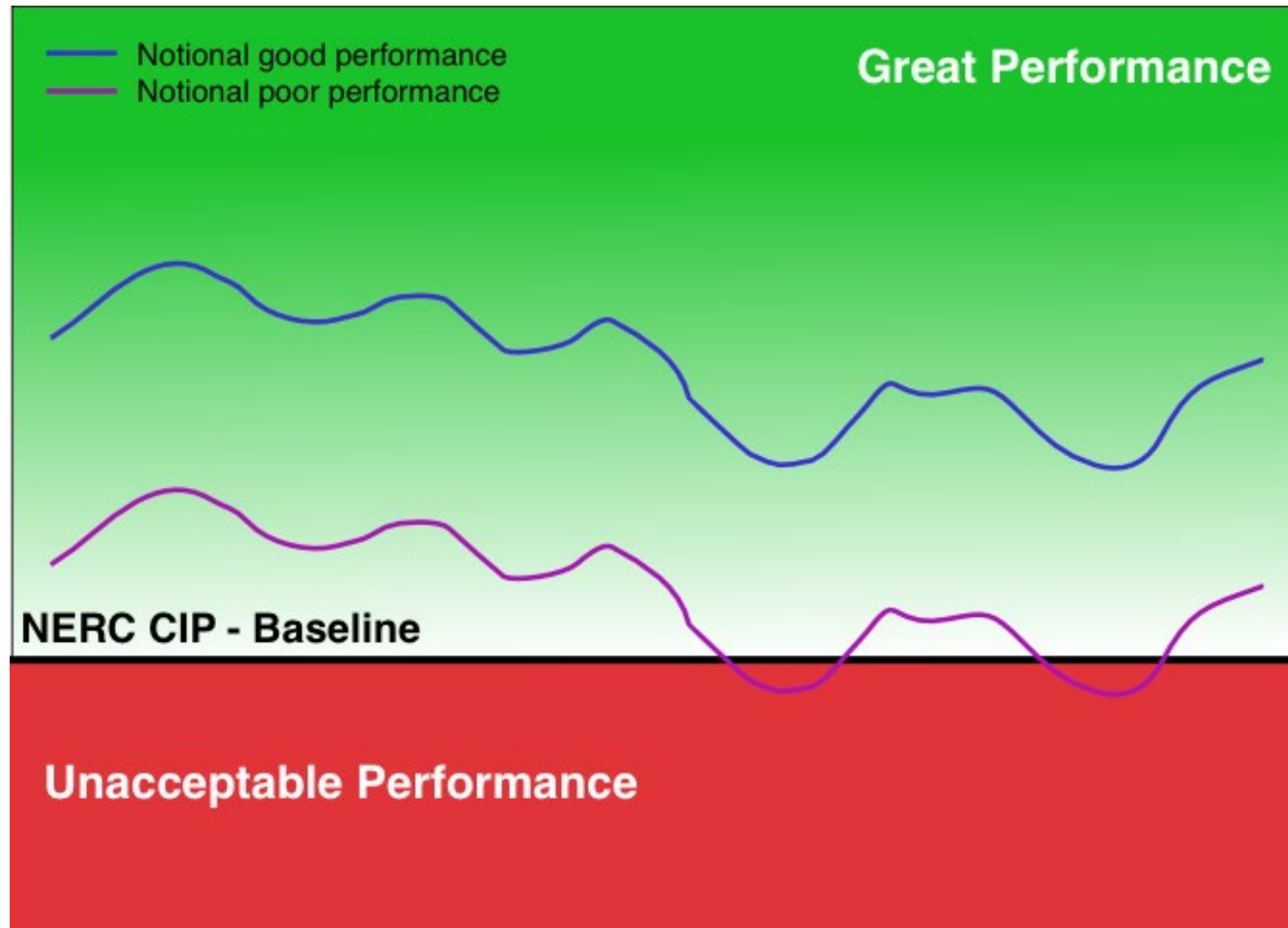
NIST CSF, NIST 800-53, IEC 62443, etc.



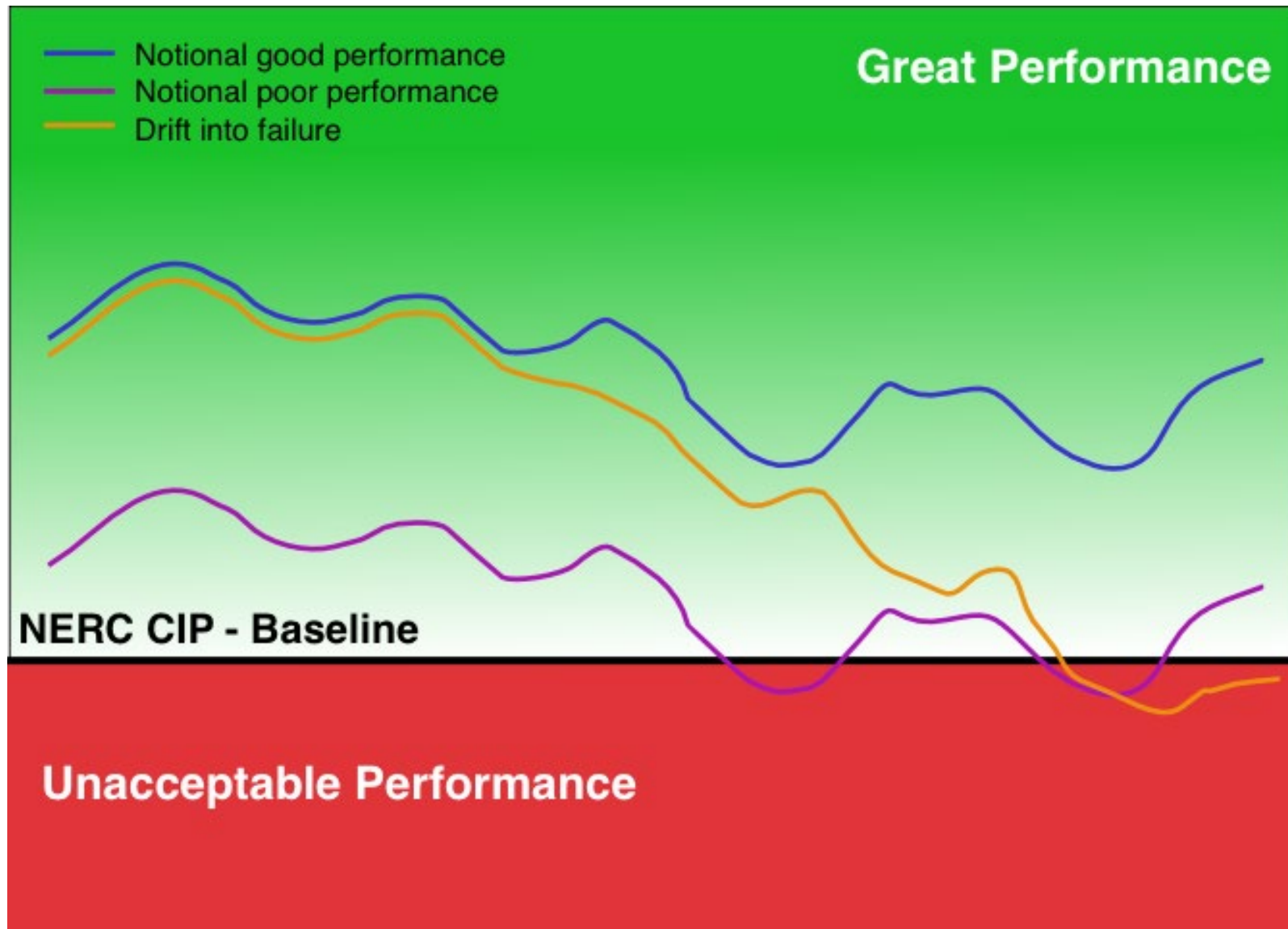
GOOD PERFORMANCE



POOR PERFORMANCE



DRIFT INTO FAILURE

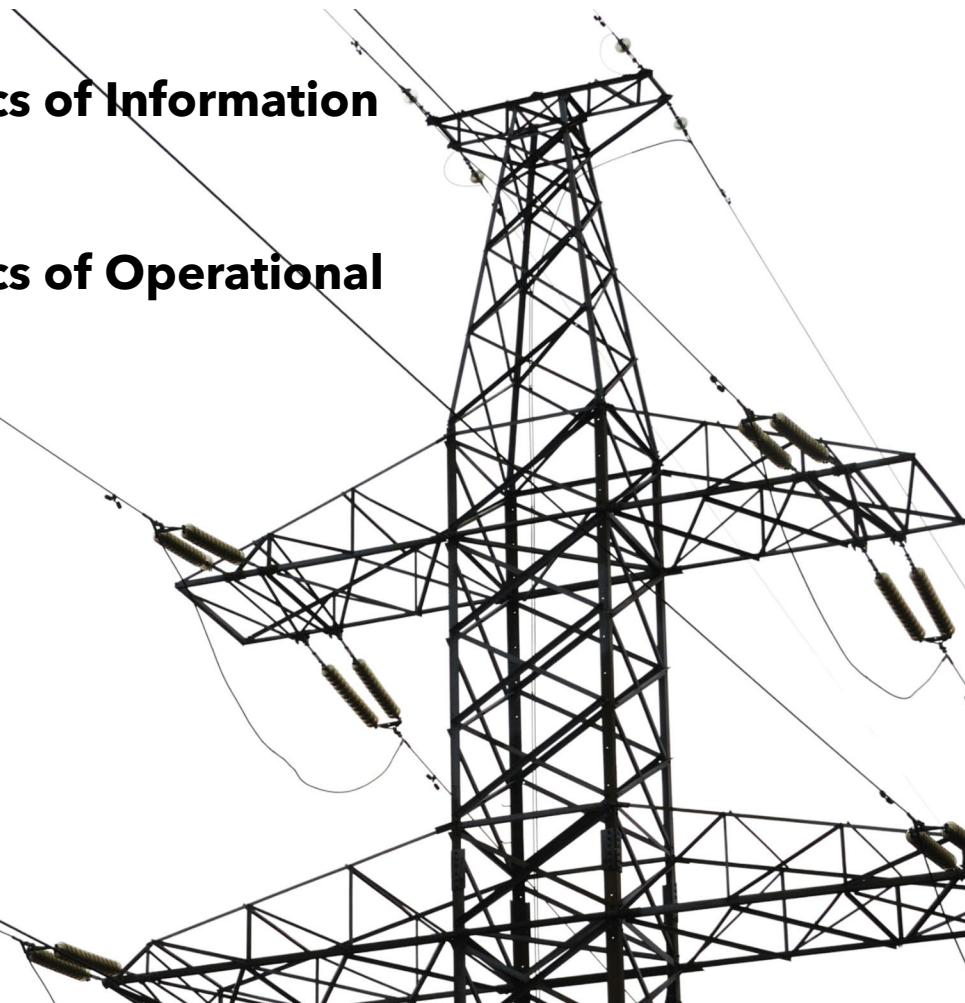




Slido Questions!!!

- **What are the skillsets you are looking for in an OT/IT professional?**
- **What are some characteristics of Information Technology?**
- **What are some characteristics of Operational Technology?**

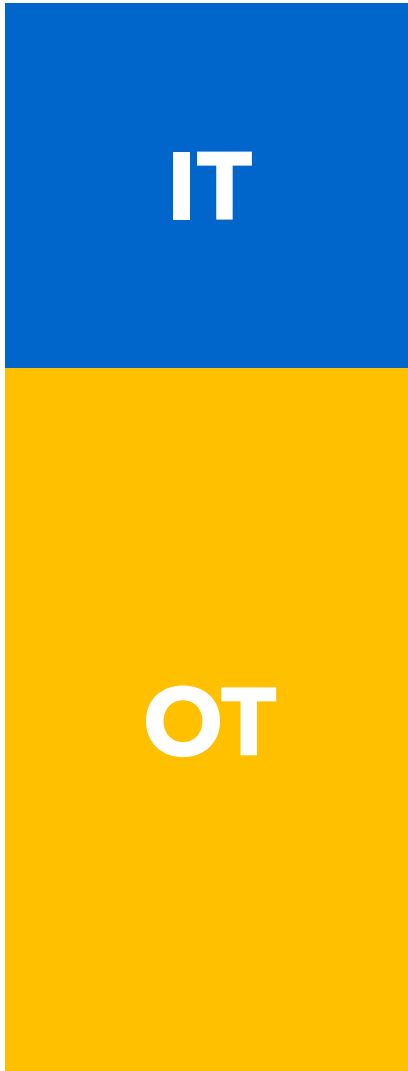
Join at
slido.com
#2071 9698
Passcode:
tzy1n4



DIFFERENCES BETWEEN IT AND OT

Information Technology (IT)	Operational Technology (OT)
Information	Control
Less sensitive to availability	Very sensitive to availability
Dynamic environment	Static environment
Shorter technology lifecycle	Longer technology lifecycle
Software errors are normal	Software errors can kill people
Human errors are routine	Human errors can kill people

WHAT IS OPERATIONAL TECHNOLOGY (OT)? (PURDUE MODEL)



- **Level 5 - Internet-facing systems**
 - Email servers, web servers
- **Level 4 - Enterprise/business systems**
 - Email client, web browser, word processing, spreadsheets
- **Level 3 - Operations systems**
 - Historian
- **Level 2 - Supervisory control**
 - SCADA, DCS, HMI
- **Level 1 - Control systems**
 - Milliseconds - Relays, RTUs, PLCs, Safety systems
- **Level 0 - Physical interfaces**
 - Temperature and pressure sensors, valve actuators, circuit breakers

CIP STANDARDS MAJOR MILESTONES

2002	First appearance of the standards that would eventually become the CIP Standards in Appendix G of a FERC NOPR.
2003	First standards approved as voluntary "Urgent Action" standards.
2006	Draft 4 of CIP version 1 approved by NERC. Industry training begins.
2008	FERC approves CIP Standards and requires modifications. The required modifications range from simple to complex.
2008	CIP version 1 becomes mandatory and enforceable.
2009	CIP audits begin.
2010	CIP version 2 addresses the simple FERC-required changes, acceptance of risk, etc.

2010	CIP version 3 adds visitor control provisions.
2013	FERC remands two Interpretations of the CIP Standards.
2015	CIP-014 adds physical security provisions for major substations and Control Centers.
2016	CIP "version 5," the first major revision of the CIP Standards, becomes enforceable; CIP versions are no longer kept in sync.
2017	Low impact provisions become effective.
2020	CIP-013 adds supply chain requirements.
2022	CIP-012 adds protection for data transmission.
2024	BCSI revisions permit limited use of cloud.
2028	CIP-015 effective for network monitoring.

PART 1 8:15-10:00

INTRODUCTION TO NERC AND THE
RELIABILITY STANDARDS - LEW

**INTRODUCTION TO THE LOW IMPACT
STANDARDS - CHRIS**

OVERVIEW OF COMPLIANCE STEPS - DAVE
IDENTIFYING YOUR CIP SENIOR MANAGER
(CIP-003 R3, R4) - RON



Slido Questions!!!

What's a book you've read that related to your role?

Join at
slido.com
#2071 9698
Passcode:
tzy1n4





Slido Questions!!!

<https://www.nerc.com/news/Documents/NERCHistoryBook.pdf>

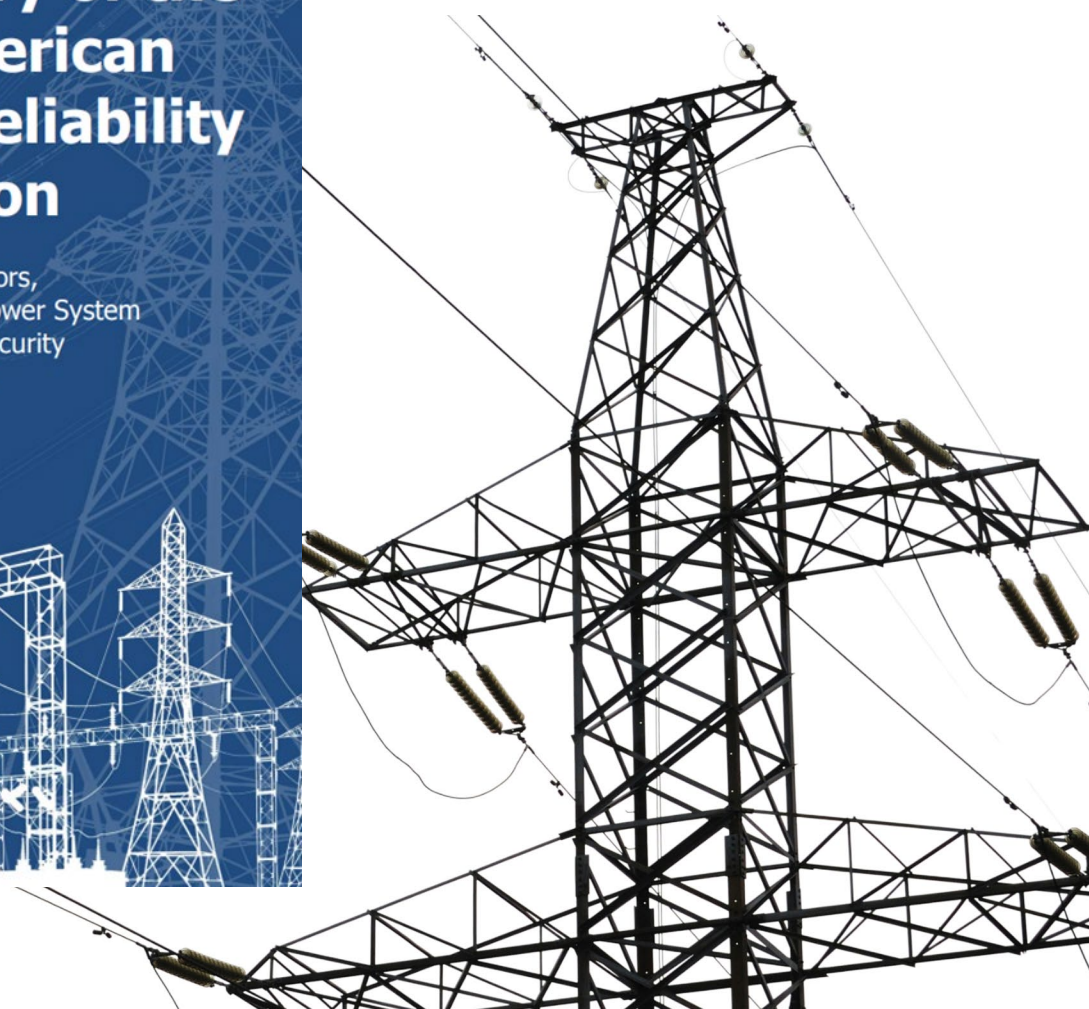
The History of the North American Electric Reliability Corporation

Helping Owners, Operators,
and Users of the Bulk Power System
Assure Reliability and Security
for More Than 50 Years

By David Nevius
Senior Vice President 1979–2012

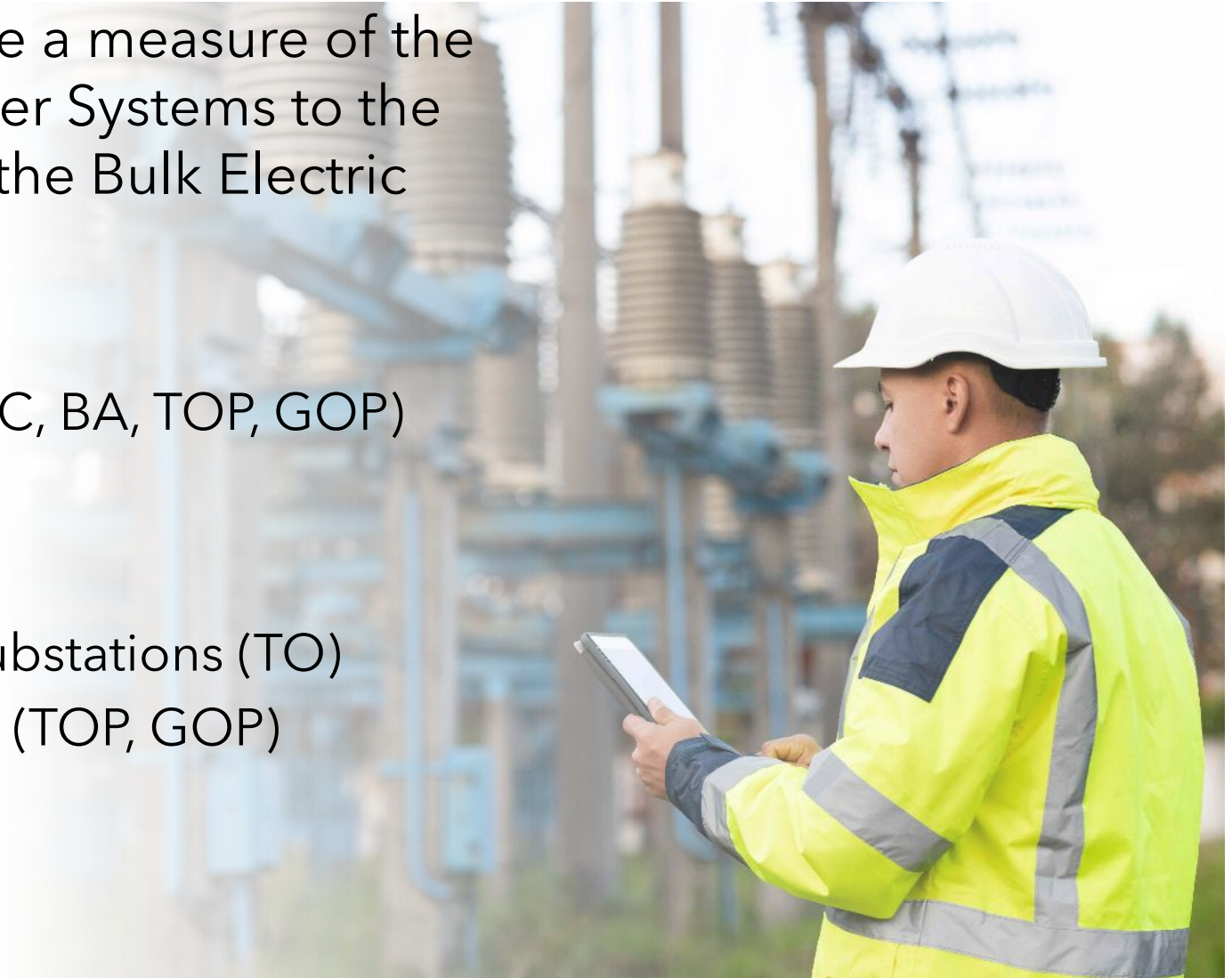


**Join at
slido.com
#2071 9698
Passcode:
tzy1n4**

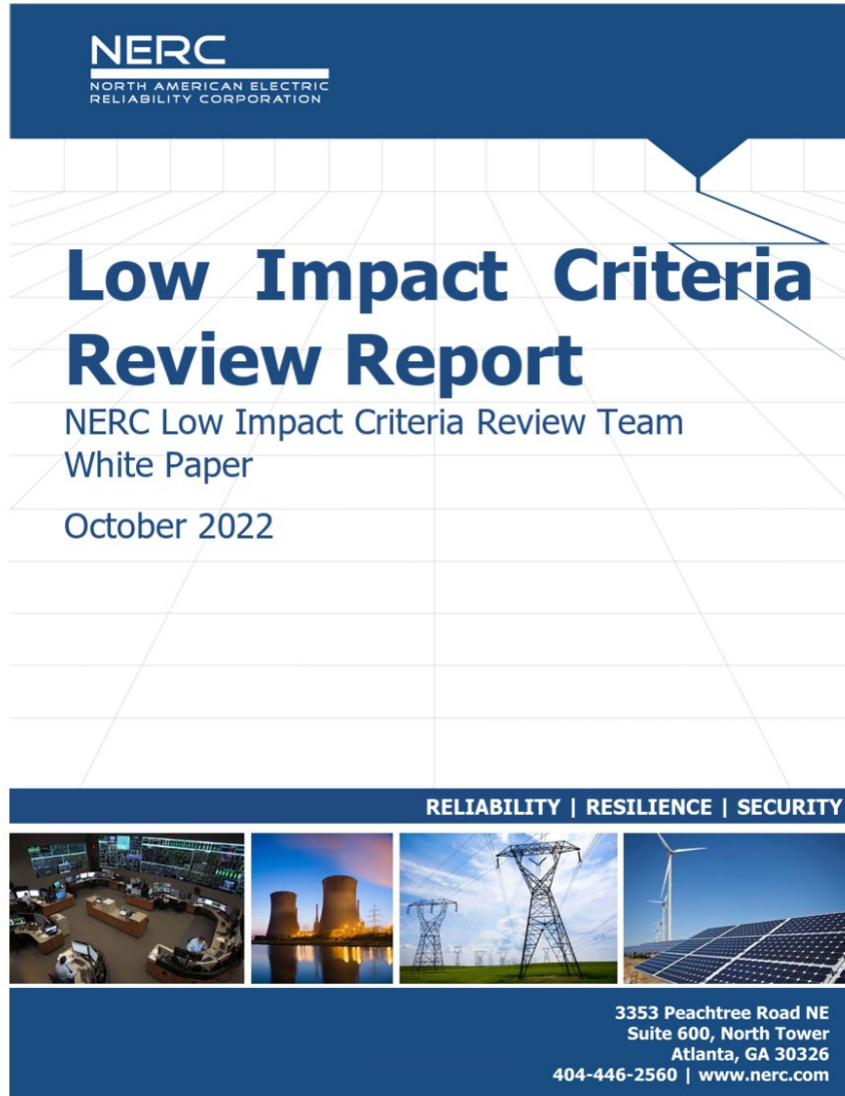


IMPACT RATINGS

- The CIP impact ratings are a measure of the risk of an asset's BES Cyber Systems to the stability and reliability of the Bulk Electric System (BES).
- High impact
 - Large control centers (RC, BA, TOP, GOP)
- Medium impact
 - Large generators (GO)
 - Large or high voltage substations (TO)
 - Mid-size control centers (TOP, GOP)
- Low impact
 - Everything else



WHY "LOW IMPACT" MATTERS



- Aggregated risk: small systems can collectively pose significant threats.
- Importance of securing even low-impact assets.
- Low-impact systems can be pivot points for malicious actors.
- Remote access is commonplace for low-impact assets.
- See the Low Impact Criteria Review Report for more detail:
 - [NERC Low Impact White Paper](#)

CIP-003 OVERVIEW

- Establishes **Management Buy-In** and involvement
(Policies, processes, plans, procedures)
- States how you take security seriously
- There is an expectation of a compliance program document that sets the tone of a strong culture of compliance



CIP-003 Security Management Controls

Specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise.

- Establish responsibility and accountability.
- Include: Emergency procedures, accessibility to procedure guidelines, a frequent review process (minimum yearly basis), management involvement, documentation of changes, information protection policies, limited access (designating personnel), and a clear cyber security policy.
- Designate a CIP Senior Manager who will act as the liaison both internally, between departments, and externally, and help formulate future CIP program plans.
- **Affects high, medium and low BES Assets**

CIP-003 Low Impact Assets

Establish responsibility, accountability and plans to secure Low Impact assets **specified in CIP-003 Attachment 1**

CIP-003 SECURITY MANAGEMENT CONTROLS

Standard CIP-003 outlines the responsibilities critical to safeguarding high and medium BES cyber systems from security risks that could compromise the reliability of the BES.

- Stakeholders of BES assets are required to implement security controls focused on:
 - Training personnel on appropriate security implementations
 - Maintaining electronic security perimeters
 - Enforcing physical security of assets
 - Reporting security incidents and initiating appropriate response protocols
 - Safeguarding sensitive information associated with BES assets
 - Creating cybersecurity awareness
 - Documentation of all security controls will help streamline the safeguards implemented across assets on the BES.



CIP-003 LOW IMPACT REQUIREMENTS

CIP-003-9 has **specific** requirements to protect Low Impact BES Cyber Systems and requires that registered entities develop one or more security plans that address each of these risk areas detailed in **Attachment 1**:

- Section 1. Cyber Security Awareness
- Section 2. Physical Security Controls
- Section 3. Electronic Access Controls
- Section 4. Cyber Security Incident Response
- Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation
- **Section 6. Vendor Electronic Remote Access Security Controls**

Additionally, **requirement 1.2.6 requires** a plan for declaring and responding to CIP Exceptional Circumstances.

More details on developing your security plans coming later in this workshop.



GO/GOP CATEGORY 2

- Operates (GOP) or owns and maintains (GO) “non-BES inverter based generating resources that either have or contribute to an aggregate nameplate capacity of greater than or equal to 20 MVA, connected through a system designed primarily for delivering such capacity to a common point of connection at a voltage greater than or equal to 60 kV.” [NERC Rules of Procedure Appendix 2, Definitions]
- Identification and registration of Category 2 GO/GOP entities is underway.
- Standards needed for Category 2 are identified*. Some are in development.

*Reliability Standards Compliance Dates for Generator Owners & Generator Operators

PART 1 8:15-10:00

INTRODUCTION TO NERC AND THE
RELIABILITY STANDARDS - LEW

INTRODUCTION TO THE LOW IMPACT
STANDARDS - CHRIS

OVERVIEW OF COMPLIANCE STEPS - DAVE

IDENTIFYING YOUR CIP SENIOR MANAGER
(CIP-003 R3, R4) - RON

OVERVIEW OF THE COMPLIANCE STEPS



There is a certain order imposed on these steps by the CIP Standards. For example, you don't know which set of cyber security policies you must develop until you know the impact ratings of your cyber systems.

The following slides are recommendations for the order of developing your initial CIP compliance program.

- **Note... that this is just an overview, and each step in the outline will receive its own section throughout the workshop.**
- **Note... Each of the items marked with an asterisk (*) also contains a periodic element that will need to be reviewed on an appropriate schedule.**

DESIGNATE YOUR CIP SENIOR MANAGER

This should be done first because it is the CIP Senior Manager who is responsible for all of the following steps. (**CIP-003 R3, Cyber Security – Security Management Controls**)

Should:

- Understand compliance responsibilities.
- Know how to manage delegated tasks.

Responsible for:

- Approving CIP policies *
- Approving List of BES Assets containing Low Impact BES Cyber Assets *
- Ensuring compliance
- Overseeing implementation



IDENTIFY YOUR PHYSICAL BES ASSETS

- Identify your physical BES assets.
- Perform a preliminary classification of your BES assets (**CIP-002-5.1a**

Attachment 1, Cyber Security – BES Cyber System Categorization)



Note: As we move to the other steps, we will be revisiting and updating this classification of BES Assets as we learn more and gather more information about our BES Assets.

DEVELOP AND APPROVE* CYBER SECURITY POLICIES

(CIP-003-9 R1 Part 1.2, Cyber Security – Security Management Controls):

- Cyber security awareness;
- Physical security controls;
- Electronic access controls;
- Cyber Security Incident response;
- Transient Cyber Assets and Removable Media malicious code risk mitigation; and
- Vendor Electronic Remote Access Security Controls
- Declaring and responding to CIP Exceptional Circumstances.



Note: Developing Cyber Security Policies is not a one and done process. They must be reviewed, updated, and implemented and communicated on an annual basis.

DEVELOP CYBER ASSET PROTECTION STRATEGY

For each BES asset that contains a low impact BES Cyber System, decide whether you will be protecting all Cyber Assets at the BES asset or only the low impact BES Cyber Systems at the asset (you can make this determination for each BES asset):

- All Cyber Assets at the BES asset
 - Develop* the list of BES assets containing low impact BES Cyber Systems (**CIP-002-5.1a R1 Part 1.3, Cyber Security – BES Cyber System Categorization**).



CONTINUED- DEVELOP CYBER ASSET PROTECTION STRATEGY

- Only the low impact BES Cyber Systems at the asset
 - Develop* the list of BES assets containing low impact BES Cyber Systems (**CIP-002-5.1a R1 Part 1.3, Cyber Security – BES Cyber System Categorization**). Identify all Cyber Assets associated with the BES asset.
 - Develop* the list of low impact BES Cyber Systems at each BES asset. This list will be needed later when you develop your physical and electronic access controls.
 - **Note...** that, according to **CIP-002-5.1a R1 Part 1.3 (Cyber Security – BES Cyber System Categorization)**, you only need to identify the BES asset containing the low impact BES Cyber Systems. This remains true, but since you are not protecting all of the Cyber Assets at the BES asset, you must be able to identify those Cyber Assets you are protecting (i.e., a discrete BES Cyber System list **is not required** for low impact to demonstrate compliance. However, it **should** be done to know “what” you are protecting and “how”.)



DEVELOP AND IMPLEMENT ONE OR MORE CYBER SECURITY PLANS



- **(CIP-003-9 R2, Cyber Security – Security Management Controls)**. These plans must include the Sections in **CIP-003-9 Attachment 1**:
 - Cyber Security Awareness*
 - Physical Security Controls
 - Electronic Access Controls
 - Cyber Security Incident Response*
 - Vendor Electronic Remote Access Security Controls
 - Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation

IF YOU OWN OR OPERATE A CONTROL CENTER...



...per the NERC Glossary definition, determine if you send or receive Real-time Assessment or Real-time monitoring data to another Control Center. If so, you need to protect the data being communicated in accordance with **CIP-012-2** (**Cyber Security - Communications between Control Centers**).

Note... Regardless of BES Cyber System Impact Rating, CIP-012 is applicable to Control Centers that send or receive Real-time Monitoring/Assessment data

[NERC Glossary of Terms](#)

PART 1 8:15-10:00

INTRODUCTION TO NERC AND THE
RELIABILITY STANDARDS - LEW

INTRODUCTION TO THE LOW IMPACT
STANDARDS - CHRIS

OVERVIEW OF COMPLIANCE STEPS - DAVE

**IDENTIFYING YOUR CIP SENIOR MANAGER
(CIP-003 R3, R4) - RON**



Slido Questions!!!

At what level within your organization does your CIP Senior Manager reside? ("Don't Know" is an OK response too.)

**Join at
slido.com
#2071 9698
Passcode:
tzy1n4**



WHAT MUST THE ORGANIZATION DO?



Identify a CIP Senior Manager

- Designate one individual by name as the CIP Senior Manager.
- Include a date of designation in the documentation.

Grant Responsibility and Authority

- Responsibility is not enough—authority must also be granted.
- CIP Senior Manager must have:
 - The power to make decisions.
 - Adequate resources (staff, budget).

Initial Implementation

The CIP Senior Manager must lead:

- Initial implementation of the NERC CIP program.
- Development of the program, if not already in place.
- Revisions as standards evolve or new ones apply.

Ongoing Compliance

Compliance is a continuous process, not a one-time task.

WHAT SHOULD THE ORGANIZATION DO?



- A strong CIP compliance program is designed to monitor the OT (Operational Technology) cybersecurity program.
 - Ensures that all security processes are carried out properly and on time.
- The CIP Senior Manager should have authority over the OT cybersecurity program.

WHO IS THE CIP SENIOR MANAGER?



Defined in the NERC Glossary of Terms

"A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011."

Responsible for:

- Approving CIP policies
- Approving List of BES Assets containing Low Impact BES Cyber Assets
- Ensuring compliance
- Overseeing implementation

KEY QUALIFICATIONS

Senior-level authority in the organization.

Must have the necessary resources and oversight capabilities.

Should:

- Understand compliance responsibilities.
- Know how to manage delegated tasks.



SELECTING THE RIGHT PERSON

Should be someone who:

- Has executive backing.
- Can influence cross-functional teams (IT, OT, compliance, etc.).

Ideally in roles like:

- Director of Compliance
- IT/OT Executive
- Security Program Manager
- Plant Manager



DELEGATION VS ACCOUNTABILITY

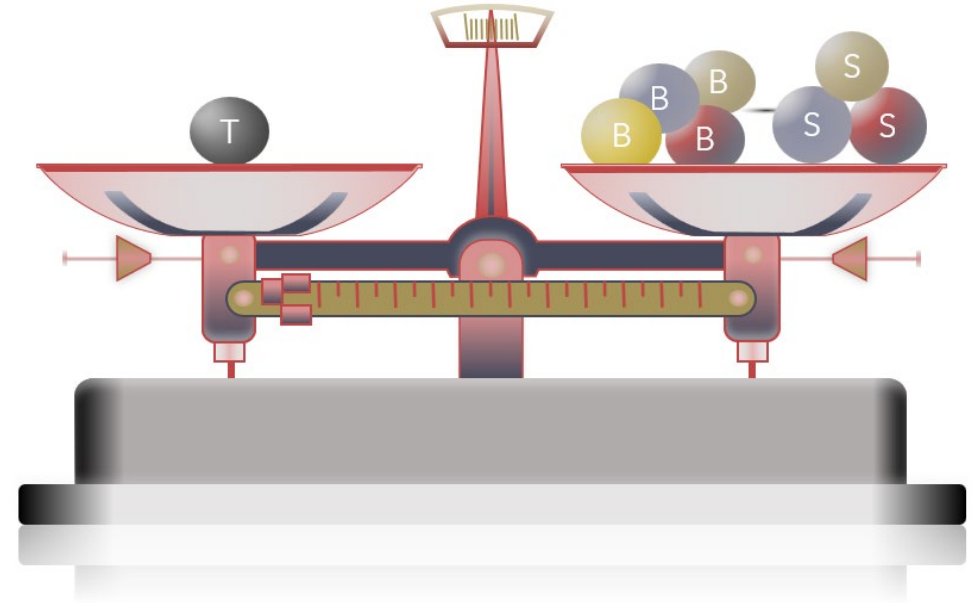
Tasks can be delegated.

Accountability cannot!

The CIP Senior Manager:

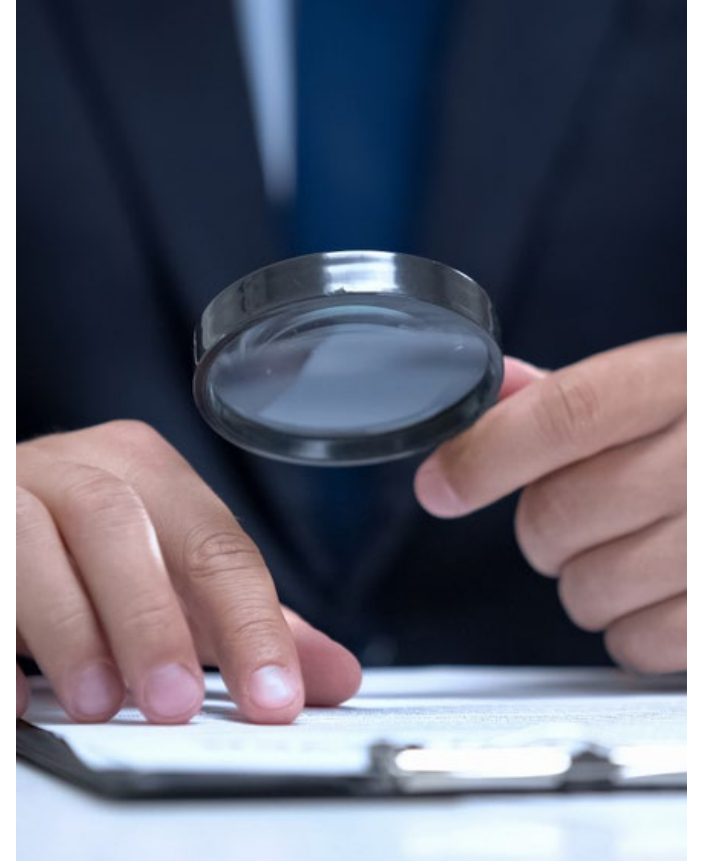
- Must own the program.
- Is responsible to regulators (NERC, FERC, etc.).

Delegation changes must be documented within 30 days of the change



COMMON MISSTEPS

- Assigning someone too inexperienced
- Designation of a "non-senior" person
- Treating the role as a "checkbox"
- Lack of clarity in responsibilities
- Lack of authority for the role and responsibilities



REQUIREMENTS AND BEST PRACTICES



- Formalize the appointment
- Regularly review roles and responsibilities, especially if delegating
- Provide training and support
- Ensure visible executive support

FINALLY...

The right CIP Senior Manager =

Stronger compliance posture.

This role sets the tone at the top and communicates that tone to the organization (i.e., **EVERYONE**).

Make the decision carefully and intentionally.

For more information see Lew Folkerth's Lighthouse article "*CIP low impact from the ground up - Part 4, Identifying your CIP Senior Manager*"

[The Lighthouse: CIP low impact from the ground up - ReliabilityFirst](#)

PART 2 10:15- 12:00

IDENTIFYING BES ASSETS CONTAINING LOW IMPACT BCS (CIP-002) - RON

GOVERNANCE AND POLICY (LOW IMPACT
ONLY) - CHRIS

WHAT IS AN IMPACT RATING?



Impact ratings measure the importance of assets to the Bulk Electric System (BES).

CIP-002-5.1a defines three levels:

High: Major Control Centers

Medium: Large substations, large generators, some Control Centers

Low: All other applicable BES assets

UNDERSTANDING LOW IMPACT RATINGS

Low impact = low effect on BES reliability/stability

However, can still cause significant local disruption

For example, Heathrow Airport substation outage

Impact ratings are contextual to BES reliability, not public/industry impact



BES CYBER SYSTEMS & PHYSICAL ASSETS

Impact ratings technically apply to BES Cyber Systems

But in practice, discussed in terms of physical assets

CIP-002-5.1a Part 1.3:

- Requires identification of physical assets with low impact BES Cyber Systems

- Does not require listing individual BES Cyber Systems



WHAT IS A BES CYBER SYSTEM?

Cyber Asset: "Programmable electronic devices, including the hardware, software, and data in those devices. "

Programmable electronic device (anything with a CPU)

BES Cyber Asset: "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non operation, adversely impact one or more Facilities, systems, or equipment [...]."

BES Cyber System: "One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity."

Examples:

Relay: Milliseconds impact

PLC controlling boiler: Seconds impact

Billing meter: Not BES Cyber Asset



REDUNDANCY DOESN'T EXCLUDE IMPACT

- Do not discount Cyber Assets due to redundancy
- Even one operator console, if compromised, can be used maliciously
- Every Cyber Asset must be assessed on its potential impact

GROUPING BES CYBER ASSETS



A BES Cyber System = group of BES Cyber Assets



Grouping is flexible:

- One per system
- Entire site
- Any logical configuration



Use CIP-002-5.1a Application Guide (esp. pg. 14) for methodology

IDENTIFY & DOCUMENT LOW IMPACT ASSETS



Create a list of assets with low impact BES Cyber Systems



Document your identification process



Get approval from CIP Senior Manager



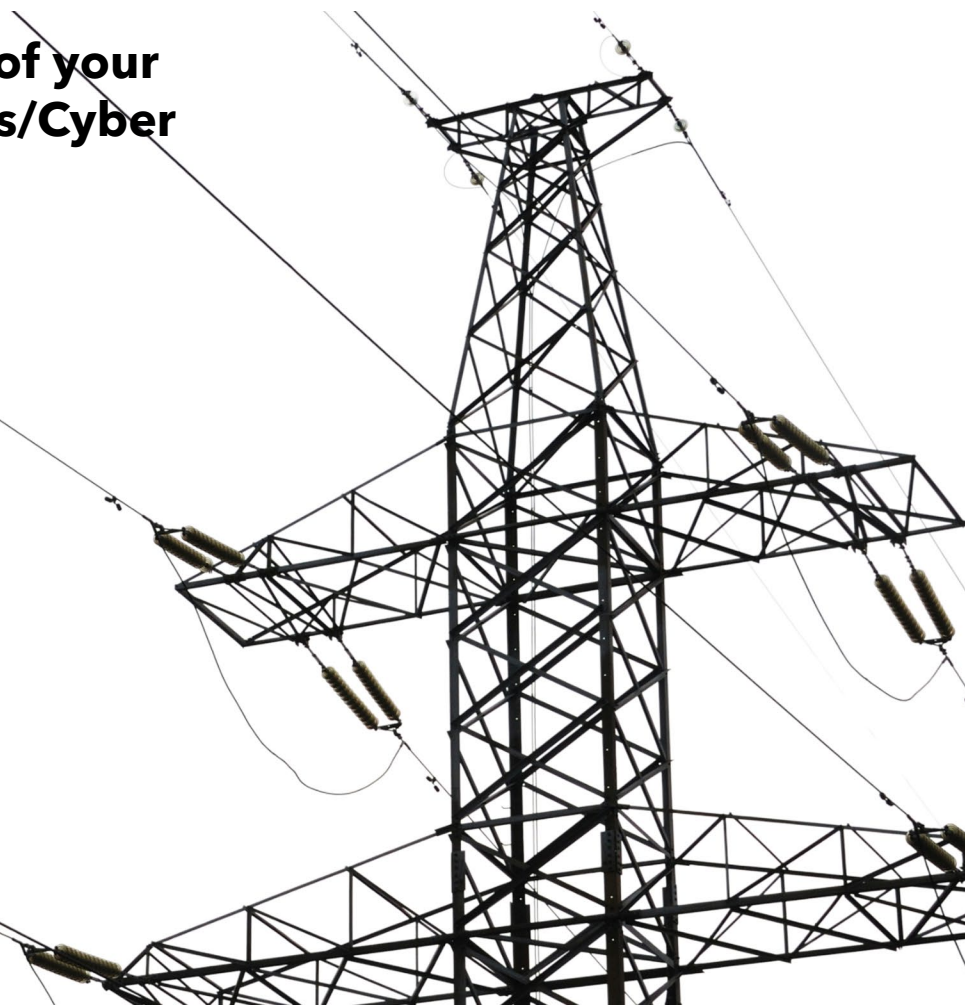
Retain list and documentation for audits



Slido Questions!!!

**Do you maintain an inventory of your
Low Impact BES Cyber Systems/Cyber
Assets?**

**Join at
slido.com
#2071 9698
Passcode:
tzy1n4**



CHOOSE YOUR PROTECTION APPROACH

TWO OPTIONS:

1. PROTECT ENTIRE PHYSICAL ASSET
2. PROTECT ONLY LOW IMPACT BES CYBER SYSTEMS
 - Requires identifying those systems (even if not required by standard)
 - Needed for audit assurance and effective protection

ASSET-BY-ASSET DECISIONS

YOU MAY CHOOSE PROTECTION METHOD PER
ASSET

NO NEED TO APPLY ONE METHOD ACROSS
THE WHOLE ORGANIZATION

CONSIDER:

- Time sources (GPS clocks)
- Stability systems (PMUs)
- Other critical support devices

GENERATOR SEGMENTATION

For generation
 ≥ 1500 MW:

- Use Impact Rating Criterion 2.1 for segmentation

Recommended
resources:

- "Lessons Learned" document on shared BES Cyber Systems
- Generation Segmentation CMEP Practice Guide

PART 2 10:15- 12:00

IDENTIFYING BES ASSETS CONTAINING LOW
IMPACT BCS (CIP-002) - RON

**GOVERNANCE AND POLICY (LOW IMPACT
ONLY) - CHRIS**

GOVERNANCE AND POLICY

Compliance and Security are both continuous processes, NOT end states



Can we state with certainty that we are fully compliant?

Today?

Tomorrow?

Can we state with certainty that we are fully secure?

Today?

Tomorrow?

WHAT

It starts

Well

Go
pla
yo
Go
yo
the



es

s

sses

POLICIES

“The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities’ management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.”

Defined in CIP-003-6 Section A.6, Background

POLICY ORGANIZATION

- You may have one policy for your entire organization and for all required policy topics
- You may separate each required topic into its own policy
- You may have different policies for different asset types (e.g., control centers, generators, substations).

As you can see, it's your choice!

We recommend an overarching Master Policy if you have multiple policies that:

- Identify each individual policy
- Describe the applicability of each
- Describe how they cover all the required topics for ALL required assets
- Communication is key*

*Real-life example of issues with mis- or non-communication

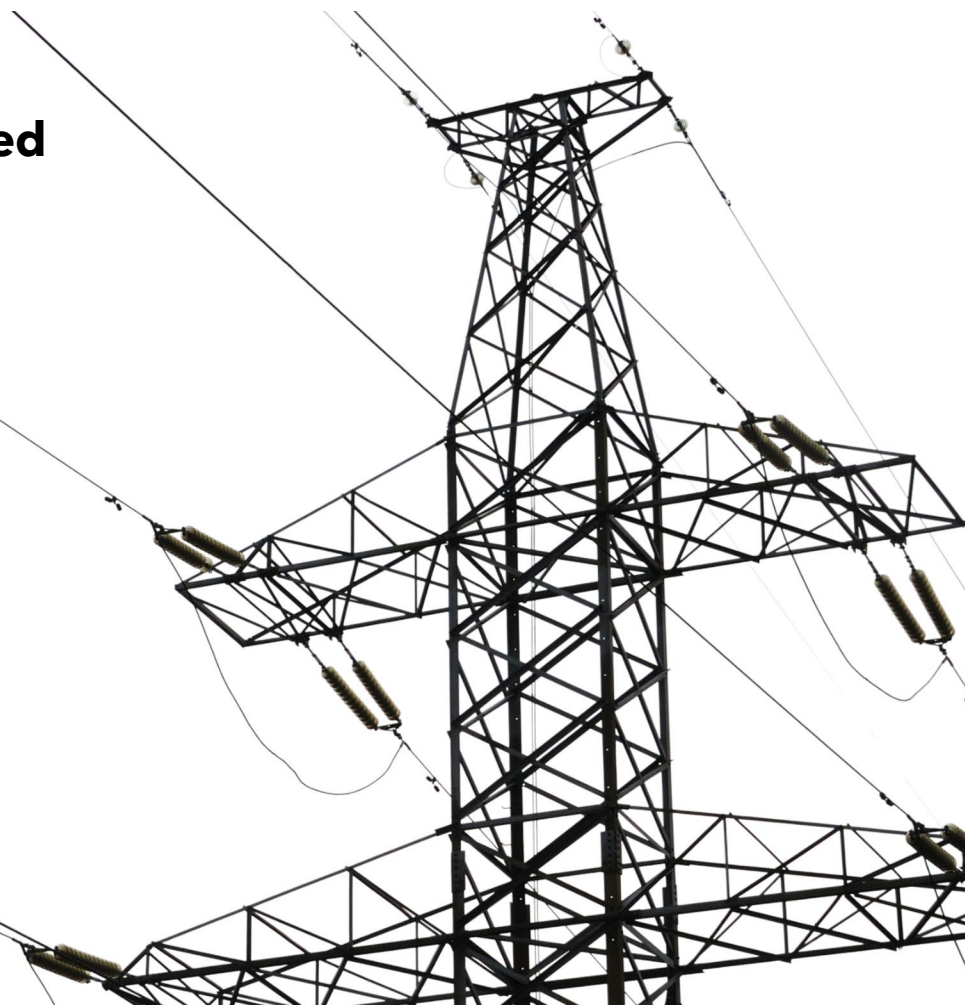




Slido Questions!!!

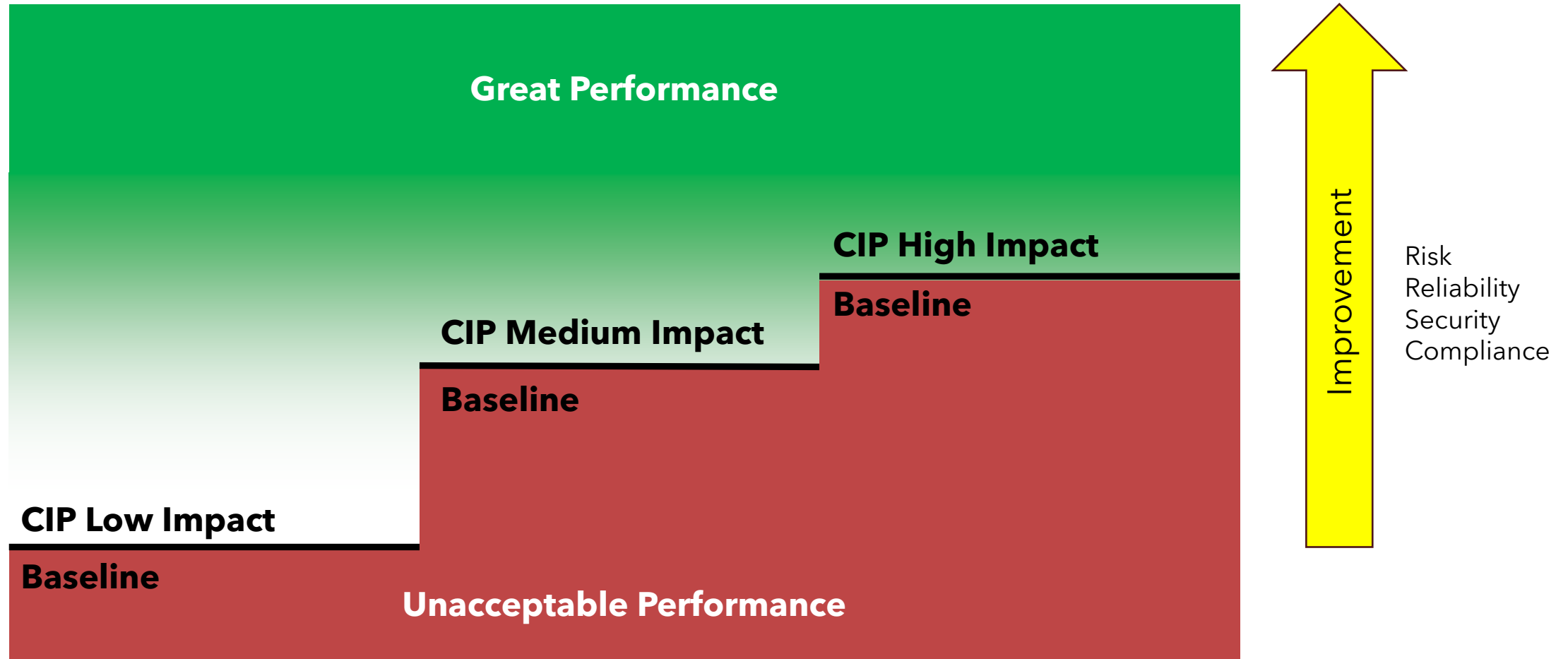
**How are your policies structured
in your organization?**

**Join at
slido.com
#2071 9698
Passcode:
tzy1n4**



FOUNDATIONAL VS. ASPIRATIONAL

NIST CSF, NIST 800-53, IEC 62443, etc.



ABOVE VS "JUST AT" THE BASELINE

Policies can allow and encourage you to aspire to go above the baseline

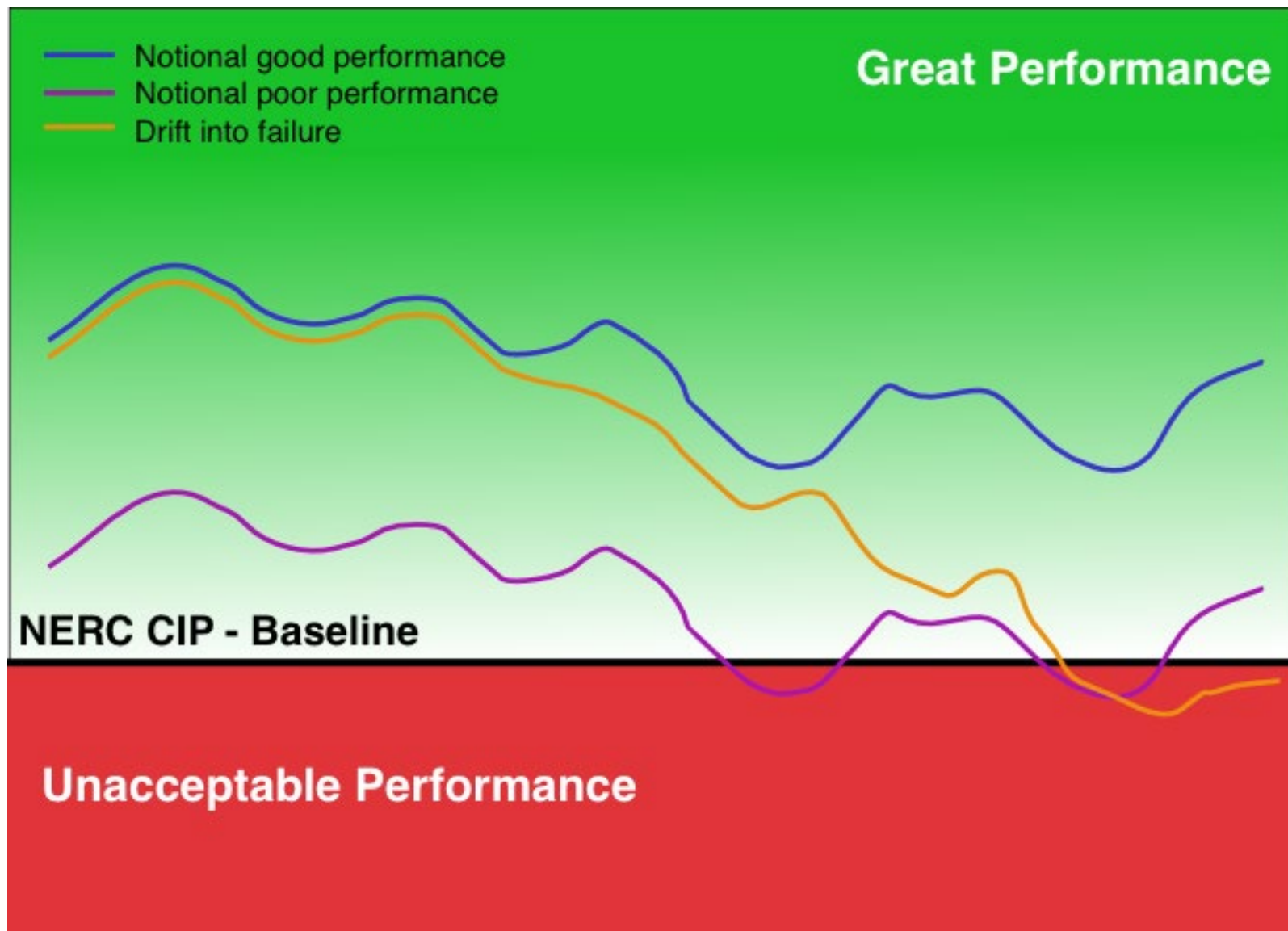
Example 1:

- Your cyber security incident response plans must be tested once every 36 months for low impact
 - Is that really adequate?
 - You can state in your policy that you will have your incident response team receive regular training and your response plan will be tested annually

Example 2 :

- Your Cyber Security Awareness program must reinforce cyber security practices every 15 months
 - Is that really adequate for your organization?
 - You can state in your policy that you will reinforce your cyber security practices every 3 months

DRIFT INTO FAILURE



POLICY SUGGESTIONS

The golden rule: Do not simply replicate or paraphrase the language of the requirement!

We have seen entities state “All physical access to assets must be controlled” in a physical access policy.

A much better way to state this might be:

“Access to assets will be granted only on demonstrated and documented need. Access to the control center will be by key card and PIN. Access to substations will be by physical key, with all keys managed by the Key Inventory Management Program.”

Advantages:

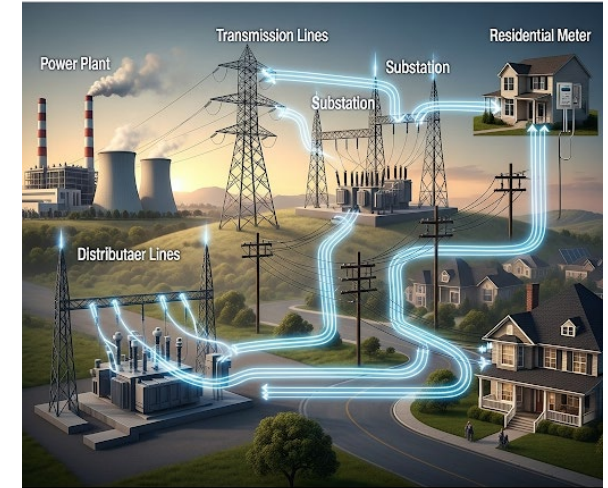
- States how you view the requirement and how you will approach implementation
 - No specifics such as vendor names are stated, as those can change with time
 - Risk to the protected systems is addressed, with higher risk systems receiving greater protection
 - The scope is also addressed



SUMMARY

A well written cyber security policy will accomplish the following:

- Articulate goals
- Define objectives
- State expectations
- Encourage “above the baseline” aspirations
- Ensure consistency across facilities and business units



This also clearly demonstrates a tone from the top that security and compliance are high priorities for **everyone** and not options.

PART 3 1:00-2:30

DEVELOPING YOUR LOW IMPACT CYBER SECURITY PLANS - LEW/RON

READING THE STANDARDS

- Make sure you're reading the correct version of the Standard
 - <https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx>
 - Inactive
 - Subject to Enforcement
 - Subject to Future Enforcement
 - Filed and Pending Regulatory Approval
 - Pending Regulatory Filing
- Capitalized terms are defined in the NERC Glossary
 - https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf
 - Subject to Enforcement
 - Pending Enforcement
 - Filed and Pending Regulatory Approval
 - Retired Terms

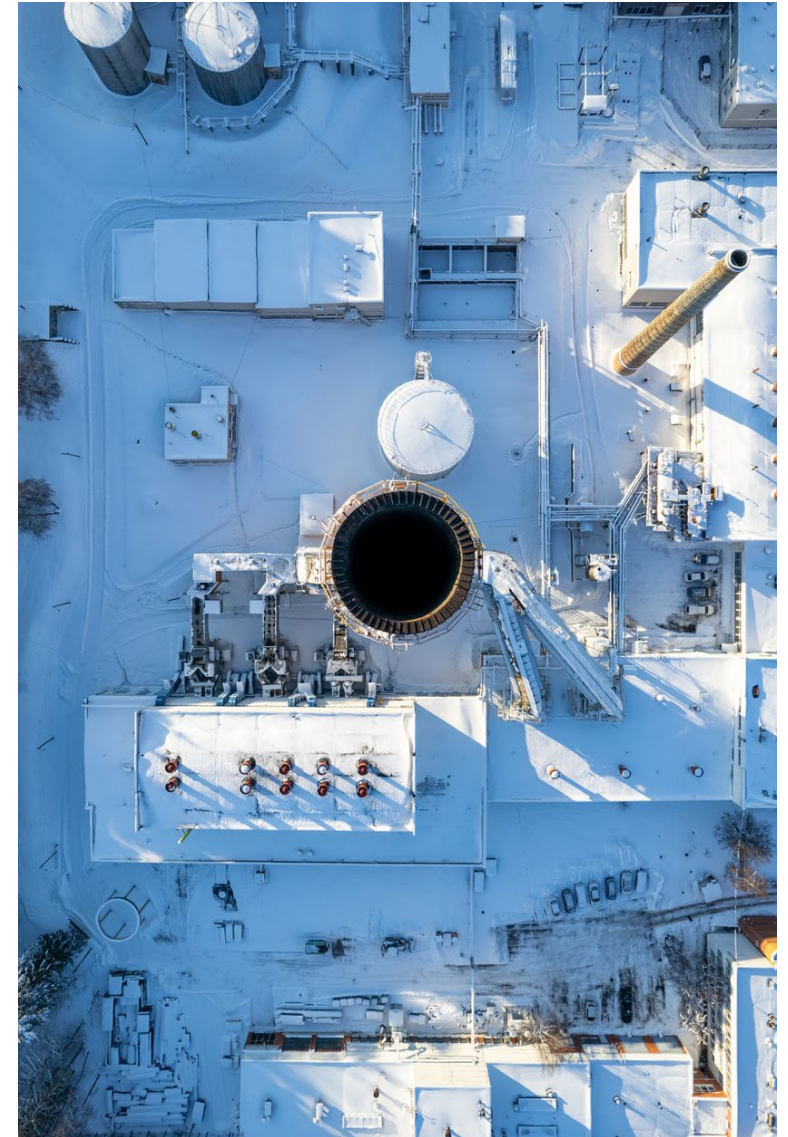
CYBER SECURITY PLANS

CIP-003 R2

If you have one or more assets containing low impact BES Cyber Systems, you must:

- Develop, document and implement
- At least one cyber security plan
- For low impact BES Cyber Systems
- As specified in Attachment 1

“Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.”



CIP-003-9 ATTACHMENT 1

- Called into scope by R2
- Six Sections:
 1. Cyber Security Awareness
 2. Physical Security Controls
 3. Electronic Access Controls
 4. Cyber Security Incident Response
 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation
 6. Vendor Electronic Remote Access Security Controls

CYBER SECURITY PLANS

	Plants	GOPCC
S1 Aware	Plan 1 General	
S2 Phys	Plan 2	Plan 4
S3 Elec	Plan 3	
S4 IRP	Plan 1 General	
S5 TCA		
S6 VRA		

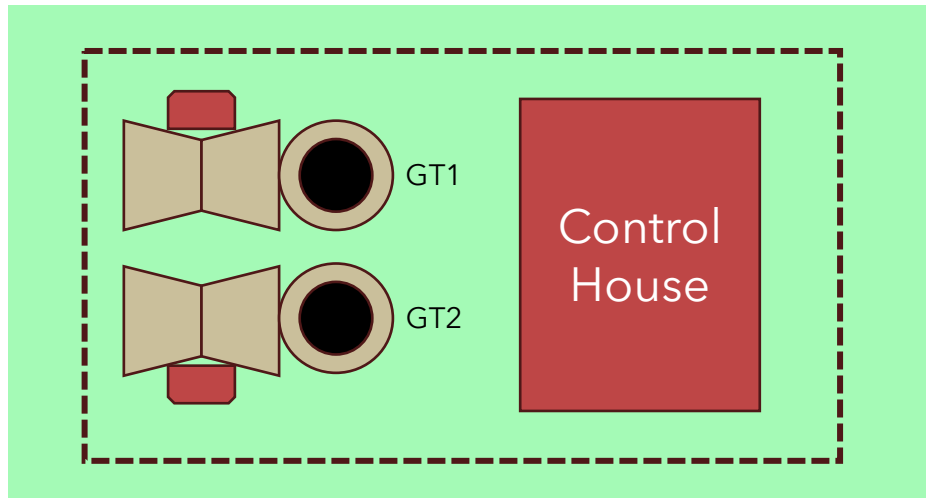
- May have one plan to cover all low impact assets
- May have multiple plans
- May group as needed or desired
- Each asset **must** have a plan for each of the six Sections
- May use plans from high or medium impact BES Cyber Systems

Notional low impact plan organization

A CHOICE

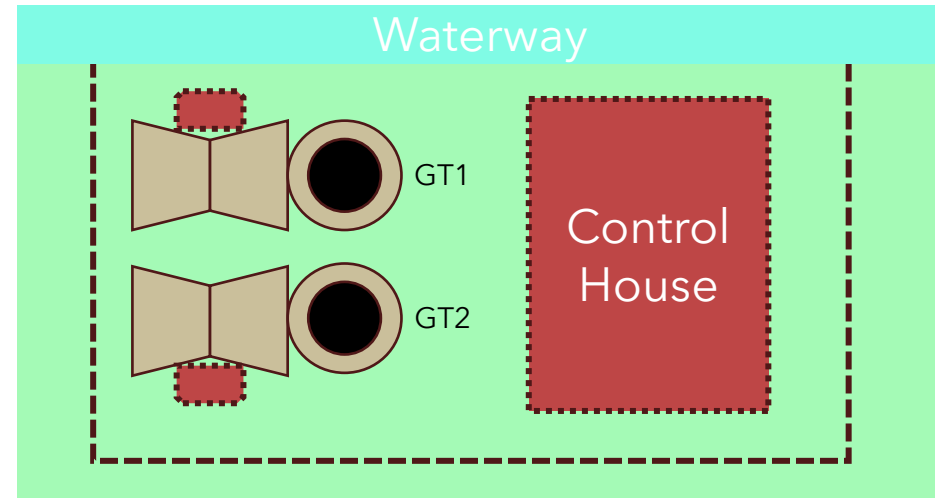
Asset-level protection

Implement physical or electronic access controls at the asset (plant, substation, Control Center) level.



BES Cyber System-level protection

Implement physical or electronic access controls at the device (computer, relay, RTU, etc.) level.



A CONTRADICTION?

BES Cyber System-level protection

- **Must** control access to each low impact BES Cyber System and electronic access control system
- **Must** know what and where the systems are in order to protect them
- **Must** be able to provide evidence of protection for each system

No list of BES Cyber Systems required

- Auditors must have reasonable assurance of compliance
- Auditors cannot require a list of systems
- If auditors cannot obtain reasonable assurance of compliance, they will write a violation based on non-performance of Section 2 or Section 3, not absence of list

SECTION 1

Cyber Security Awareness

- Awareness/reinforcement is not training
 - Asset or group oriented, not individual
 - Training is direct person-to-person or teaching-system-to-person
 - Awareness/reinforcement may be direct or indirect (e.g., poster, email, etc.)

Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

SECTION 1

Cyber Security Awareness

- What you **must** do:
 - Document that you have performed reinforcement of cyber security practices (which may include physical security practices) at least once every 15 calendar months.
- What you **could** do:
 - You could fold it into your annual HR policy review.
 - You could include a cyber tip in your pre-job safety briefings.
 - You could get creative - posters, quizzes, even a “phish of the month” club.
 - The key is to make it stick. If your team can’t remember the last time they heard about cyber security, it’s time to rethink your approach.

SECTION 2

Physical Security Controls

Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to

(1)

the asset or

the locations of the low impact BES Cyber Systems within the asset, and

(2)

the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

SECTION 2

Physical Security Controls

- What you **must** do:
 - Control physical access – preventive control
 - Monitoring is a detective control and is insufficient to control physical access by itself
 - On an asset-by-asset basis, choose to either protect the asset as a whole, or the individual BES Cyber Systems and electronic control systems within the asset
- Note that a Physical Security Perimeter (PSP) is not required

SECTION 3

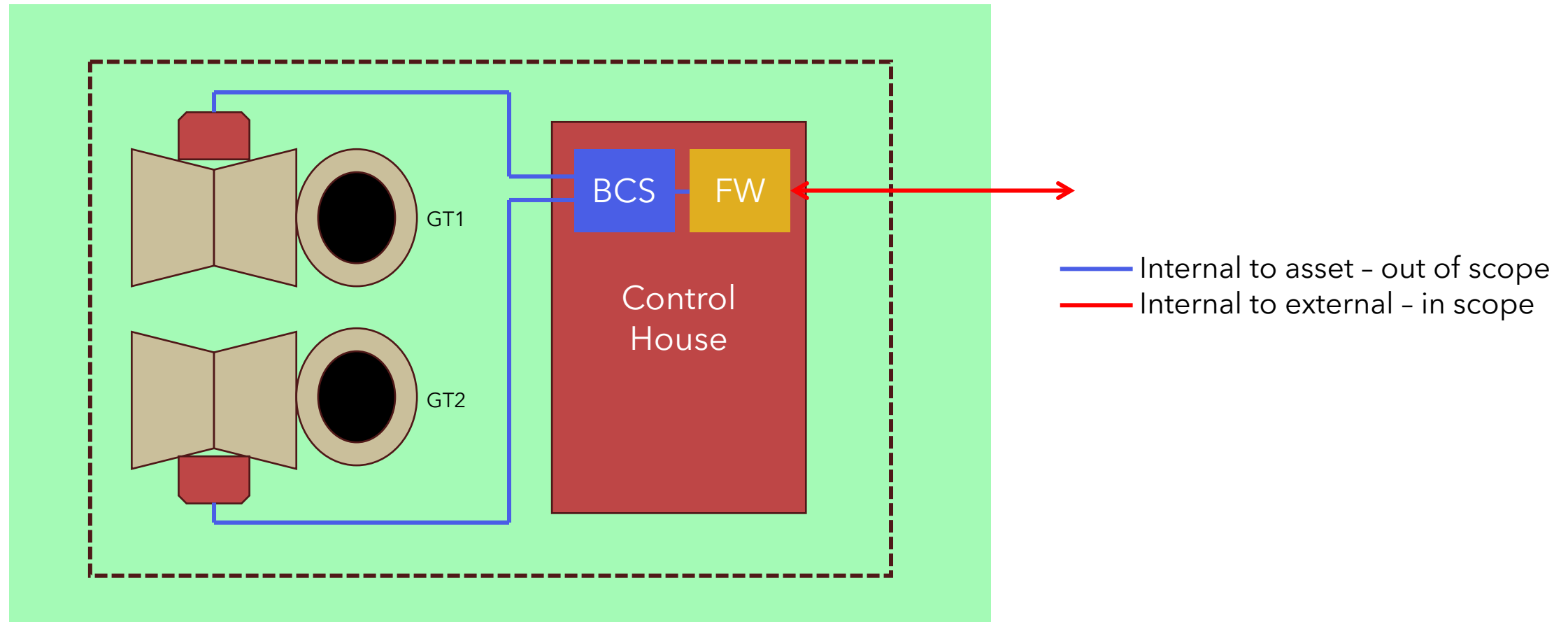
Electronic Access Controls (network)

For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

- 3.1** Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:
- i.** between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
 - ii.** using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and
 - iii.** not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC-61850-90-5 R-GOOSE).

SECTION 3

Electronic Access Controls (network)



SECTION 3

Electronic Access Controls (network)

- What you **must** do:
 - Deny by default (implied)
 - “[P]ermit only necessary”
 - How do you document what is necessary?
 - Source & destination addresses
 - Protocol
 - Business need

SECTION 3

Electronic Access Controls (network)

- What you **should** do:
 - Firewall change management
 - Periodic reviews
- Note that an Electronic Security Perimeter (ESP) is not required

SECTION 3

Electronic Access Controls (dial-up)

For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

- What you **must** do:
 - Use some form of authentication, such as:
 - ID/password
 - Dial-back mechanism.
 - Dial-up is usually non-routable, but if the traffic is routable, you must also use a firewall or filter.

SECTION 4

Cyber Security Incident Response

Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

- What you **must** do:
 - Develop a Cyber Security Incident response plan (CSIRP) for each asset containing a low impact BES Cyber System - a single CSIRP may cover multiple assets, but each asset must have a CSIRP.
 - Each CSIRP must contain provisions to identify Cyber Security Incidents.
 - Each CSIRP must contain provisions to classify Cyber Security Incidents.
 - Each CSIRP must contain provisions to respond to Cyber Security Incidents.

SECTION 4

Cyber Security Incident Response

Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

- What you **must** do:
 - Include provisions in your CSIRP to determine if a Cyber Security Incident meets the definition of a Reportable Cyber Security Incident.
 - Include provisions in your CSIRP to report a Reportable Cyber Security Incident to the E-ISAC.
 - If there are legal concerns about reporting to the E-ISAC, they must be documented in your CSIRP.

SECTION 4

Cyber Security Incident Response

Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

- 4.3** Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;
- What you **must** do:
 - Your CSIRP must identify roles and responsibilities for the incident response team.
 - What you **should** do:
 - Ensure your incident response team has all of the skill sets the team is likely to need.
 - An incident response team is a team. They need to practice their incident response skills and they need to practice working as a team.

SECTION 4

Cyber Security Incident Response

Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.4 Incident handling for Cyber Security Incidents;

- What you **must** do:
 - Include incident handling provisions in your CSIRP.
 - Ensure your CSIRP covers each BES Cyber System at the asset.
- What you **should** do:
 - Ensure your CSIRP covers likely threat scenarios (cyber threat intelligence can help with this).
 - Ensure your CSIRP includes good practices from one or more of the reference sources.

References:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf>

<https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls>

[https://www.cisa.gov/sites/default/files/2024-08/Federal Government Cybersecurity Incident and Vulnerability Response Playbooks 508C.pdf](https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf)

SECTION 4

Cyber Security Incident Response

Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by:

- (1) responding to an actual Reportable Cyber Security Incident;
 - (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or
 - (3) using an operational exercise of a Reportable Cyber Security Incident; and
- What you **must** do:
 - Your CSIRP must include provisions to test the CSIRP at least once every three years. If a CSIRP covers more than one asset, you do not need to test the CSIRP for each asset.
 - If a single CSIRP covers assets at multiple Registered Entities, you must test the CSIRP for each Registered Entity.
 - You must test a Reportable Cyber Security Incident to be considered a valid test.

SECTION 4

Cyber Security Incident Response

Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

- 4.6** Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.
- What you **must** do:
 - Your CSIRP must contain provisions for updating itself with lessons learned within 180 days of a test or actual response.
 - What you **should** do:
 - Don't let it go half a year. You'll forget what needs to be updated.
 - Consider using a checklist for the major steps in the CSIRP. Leave space to note suggestions for improvement. The completed and dated checklist can then become your evidence of completion of the test.

Transient Cyber Assets and Removable Media

- **Objective**

Understand the risks and best practices for managing Transient Cyber Assets (TCAs) and Removable Media (RM) for Low Impact entities.

- **Why It Matters**

TCAs and removable media are common entry points for malware and cyberattacks on critical infrastructure.

- **Regulatory Context**

CIP-003-8 mandates control of these devices for Low Impact entities.



Transient Cyber Asset (TCA)

A Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
 - BES Cyber Asset,
 - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
 - PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.



Removable Media (RM)

Storage media that:

1. are not Cyber Assets,
2. are capable of transferring executable code,
3. can be used to store, copy, move, or access data, and
4. are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Removable Media include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.



RISKS OF TCAs & REMOVABLE MEDIA

- Malware introduction (e.g., ransomware, keyloggers)
- Unauthorized access or data exfiltration
- Propagation of threats to BES Cyber Systems (BCS)
- Compliance violations and fines



ISSUES SEEN WITH TCA AND RM

- Third-party TCAs - entity does not ensure they are being checked before use
- Documentation of TCAs and RM
- Training of personnel on use of RM and implementation of processes
- Scanning TCAs - AntiVirus (AV) not up-to-date
- Vendor attestation that they performed the requirements, but no verification from entity
- Lack of scanning RM for those plugging into BCS
- Lack of retention of evidence for scans, such as forms, screenshots, etc.

ISSUES SEEN WITH TCA AND RM

- Scans of device that fails checks, entity lacks controls to prevent bypassing failures for scanning TCAs or RM
- Lack of methods to mitigate introduction of malicious code
- Lack of consistent and repeatable processes to do the scanning and inspection, performing these duties each time
- Entities that claim not to use RM (in policies, etc.), but do use RM
- Devices connected more than 30 days - compliance issues

BEST PRACTICES

- Create forms with directions - repeatability
- Record AV signature status
- When devices are plugged in, send an alert if possible - compliance team can check logs to review those devices that were plugged in - technical/procedural control and review if the process to check the TCA or RM was followed
- Create a jump host, i.e. a common area to plug into - provide control over what is connecting
- Make it a part of the Job Safety Briefing - briefing before entering or doing work at Low Impact locations
- Asset management for TCAs and RM - know what you have



BEST PRACTICES CONTINUED

- Make sure AV is up-to-date; check AV every two weeks to a month
- Engine updates
 - Knowing that AV is up-to-date is good, but also consider real-time monitoring
- Provide the log of the scan, in addition to a screenshot - screenshots are usually not good by themselves, logs provide more context
- Easiest way to show that AV is up-to-date can be a central console showing agents checking in; reporting of TCAs - patches and signatures; if not updated for two weeks, they contact person to let them know to update
- Supply screenshots from the TCA
- Use whitelisting



SECTION 6 (EFFECTIVE 4/1/2026)

Vendor Electronic Remote Access Security Controls

For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

- 6.1** One or more method(s) for determining vendor electronic remote access;
 - What you **must** do:
 - Include in your cyber security plan a provision for determining (detecting and identifying) all remote access by a vendor.

SECTION 6

Vendor Electronic Remote Access Security Controls

For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.2 One or more method(s) for disabling vendor electronic remote access; and

- What you **must** do:
 - Include in your cyber security plan a provision for disconnecting existing vendor remote access sessions and disabling future vendor remote access sessions.

SECTION 6

Vendor Electronic Remote Access Security Controls

For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

- What you **must** do:
 - Include in your cyber security plan a provision for detecting malicious communications during remote access by a vendor.

PART 4 2:45-4:45

CIP-012 - DAVE

CIP-014 - CHRIS

FUTURE STATE - -10,-11,-12, CATEGORY 2 -
CHRIS

QUALITY EVIDENCE/RSAW/ERT - LEW

CLOUD - LEW

WRAP-UP - REFERENCES, WEBINARS

IF YOU OWN OR OPERATE A CONTROL CENTER... CIP-012-1



...per the NERC Glossary definition, determine if you send or receive Real-time Assessment or Real-time monitoring data to another Control Center. If so, you need to protect the data being communicated in accordance with **CIP-012-1 (Cyber Security - Communications between Control Centers)**.

Note... **CIP-012-2** is subject to future enforcement in 7/1/2026!

[Project 2016-02 Modifications to CIP Standards \(CIP-012-1\)](#)

[Project 2020-04 Modifications to CIP-012 \(CIP-012-2\)](#)

WAIT... ARE YOU SURE I NEED TO DO THIS?

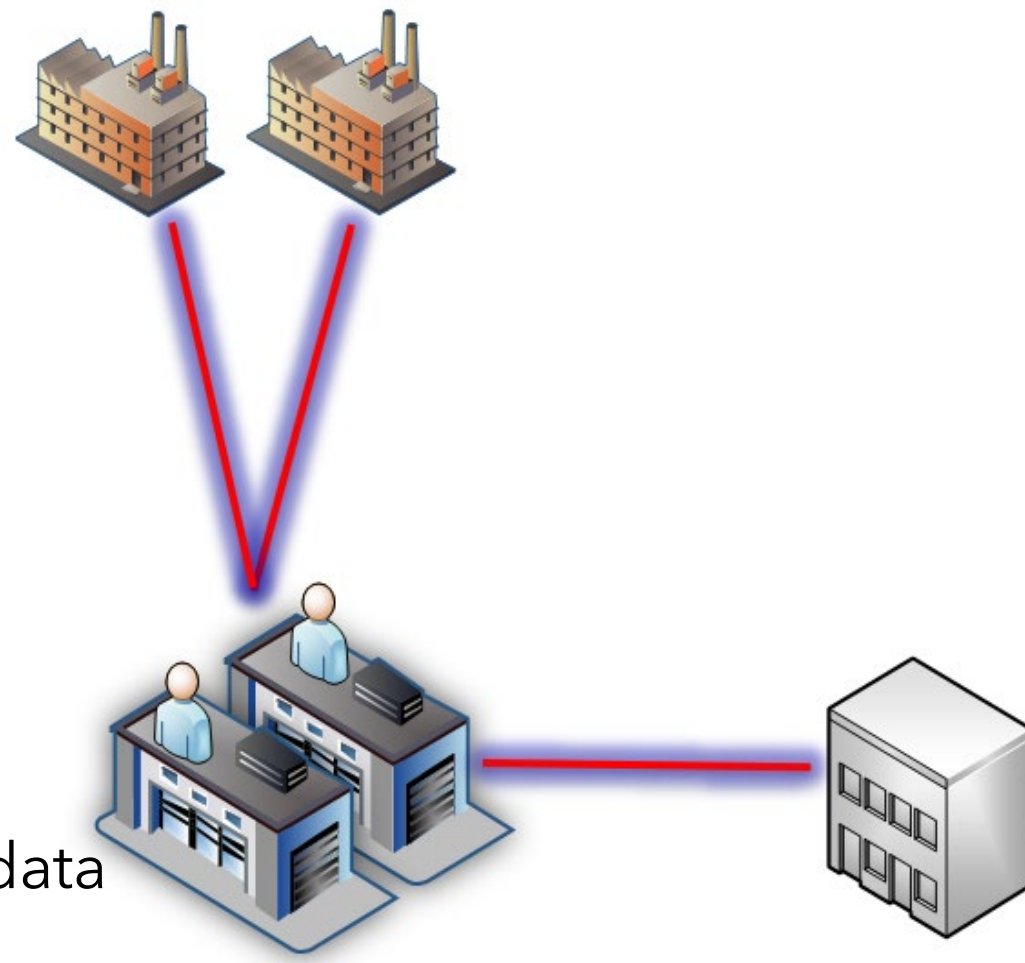
What Functional Entities does this apply to?

RC	GO	TO
BA	GOP	TOP

What type of data are we trying to protect?

Real-time Assessment (RTA) and Real-time monitoring data (RTM) transmitted between Control Centers.

- Additional information on RTA and RTM data can be found in TOP-003 and IRO-010



WAIT... WHAT ARE WE CALLING A CONTROL CENTER?

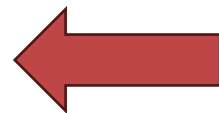
Subject to Enforcement						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Control Center	Project 2008-06		11/26/2012	11/22/2013	7/1/2016	One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

**PENDING FERC APPROVAL

Filed and Pending Regulatory Approval						
Continent-wide Term	Link to Project Page	Acronym	BOT Adoption Date	FERC Approval Date	Effective Date	Definition
Control Center	Project 2021-03		12/10/2024			One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks <u>including their associated data centers</u> , of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations. OR One or more facilities of a Transmission Owner that have the capability to control transmission Facilities at two or more locations in real-time using Supervisory Control and Data Acquisition (SCADA), including their associated data centers, and excluding field Cyber Assets used for telemetry.

NERC Glossary of Terms

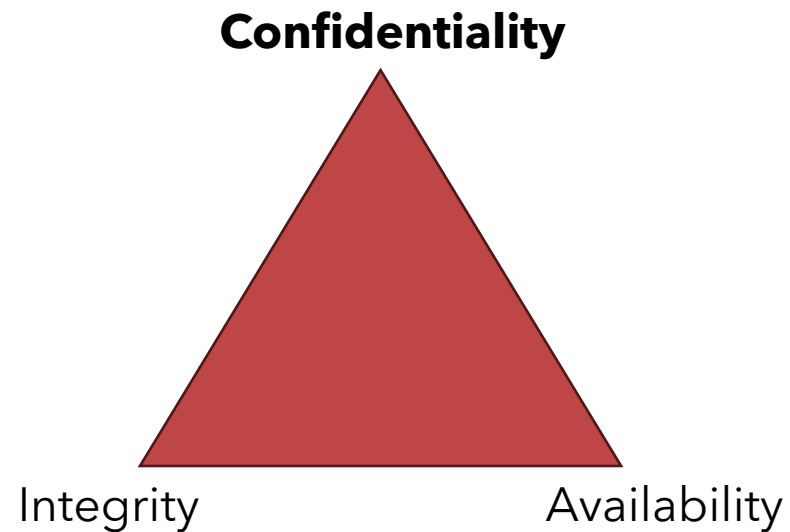
Project 2021-03 CIP-002



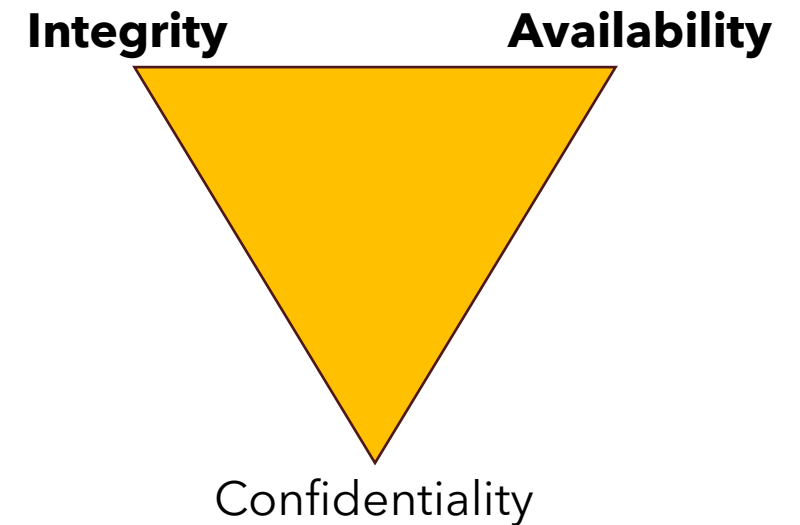
** Keep an eye on this!!

GENERAL CYBER SECURITY PRINCIPALS

IT Cyber Security Triad



OT Cyber Security Triad

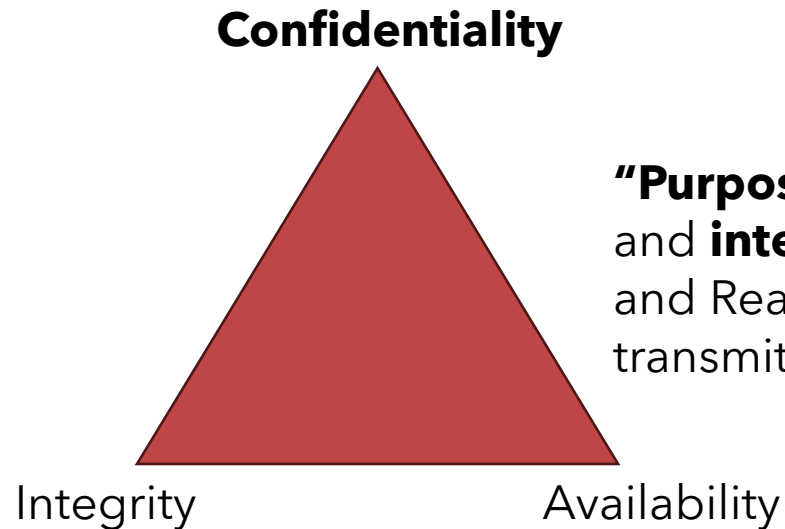


CIP-012-1 VS CIP-012-2

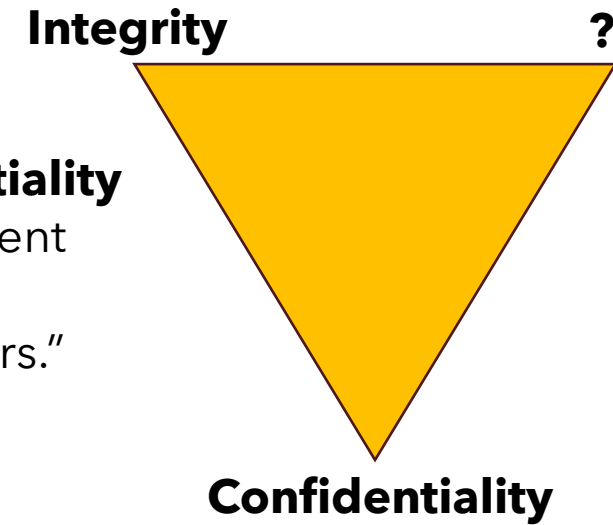
IT Cyber Security Triad

CIP-012-1

OT Cyber Security Triad



"Purpose: To protect the **confidentiality** and **integrity** of Real-time Assessment and Real-time monitoring data transmitted between Control Centers."



Note.... Availability of redundant and diversely routed data exchanges is also addressed in TOP-001. However CIP-012-2 goes a bit further.

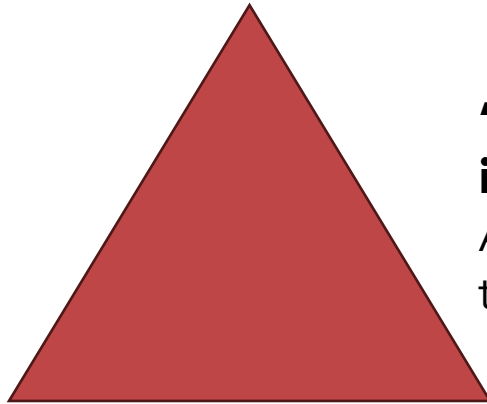
CIP-012-1 VS CIP-012-2

IT Cyber Security Triad

CIP-012-2

OT Cyber Security Triad

Confidentiality



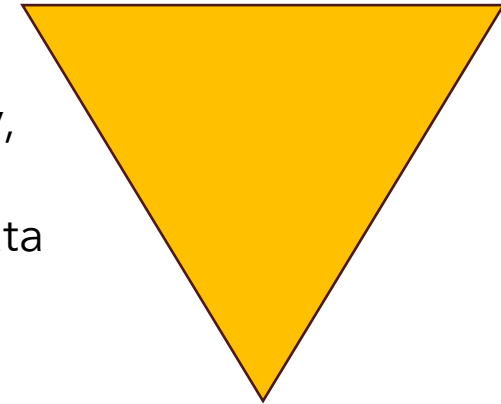
Integrity

Availability

"Purpose: To protect the **confidentiality**, **integrity**, and **availability** of Real-time Assessment and Real-time monitoring data transmitted between Control Centers."

Integrity

Availability



Confidentiality

WHAT DO I NEED TO DO IN CIP-012-1?

First you **Must** have a Plan...

"R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include:"

CIP-012-1

WHAT DO I NEED TO DO IN CIP-012-1?

You then **MUST** do the following:

"**1.1.** Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers; "

"**1.2.** Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and"

"**1.3.** If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers."

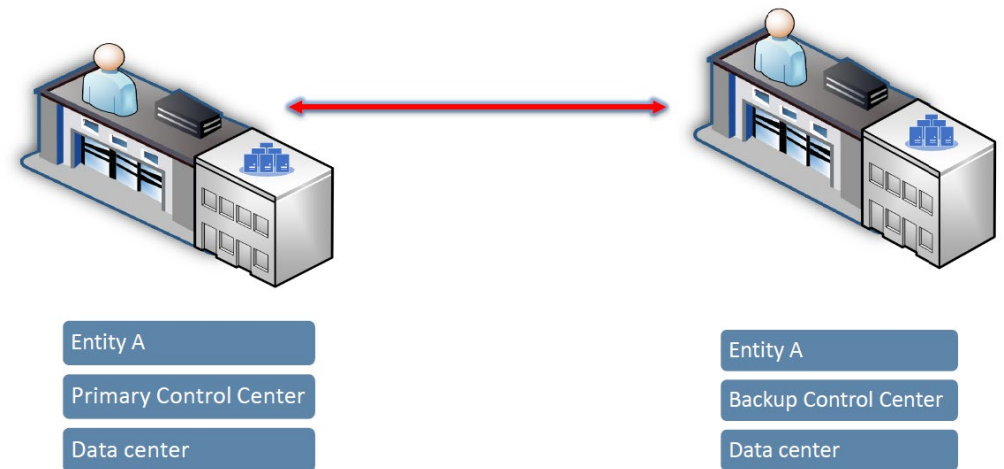
CIP-012-1

COMMON TOPOLOGIES WHERE YOU MAY FIND RTA/RTM

Let's take a look at some common examples used by registered entities where Real-time Assessment and Real-time monitoring data (RTA/RTM) is being transmitted between Control Centers.

In this first diagram we see a traditional Primary/Backup Control Center layout where each Control Center has its own data center. If the red communication link supports the transmission of RTA/RTM data (highly likely) then that link will be in scope for CIP-012.

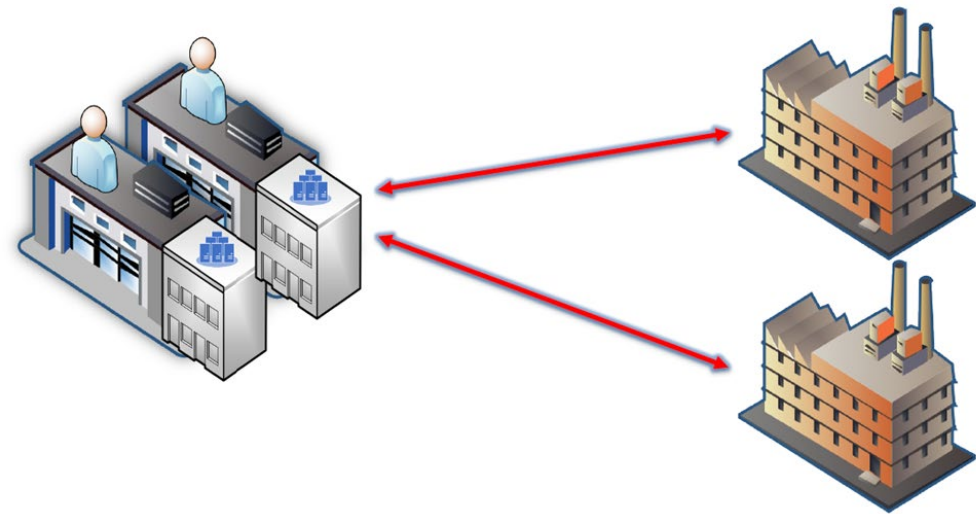
Between Primary and Backup Control Centers



COMMON TOPOLOGIES WHERE YOU MAY FIND RTA/RTM

Between Control Centers and BES Facilities

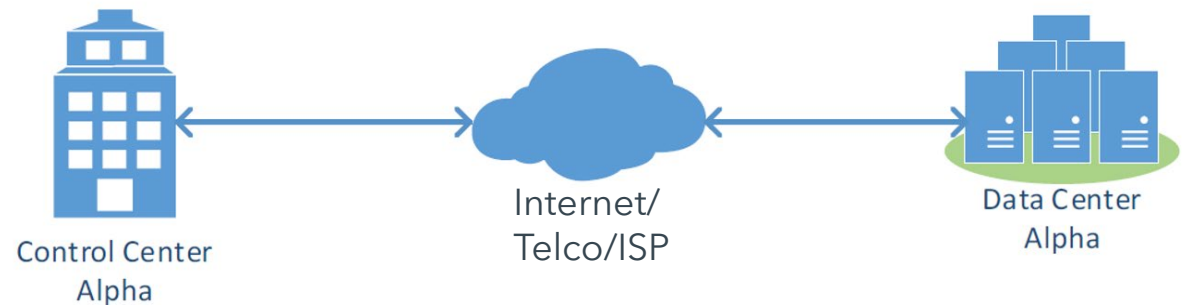
- In this next example two Control Centers are communicating with BES facilities, and if the data being transmitted is RTA/RTM data then both red communication links will be in scope for CIP-012.



COMMON TOPOLOGIES WHERE YOU MAY FIND RTA/RTM

Between Control Centers and BES Associated Data Centers

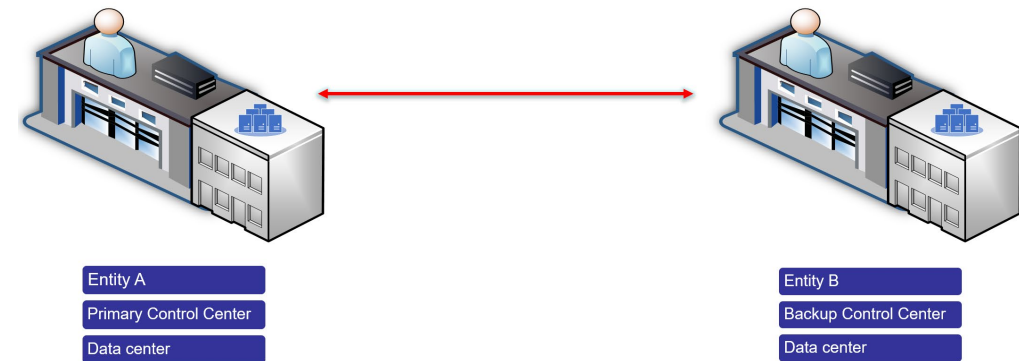
- What about a Control Center with an associated yet geographically separate data center? Again, it is almost certain that RTA/RTM data is being transmitted and as such the communications link must be protected.



COMMON TOPOLOGIES WHERE YOU MAY FIND RTA/RTM

Between two different Entities Control Centers and BES Associated Data Centers

- In many cases, two entities will be connected with a communications link to allow the transmission of RTA/RTM data. It is important to note that the responsibility for security protections lies with both registered entities and it is strongly encouraged that these two entities collaborate and share the protections with each other.



HOW DO WE PROTECT THE DATA/COMMUNICATION LINKS?

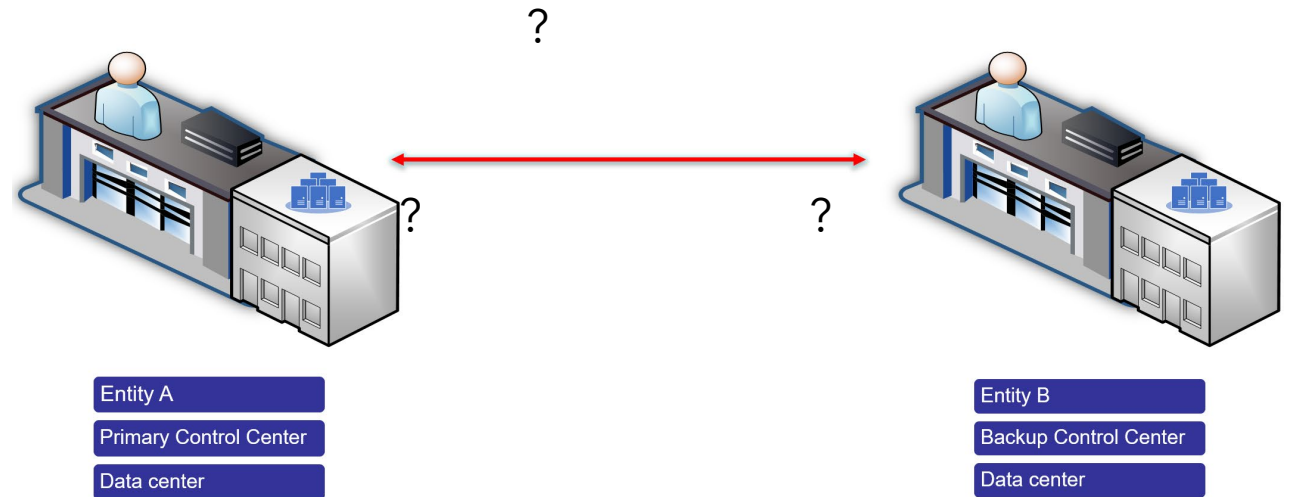
After identifying what we need to protect, we must identify how we will protect it.

- There are no mandated ways on how to protect it.
- Two common ways:
 - Physical Protection
 - Physical Access Control (for endpoint devices)
 - Conduit (for physical data links)
 - Logical Protection
 - Encryption (could be the data itself or encryption for the data links)

WHOSE LINE IS THIS ANYWAYS?

In 1.3, if you are sharing a data link you will need to have agreements of how you and the other entity will be protecting the data and data link.

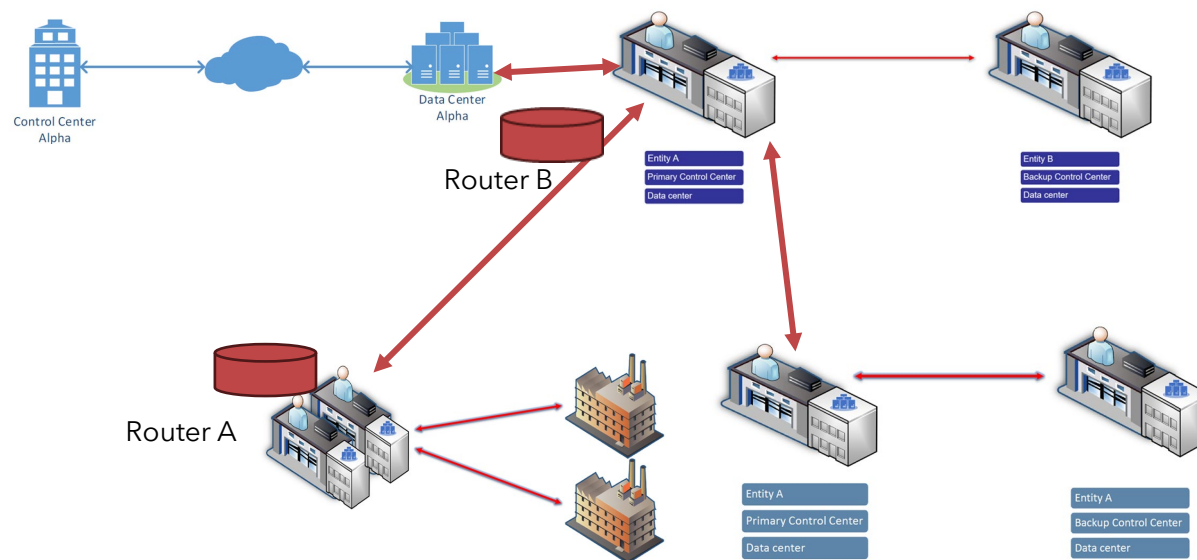
- Make sure to agree on who will be managing the devices that control the data and data link.
- You **must** document who is responsible for what



A PICTURE IS WORTH A THOUSAND WORDS

You will likely need to have 1 or more diagrams to help communicate and demonstrate the data protections

- **Must** document what your controls are, what is being implemented for your environment, and identifying what your organization is responsible for
- Could have multiple diagrams to help communicate different security protections
- Other documentation could be configurations and agreements.



CHANGES IN CIP-012-2?

- R1.** "The Responsible Entity is not required to include oral communications in its plan."
- 1.3.** "Identification of method(s) used to initiate the recovery of communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers; "
- 1.4.** "Identification of where the Responsible Entity implemented method(s) as required in Parts 1.1 and 1.2;"

CIP-012-2

PART 4 2:45-4:45

CIP-012 - DAVE

CIP-014 - CHRIS

FUTURE STATE - -10,-11,-12, CATEGORY 2 -
CHRIS

QUALITY EVIDENCE/RSAW/ERT - LEW

CLOUD - LEW

WRAP-UP - REFERENCES, WEBINARS

WHAT ABOUT CIP-014?

- CIP-014 Applies to Transmission Owners and Transmission Operators ONLY
- TOs must assess their BES assets according to the CIP-002 criteria in Attachment 1
- The applicability parts in CIP-014 directly match the criteria 2.4, 2.5, 2.6, and 2.7 in CIP-002*
- *HOWEVER*: CIP-014 has nothing to do with cyber assets!
 - You can have a substation with no cyber assets that can be in scope for CIP-014



APPLICABILITY CRITERIA

CIP-014

- 4.1.1** Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:
- 4.1.1.1** Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.
 - 4.1.1.2** Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.
- | Voltage Value of a Line | Weight Value per Line |
|-----------------------------------|-----------------------|
| less than 200 kV (not applicable) | (not applicable) |
| 200 kV to 299 kV | 700 |
| 300 kV to 499 kV | 1300 |
| 500 kV and above | 0 |
- 4.1.1.3** Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
 - 4.1.1.4** Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
- 4.1.2** Transmission Operator.

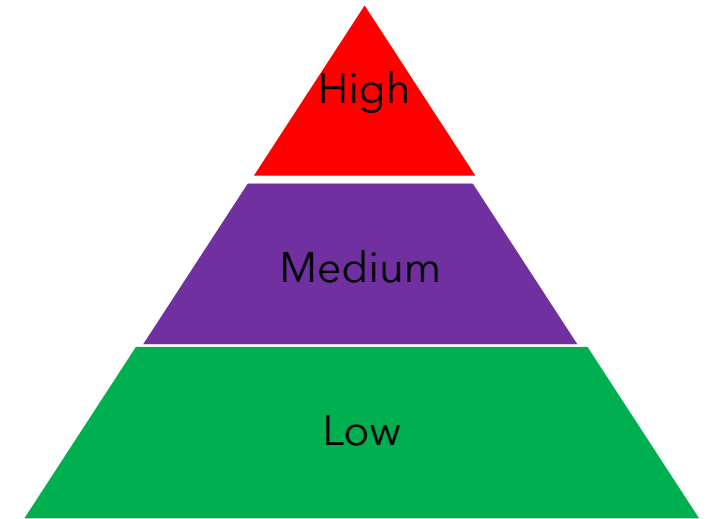


CIP-002

- 2.4.** Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.
 - 2.5.** Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.
- | Voltage Value of a Line | Weight Value per Line |
|-----------------------------------|-----------------------|
| less than 200 kV (not applicable) | (not applicable) |
| 200 kV to 299 kV | 700 |
| 300 kV to 499 kV | 1300 |
| 500 kV and above | 0 |
- 2.6.** Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.
 - 2.7.** Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

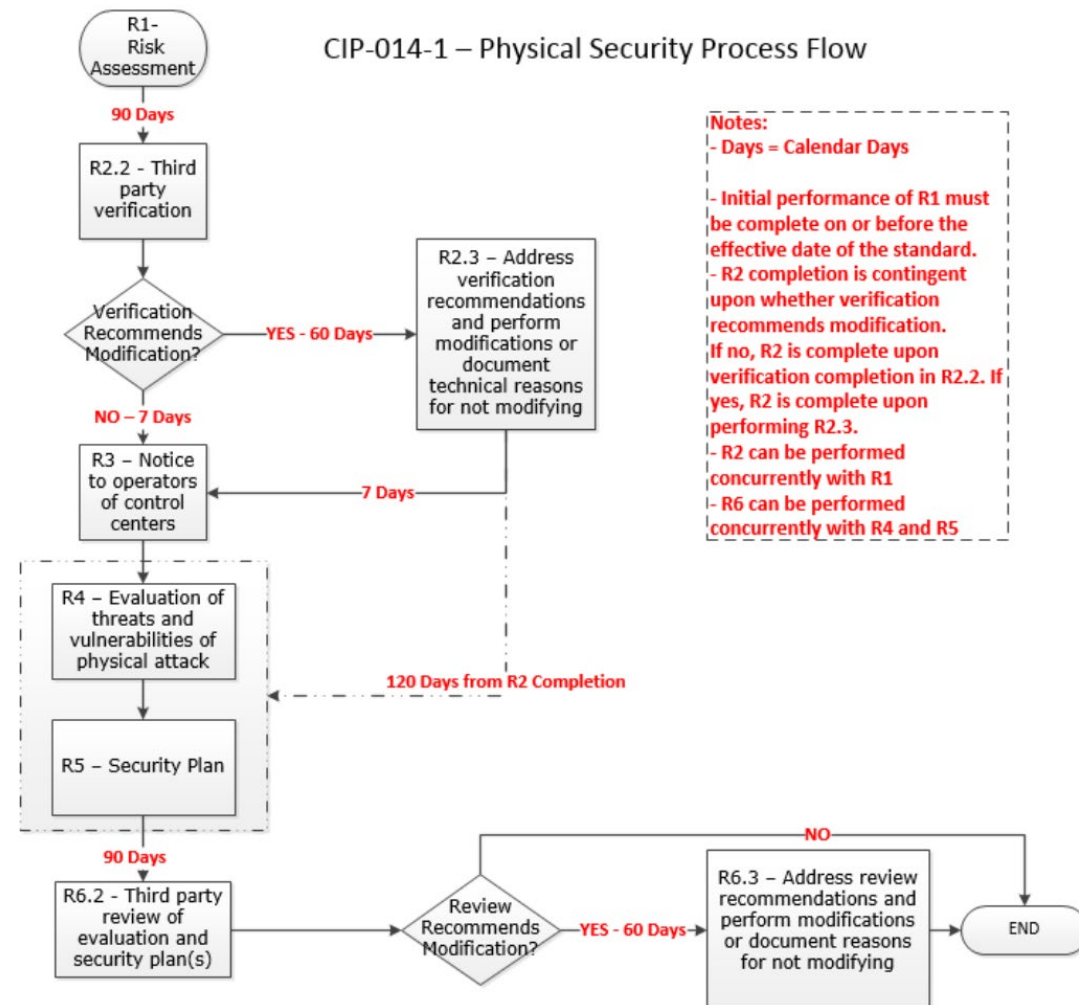
EXPECTATIONS?

- Use your CIP-002 assessment as reference
- But remember, CIP-014 has nothing to do with cyber assets!
- Determine if you have any assets that meet the CIP-014 criteria
- If none, document that you have no assets that fall under the applicability criteria for CIP-014
- TO's should have a control to make sure the list stays accurate
- TOPs should have controls to respond to call from TOs if their control center is identified by a TO



TIMING IS EVERYTHING

Timeline



- CIP-014 has many timing issues that can be tricky
- Use the process flow chart in the standard!
- Pay attention to triggers

PART 4 2:45-4:45

CIP-012 - DAVE

CIP-014 - CHRIS

**FUTURE STATE - -10,-11,-12, CATEGORY 2 -
CHRIS**

QUALITY EVIDENCE/RSAW/ERT - LEW

CLOUD - LEW

WRAP-UP - REFERENCES, WEBINARS

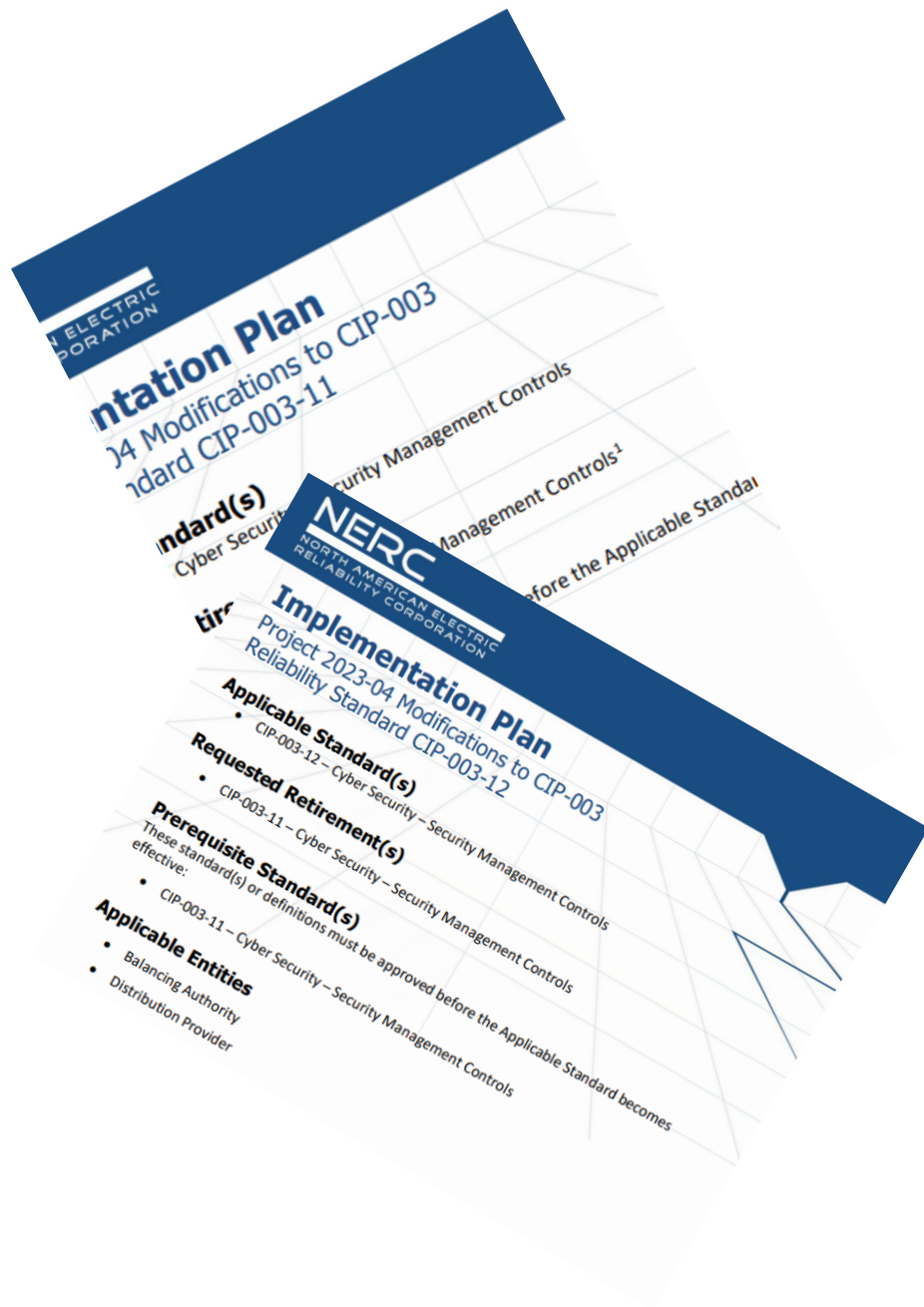


Slido Questions!!!

How many versions of CIP-003 are in development past version 8

**Join at
slido.com
#2071 9698
Passcode:
tzy1n4**





WHAT'S THE DEAL WITH CIP-003?

TODAY - VERSION 8

SECURITY POLICY

- Establishing Management Buy-In and involvement (*Policies, processes, plans, procedures*)
- State how you take security seriously
- There is an expectation of a compliance program document that sets the tone of a strong culture of compliance
- This includes a section for Low Impact Assets

CIP-003-8 LOW IMPACT REQUIREMENTS

CIP-003-8 has **specific** requirements to protect Low Impact BES Cyber Systems and requires that Registered Entities develop one or more security plans that address each of these risk areas detailed in **Attachment 1**:

- Section 1. Cyber Security Awareness
- Section 2. Physical Security Controls
- Section 3. Electronic Access Controls
- Section 4. Cyber Security Incident Response
- Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation

Additionally, **requirement 1.2.6 requires** a plan for declaring and responding to CIP Exceptional Circumstances.

More details on developing your security plans coming later in this workshop.



The new standard, entitled Reliability Standard CIP-003-9, will require responsible entities to include the topic of "vendor electronic remote access security controls" in their cybersecurity policies and have methods for determining and disabling vendor electronic remote access (New Requirement: 1.2.6 and New Section 6 in Attachment 1).

1. Requires entities to include the topic of "vendor electronic remote access security controls" in their cyber security policies
2. Requires entities with assets containing low-impact BES cyber systems to have methods for determining and disabling vendor electronic remote access
3. Requires entities with assets containing low-impact BES cyber systems to have methods for detecting malicious communications for vendor electronic remote access

Why are there new versions on the horizon? (CIP-003-
10,11,12)

NERC assembled a cybersecurity team (LICRT - Low Impact Criteria Review Team) to study potential threats and risks posed by a coordinated cyber attack on **Low Impact BES Cyber Systems** and FERC issued an order to mitigate these risks.

*NERC Project page for the modifications:
[Project 2023-04 Modifications to CIP-003 \(nerc.com\)](#)*

*Tom Alrich article on CIP-003 changes:
[Are you confused about what's going on with NERC CIP-003? If not, you should be... | Energy Central](#)*

The evolution of CIP-003 from version 9 through version 12 reflects two parallel efforts to enhance cybersecurity for low impact BES Cyber Systems (BCS):

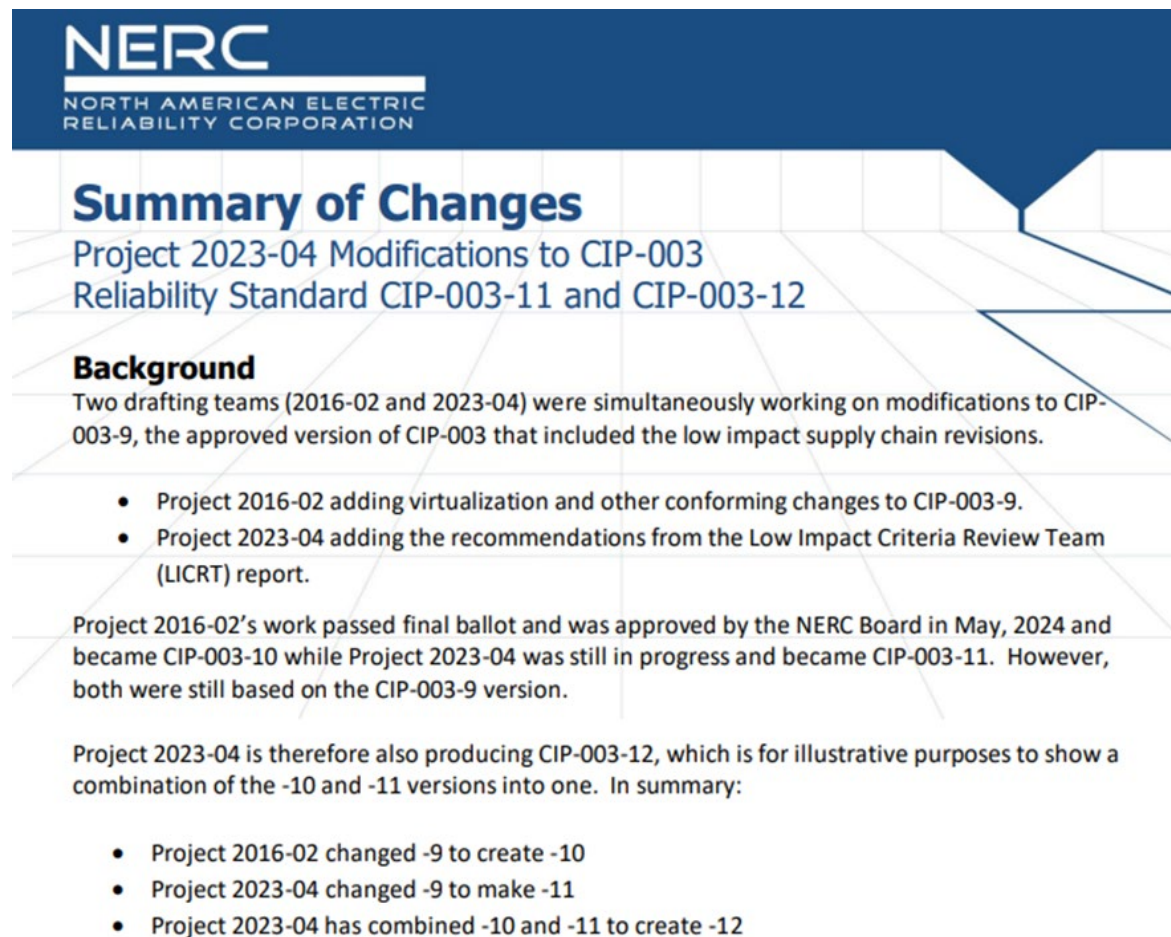
- **CIP-003-10** (Project 2016-02): Introduced support for virtualization by defining *Virtual Cyber Assets (VCA)* and *Shared Cyber Infrastructure (SCI)*. It also established the broader term *Cyber System* to encompass traditional Cyber Assets, VCAs, and SCI.
- **CIP-003-11** (Project 2023-04): Focused on refining criteria for low impact BCS based on the Low Impact Criteria Review Team's recommendations. It introduced SCI into Attachment 1, Section 3, clarifying that SCI supporting low impact BCS must meet the same access control requirements.
- **CIP-003-12**: A combined version integrating changes from both CIP-003-10 and CIP-003-11. It aligns terminology (e.g., consistent use of acronyms like BCS) and formally incorporates SCI and Cyber System definitions to support virtualization environments.

VERSIONS 10 TO 12 SUMMARY

- Virtual systems (like virtual machines) will be clearly supported and secured.
- Shared Cyber Infrastructure (SCI) must follow the same protections.
- New consistent terminology (e.g., 'Cyber System') makes the standard easier to follow.



NERC SUMMARY OF CHANGES DOCUMENT

The image shows the cover page of a NERC document titled "Summary of Changes". The NERC logo is at the top left. The title "Summary of Changes" is in a large, bold, blue font. Below it, the subtitle "Project 2023-04 Modifications to CIP-003 Reliability Standard CIP-003-11 and CIP-003-12" is in a smaller blue font. The background of the page features a stylized grid pattern with perspective lines. The word "Background" is in a bold black font, followed by a paragraph of text. Below this is a bulleted list of two items. Another paragraph follows, and then another bulleted list of three items. The text is all in a clean, sans-serif font.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Summary of Changes

Project 2023-04 Modifications to CIP-003 Reliability Standard CIP-003-11 and CIP-003-12

Background

Two drafting teams (2016-02 and 2023-04) were simultaneously working on modifications to CIP-003-9, the approved version of CIP-003 that included the low impact supply chain revisions.

- Project 2016-02 adding virtualization and other conforming changes to CIP-003-9.
- Project 2023-04 adding the recommendations from the Low Impact Criteria Review Team (LICRT) report.

Project 2016-02's work passed final ballot and was approved by the NERC Board in May, 2024 and became CIP-003-10 while Project 2023-04 was still in progress and became CIP-003-11. However, both were still based on the CIP-003-9 version.

Project 2023-04 is therefore also producing CIP-003-12, which is for illustrative purposes to show a combination of the -10 and -11 versions into one. In summary:

- Project 2016-02 changed -9 to create -10
- Project 2023-04 changed -9 to make -11
- Project 2023-04 has combined -10 and -11 to create -12

[2023-04 Summary of Changes V11-V12 061224.pdf \(nerc.com\)](#)

PART 4 2:45-4:45

CIP-012 - DAVE

CIP-014 - CHRIS

FUTURE STATE - -10,-11,-12, CATEGORY 2 -
CHRIS

QUALITY EVIDENCE/RSAW/ERT - LEW

CLOUD - LEW

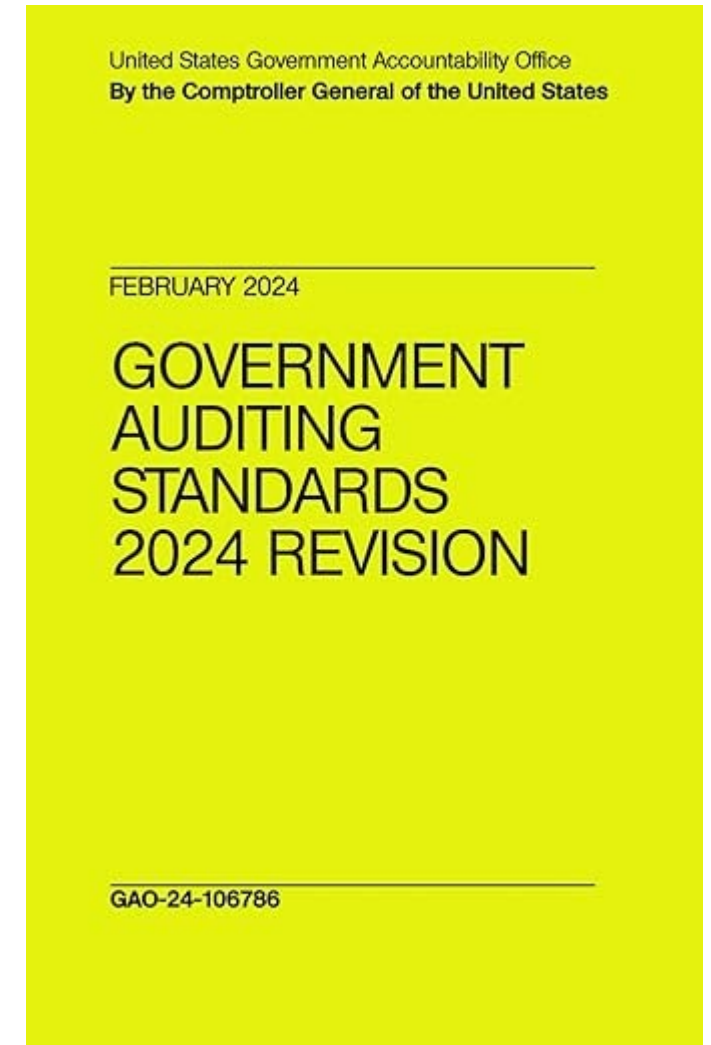
WRAP-UP - REFERENCES, WEBINARS

QUALITY EVIDENCE

- Evidence can be considered the culmination of your compliance program
 - Poor evidence can appear sloppy, haphazard, or incomplete - even when none of those words apply to your compliance program
 - Just as a resume is the summary of your career in a job interview, so your evidence is the summary of your compliance program
- Ideally, quality evidence submitted in advance to an audit team can greatly reduce or even eliminate the need for an on-site audit
- Conversely, poor evidence can lead to adverse audit findings, even if the underlying work has been done properly and on time

WHY EVIDENCE?

- Audit teams need to obtain *reasonable assurance* of your compliance with the Standards
- Reasonable assurance is obtained by examining *sufficient, appropriate evidence*
- Detailed in *Generally Accepted Government Auditing Standards*, available at: <http://www.gao.gov/yellowbook>



SUFFICIENT EVIDENCE

- Sufficiency is a measure of the quantity of evidence needed to support the audit findings
- Appropriateness is a measure of the quality of evidence
- These two characteristics are related: when evidence is of higher quality, a lesser quantity is needed to support the audit findings

APPROPRIATE EVIDENCE

- Relevant
 - Relevant evidence is evidence that has a direct relationship with the Reliability Standard and requirement being audited
- Valid
 - Valid evidence means the evidence is a meaningful measure of the tasks performed to achieve compliance with the subject being audited
- Reliable
 - Reliable evidence refers to the consistency of evidence in demonstrating compliance

TYPES OF EVIDENCE

- Physical
 - Physical evidence is obtained by direct observation by the audit team. This could be a walkthrough of a physical facility. It might also be a live demonstration of a real-time capability such as response to an alarm.
- Testimonial
 - Testimonial evidence is generally only used at a compliance audit for attestations and is considered the weakest form of evidence. Usually, an attestation will be used to document a negative, such as having no Reportable Cyber Security Incidents. Your subject matter experts (SMEs) may be interviewed by the audit team to explain the documentary evidence, but they will not be delivering sworn testimony.
- Documentary
 - Documentary evidence may be written policies, plans, processes, procedures, or other types of documents. It may also be evidence that a task has been carried out.

CHEAT SHEET 1

Questions your documentary evidence should answer:

Is the document credible?

What task was performed?

Who performed the task?

Why was the task performed?

Which assets were affected by the task?

When was the task performed?

Who authorized the task?

What was the state of the asset before the task was performed?

What was the state of the asset after the task was performed?

Was the result of the task reviewed, and if so, when and by whom?

Jane Smith is hereby designated as the CIP Senior Manager.

WEAK EVIDENCE



QUALITY EVIDENCE

Designation of CIP Senior Manager

9/19/2023

Jane Smith, Vice President of Operations, is hereby designated as the CIP Senior Manager for Nosuch Generation, LLC, NCR98765, effective September 19, 2023.

Signed,

R. C. Lincoln

R. C. Lincoln, CEO

NOSUCH GENERATION,
LLC

123 Any Street
Nosuch City, MI 49999

Phone: 999-999-9999
E-mail:
rcl@nosuchgeneration.com

CHEAT SHEET 2A

Low Folkerth's advice for keeping consistent quality for various types of documents you might use as evidence:

Document	Evidence
Policies, plans, processes, and procedures	Develop a standard template for this type of document that includes the document title, document revision number and date, company name or logo, applicable NCR numbers if you have multiple registrations, the person or group responsible for the document content, and the person, group or asset type the document applies to. Keep detailed revision histories and effective dates for each version of the document. For cyber security policies per CIP-003, make sure the CIP Senior Manager's approval of each policy is clear and accompanied by the date of approval.
Periodic actions, such as asset list reviews	Dated documentation of actions performed is particularly important for periodic requirements. Ensure your documents clearly identify the action taken and the resulting changes, if any.

CHEAT SHEET 2B

Low Folkerth’s advice for keeping consistent quality for various types of documents you might use as evidence:

Document	Evidence
Event-triggered actions, such as incident response	Some of the CIP Standards require action based on a triggering event, such as incident response to a Cyber Security Incident, or a malware check for a Transient Cyber Asset. For these types of actions, I recommend that you use a checklist to ensure each required step of the applicable process or plan is performed. The checklist, when appropriately completed, signed, and dated, becomes your evidence of implementing the steps in your process or plan.
Ongoing actions, such as access control	For ongoing actions, such as managing a firewall ruleset to control electronic access to a Bulk Electric System asset, I suggest using a combination of change control and periodic review. The change control process will ensure that access control is not compromised by an unauthorized change, and the completed change control tickets will document this ongoing effort. The periodic review will ensure that old information is purged and current information is adequately documented.

CHEAT SHEET 2C

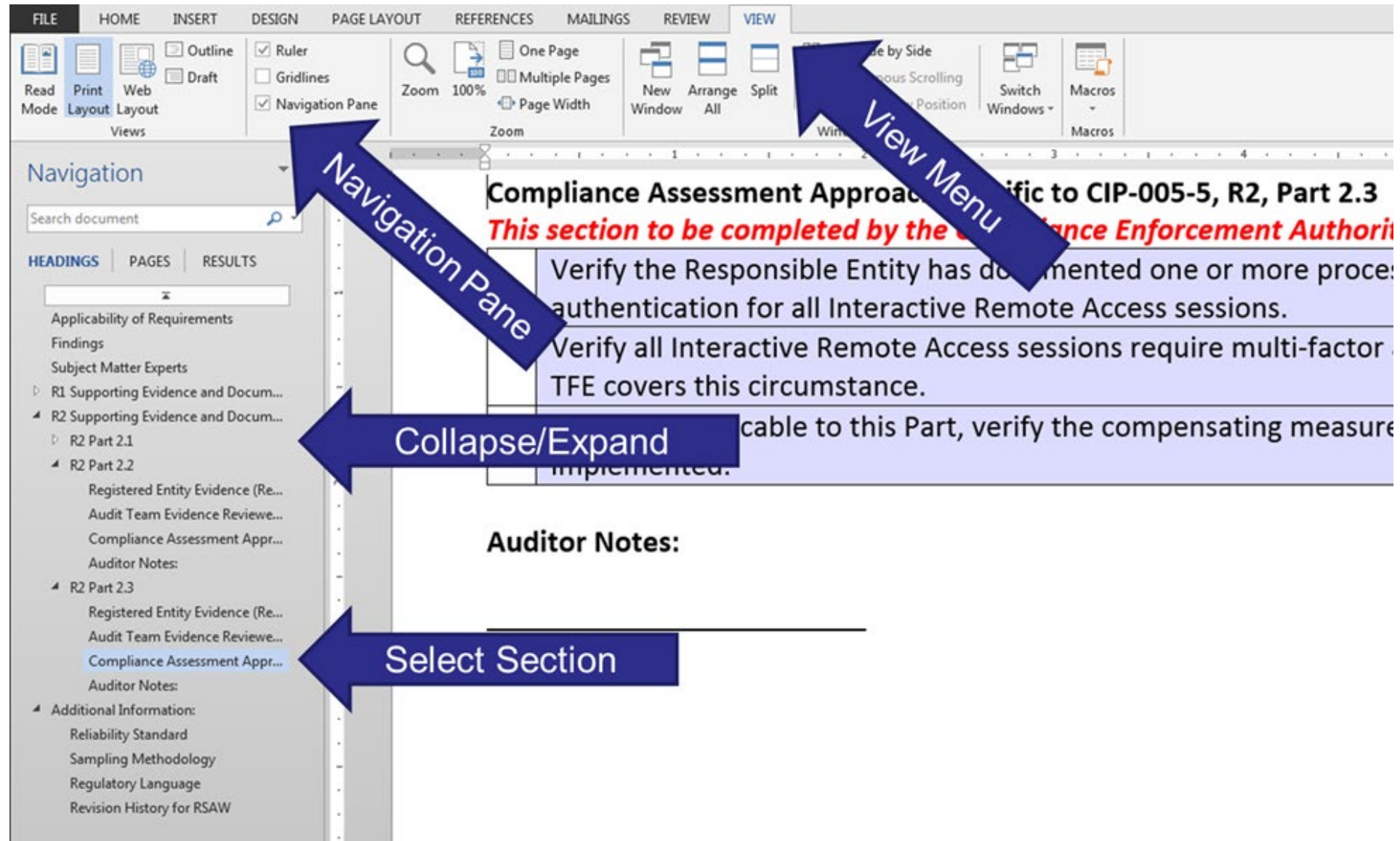
Low Folkerth's advice for keeping consistent quality for various types of documents you might use as evidence:

Document	Evidence
General considerations	All documentary evidence should identify your company, should carry a date, and should be page numbered to show that the document is complete, and no pages are missing.

RSAWS

- The Role of the RSAW
 - Organizes transmittal of evidence and compliance approach to the audit team
 - Record keeping tool for the audit team

RSAWS



EVIDENCE REQUEST TOOL

	A	B	C	D	
1					
2	Detail Tab or Request ID ▾	Standard ▾	Requirement ▾	Evidence Request ▾	
3	BES Assets	CIP-002 CIP-003 CIP-012		Provide a listing of all BES assets, of a type listed in the Asset Type field, in service during the audit period for which you have or share compliance responsibility by using the BES Assets tab of this spreadsheet. Include data center(s) associated with each Control Center.	,ERT
4	CA	CIP-002 CIP-005 CIP-006 CIP-007 CIP-010		Provide a listing of all Cyber Assets that are included in or associated with a high or medium impact BES Cyber System on the CA tab of this spreadsheet, ensure to include VMs and their associated host or cluster.	,ERT
5	Low CA	CIP-002		Provide evidence of BES Cyber Assets that are included in or associated with low impact BES Cyber System, one-line diagrams, network configuration files, or other documentation. The Low CA tab of this spreadsheet is included for those entities that have chosen to have a list. This tab is NOT MANDATORY and is ONLY OPTIONAL .	,ERT
	Personnel	CIP-004		Provide a complete listing of individuals who are currently, or have been at any time during the audit period, authorized for: 1. electronic access; 2. unescorted physical access; 3. provisioned access to BCSL whether physical or electronic, for BCSL using the Personnel	,ERT

EVIDENCE REQUEST TOOL

	A	B	E	F	G	H	I	J	K
1	CONFIDENTIAL								
2						Contains BES Cyber System			
3	Index ▾	BES Asset ID ▾	Commission Date ▾	Decommission Date ▾	Location ▾	High Impact ▾	Medium Impact ▾	Low Impact ▾	Accessible Via a Routable Protocol - Low Impact ▾
4	1								
5	2								
6	3								
7	4								
8	5								
9	6								
10	7								
11	8								
12	9								
13	10								

< >

Instructions

Level 1

Sample Sets L2

Level 2

Sample Sets Table

BES Assets

CA

⋮

+

⋮

◀ ▶

PART 4 2:45-4:45

CIP-012 - DAVE

CIP-014 - CHRIS

FUTURE STATE - -10,-11,-12, CATEGORY 2 -
CHRIS

QUALITY EVIDENCE/RSAW/ERT - LEW

CLOUD - LEW

WRAP-UP - REFERENCES, WEBINARS

POTENTIAL CLOUD DRIVERS FOR OT

Safety – Keep people and equipment from harm

Reliability – Not letting problems happen

- Geographic diversity

- Multiplicity of physical hardware, data centers, regions

Resilience – Recovering swiftly and smoothly if problems occur

- Not all eggs in one basket – or even two baskets¹

- Multi-cloud failover – Infrastructure as Code permits creation of an entire data center in seconds or minutes

Ukrenergo: we couldn't survive without the cloud

December 12, 2022 | CEE Multi-Country News Center



¹<https://news.microsoft.com/en-cee/2022/12/12/ukrenergo-we-couldnt-survive-without-the-cloud/>

POTENTIAL CLOUD DRIVERS FOR OT

Security - Ensuring availability, integrity and confidentiality

Data centers become a less attractive target

CSP provides physical and basic network security

Elasticity/Scalability - The ability to enhance available resources on demand

Adjust resource usage based on need - expand for peaks, then contract

Flexibility - Access to new technologies as they become available to the industry

Staffing - Use of cloud services can enable entity skilled staff to focus on the most important aspects of their jobs

Preparing for the future - existing services (work management, network monitoring, etc.) are moving (or have moved) their primary, most feature-rich, versions to cloud-only services - will this eventually happen to SCADA, etc.?

CLOUD CHALLENGES FOR OT

Operational Challenges

Safety

Availability

Focus of cloud is on capability and cost, not high availability

Latency

Measure of the delay from data generation to data consumption

Mobile Access

Cloud services are easily accessed from mobile devices - this is a problem for Control Centers and other CIP assets

CLOUD CHALLENGES FOR OT

Financial Challenges

- On-premise systems - capital

- Cloud - operating

Security Challenges

- Cyber

 - Shared infrastructure - data leakage

 - Public exposure of information or services

 - Data sovereignty - privacy laws

- Physical

 - How to ensure cloud services clients reside only within a PSP?

EMP/GMD Hardening

- Are cloud providers prepared for these events?

CLOUD CHALLENGES FOR OT

Compliance Challenges

- New standards will be required

- Risk-based standards will be required

- Requires a mature approach to Standards

 - Can't get by with a letter-of-the-law approach

 - Must have compliance fully integrated into operational processes

- Auditing concerns

 - Reasonable assurance

 - Sufficient, appropriate evidence

- Internal controls will be much more important

THE PRESENT DILEMMA

Present CIP standards are device based

Cloud offerings are service-based

BCSI issue - cloud admins can access everything

Availability

Data sovereignty (Data geography)

Resource aggregation under one supplier

Jurisdiction - can't audit CSPs

THE PATH FORWARD

Project 2023-09 Drafting Team

New standards will be **voluntary** - no one will be forced into the cloud

Current standards had to accommodate existing architectures

New standards are in a position to guide security architecture

Possible architectures

- Various vendor "Well Architected Framework" documents

- Zero Trust Architecture

- NIST CSF

- Etc.

THE PATH FORWARD

Project 2023-09 Drafting Team

Building the next evolution of the CIP Standards

Determine the appropriate baseline for cloud environments

Accommodate future technologies – quantum, AI, and beyond

PART 4 2:45-4:45

CIP-012 - DAVE

CIP-014 - CHRIS

FUTURE STATE - -10,-11,-12, CATEGORY 2 -
CHRIS

QUALITY EVIDENCE/RSAW/ERT - LEW

CLOUD - LEW

WRAP-UP - REFERENCES, WEBINARS

REFERENCES

View on mobile



<https://linktr.ee/RFLowImpact>



QUESTIONS & ANSWERS



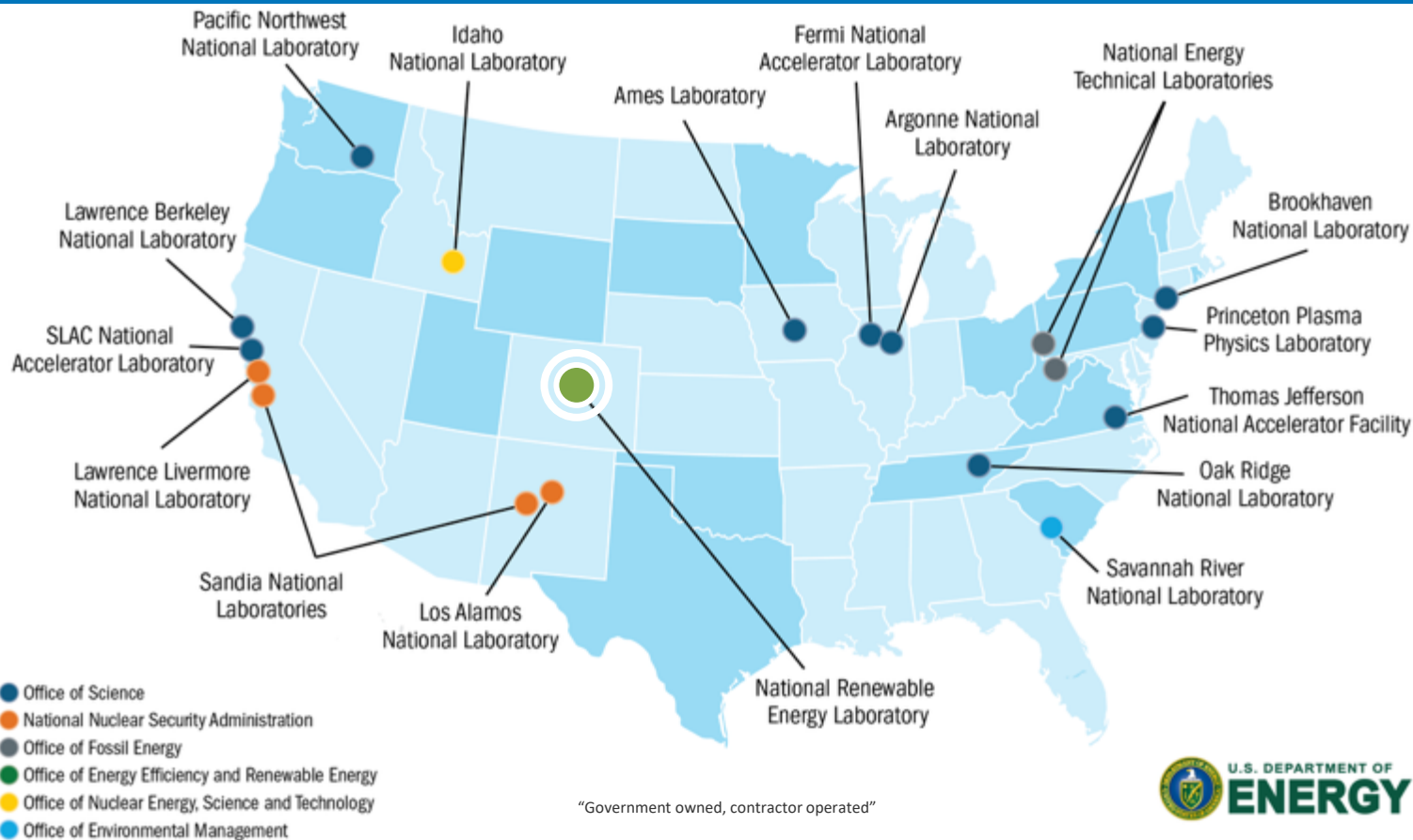
Cyber-Physical Challenges and Opportunities for Securing Inverter-Based Resources

Tami Reynolds

Reliability First Critical Infrastructure
Protection Committee Workshop

Aug. 20, 2025

17 U.S. Department of Energy National Laboratories



NREL at-a-Glance



3,185

Workforce

Including:

- 188 postdoctoral researchers
- 130 graduate students
- 73 undergraduate students



World-Class

research expertise in
renewable power, energy
efficiency, sustainable
transportation, and energy
systems integration

More than
1,000

Partnerships

with industry,
academia, and
government



3 Campuses

operate as
living laboratories

NREL's Energy Security Heritage

Energy and broader national security concerns drove the National Renewable Energy Laboratory's (NREL) founding as the Solar Energy Research Institute in 1977, in response to the economic shock of the 1973 oil crisis.



David Falconer / EPA / US National Archives

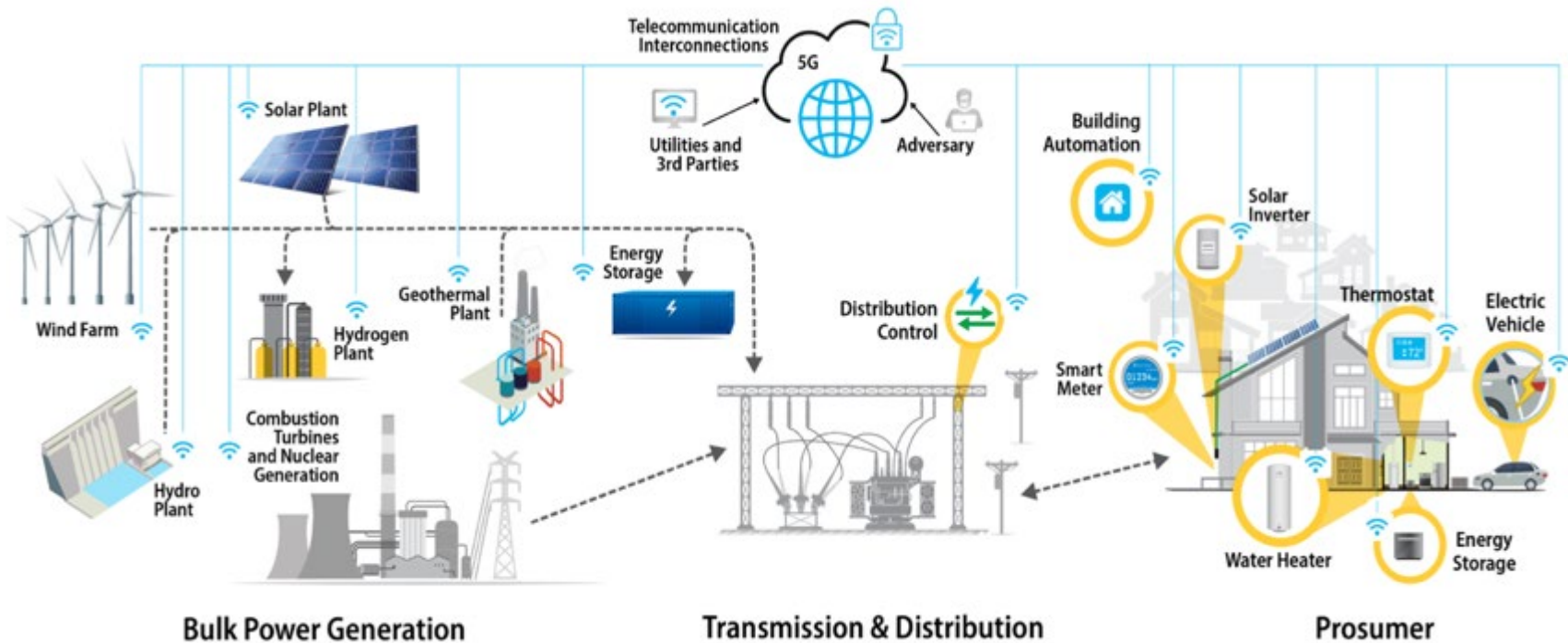


A Secure and Resilient Clean Energy Future

The energy
transformation
is secure and
resilient by
design.



The energy
transformation
creates a more
secure and
resilient world.



A New Frontier:

The grid is evolving to become more distributed, intelligent, and complex.


Coupled with aging infrastructure, the risks of emerging energy systems to disruption are not yet well understood.

Cybersecurity for Inverter-Based Resources



Photo from iStock 1181551812

- Inverter-based resources are equipped with data-driven communications networks, making the grid more flexible, intelligent, and autonomous.
- However, like all grid components, these connections and the devices can carry cyber risks if not thoroughly vetted and secured.

An aerial photograph of a city, likely New York City, with a network of glowing blue and white lines overlaid, representing a smart grid or data network. The lines connect various points across the city, including buildings and parks.

Rapid increase
in the quantity
and diversity of
connected
devices

Loss of exclusive
ownership of
utility OT and IT
systems
necessary for
grid monitoring
and control

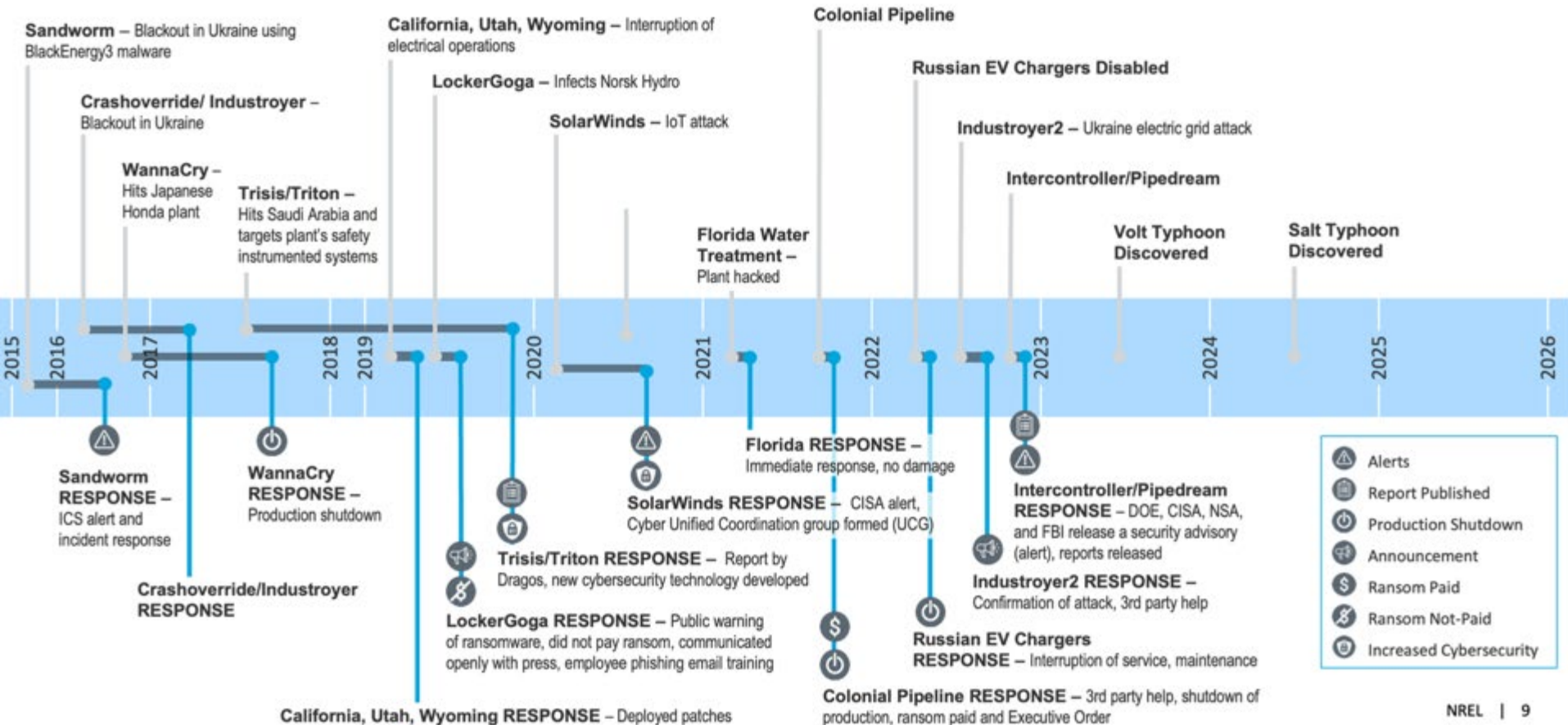
Less tractable
supply chains
impacts trust in
edge devices
and services

Legacy and
current
solutions not
prepared for
technology and
threat
revolutions

Energy System Grand Challenges

With deep expertise in the design, integration, and operation of advanced energy system technologies, NREL is equipped to address these challenges as the grid continues to evolve in becoming increasingly modern, autonomous, and complex.

Examples of Recent Cyber Events



Cyberattacks Can Cause **Physical** Consequences

Threats:

87% more ransomware attacks against industrial organizations *(compared to previous year)*.

60% more ransomware groups impacting OT/ICS in 2024.

Vulnerabilities:

70% of vulnerabilities reside deep within the network.

22% of advisories were network exploitable and perimeter facing in 2024.



Image from Dragos OT/ICS Cybersecurity Report 2025

Cybersecurity Risk Quantification, Management, and Governance

Defining Terms



Risk Quantification assigns numeric values to impact and likelihood using statistical probabilities and monetarized valuation of loss or gain



Risk Management includes conducting risk assessments, implementing mitigation strategies, and employing continuous monitoring techniques



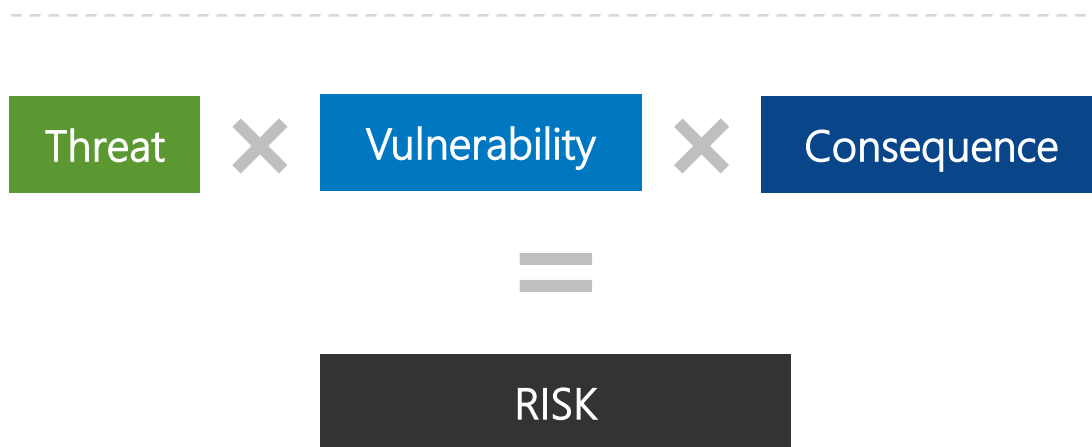
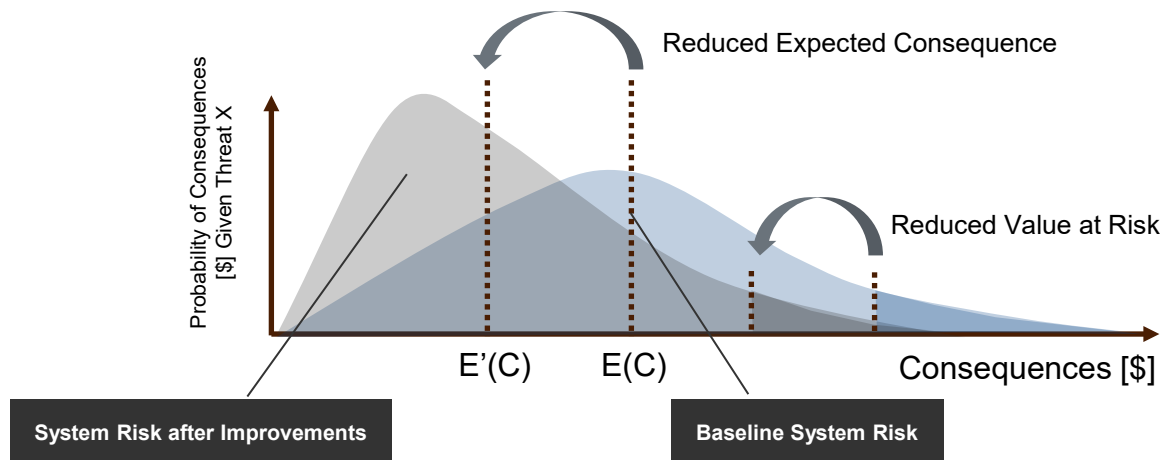
Governance is the process by which risk management evaluation, decisions, and actions are connected to enterprise strategy and objectives

Measuring Risk

Threat: What is the likelihood of threats?

Vulnerability: When the grid is subject to the threat, how likely are systems to be significantly compromised?

Consequence: When systems are compromised, what are the consequences to various entities?



Measuring and Reducing Risk

To effectively quantify and manage risk,

UTILITIES MUST UNDERSTAND:

- ✓ **Cyber** and **physical** threats to their systems
- ✓ The **robustness** of their systems against threats (i.e., cybersecurity posture)
- ✓ Their **risk tolerance**



Risk Quantification Enables Better Decision Making

- Prioritization of risk
- Investments in risk mitigation (e.g., training, assessments)
- Cost-benefit analysis
- Insurance (i.e., transfer of risk)

What is cybersecurity governance?

“The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.”

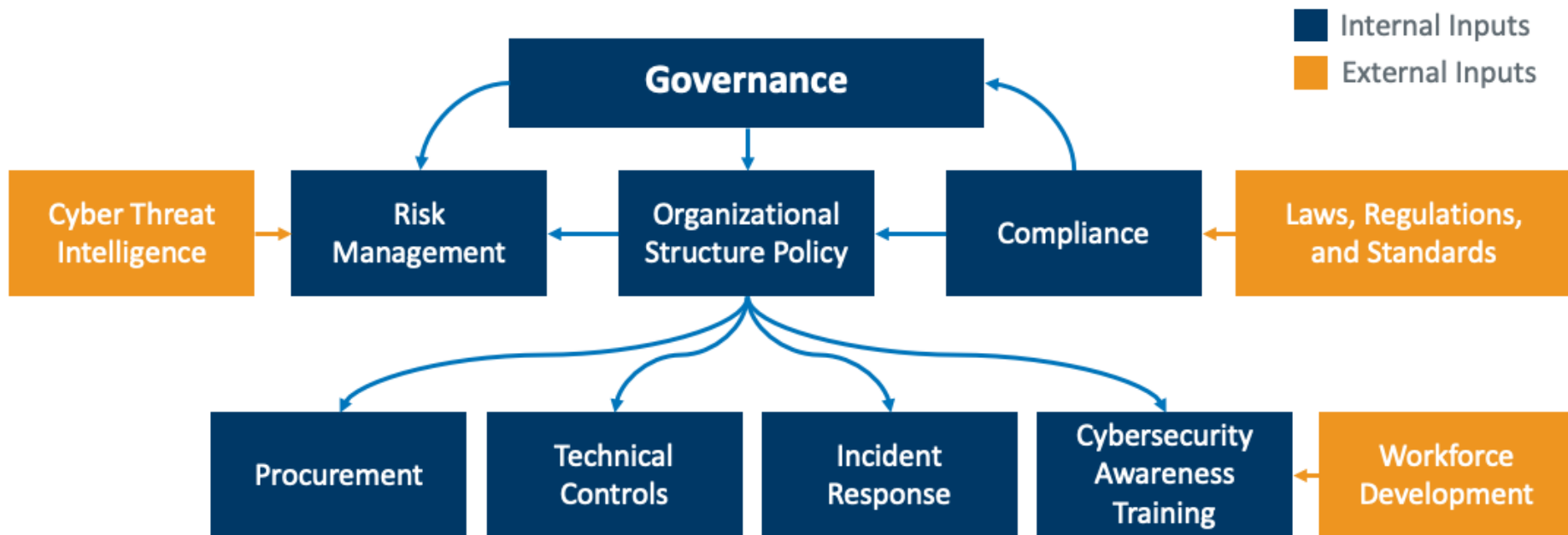
NIST Framework for Improving Critical Infrastructure Cybersecurity



Importance of Cyber Governance

Cybersecurity governance helps an organization:

- Detect, prevent, and respond to cyber incidents
- Reduce potentially costly risk exposure
- Make informed decisions based on comprehensive frameworks.



Cybersecurity Governance

Distributed Energy Resource Cybersecurity Framework



Photo from iStock 873055760

Funded by DOE's Federal Energy Management Program, the **Distributed Energy Resource Cybersecurity Framework (DER-CF)** helps organizations mitigate gaps in their cybersecurity posture for distributed energy systems.



OVERVIEW

- Free, web-based tool for evaluating cybersecurity posture of sites with IBRs
- User-focused assessments
- Customized results and action items
- Tailored assessment to individual sites
- Baseline cyber posture and repeat assessments to benchmark progress

Assessing Three Key Areas for Cybersecurity



Governance



Technical Management



Physical Security



<https://dercf.nrel.gov>



Cyber Governance Security Assessment

Domains

- Risk Management
- Asset, Change, and Configuration
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Cybersecurity Architecture
- Incident Response
- External Dependency Management
- Cybersecurity Program Management



Cyber-Physical Technical Management Security Assessment

Domains

- Account Management
 - Authentication, authorization, and accounting
 - Role-based access control
 - Remote access
 - Monitoring and logging
- Configuration Management
 - Change management
 - Access control
 - System settings
 - Cloud security
- Systems/Device Management
 - Software integrity
 - Cryptography
 - System protections



Physical Security Assessment

Domains

- Administration Controls
 - Audits
 - Awareness training
 - System security testing
 - Operational management
 - Security plan
 - Secure data
- Physical Access Controls
 - Perimeter security
 - Building security
 - Lighting
 - Signage
 - Intrusion alarm/motion detector
- Technical Controls
 - Intrusion detection/prevention assets
 - Smart card/keying/badges
 - Sensor system/proximity reader/radio-frequency identification
 - Communication system
 - Closed-circuit television

Unique from Any Other Assessment Tool

The tool expands to
DERs, specifically:

- Solar
- Wind
- Electric vehicles
(charging stations)
- Buildings
- Storage

The DER-CF uses the following standards and/or frameworks:

- DOE C2M2
- NIST 800-53, 800-30, 800-82, CSF
- Department of Homeland Security Cyber Assessments of Industrial Control Systems (ICS)
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- International Electrotechnical Commission (IEC) 62351
- Executive Order 13800



Advanced Research on Integrated Energy Systems (ARIES) Cyber Range

A state-of-the-art physical and digital sandbox to assess real-world cyber threats to current and future energy infrastructure at scale.

Photos by Josh Bauer, NREL 59215; Bryan Bechtold, NREL 82063;
Getty Images 1661051950



ARIES Cyber Range



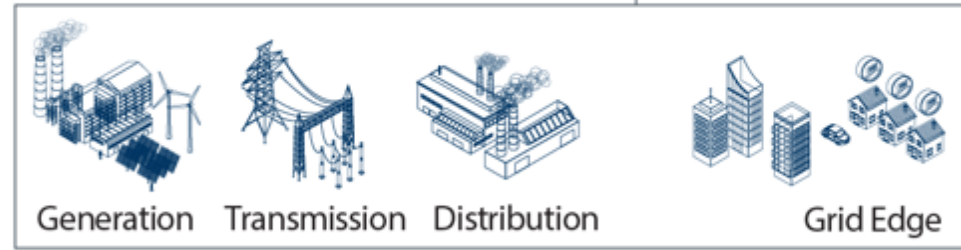
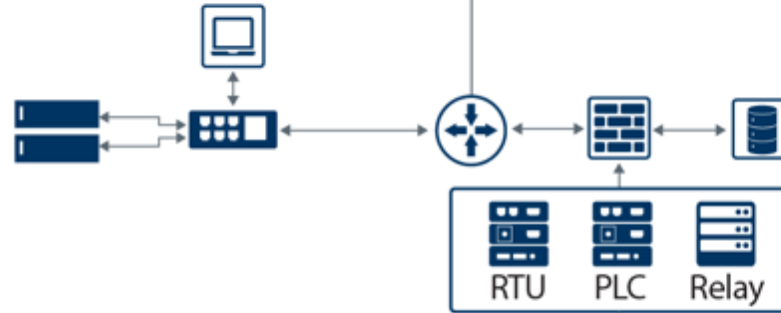
Automation and Orchestration

Hardware-in-the-Loop

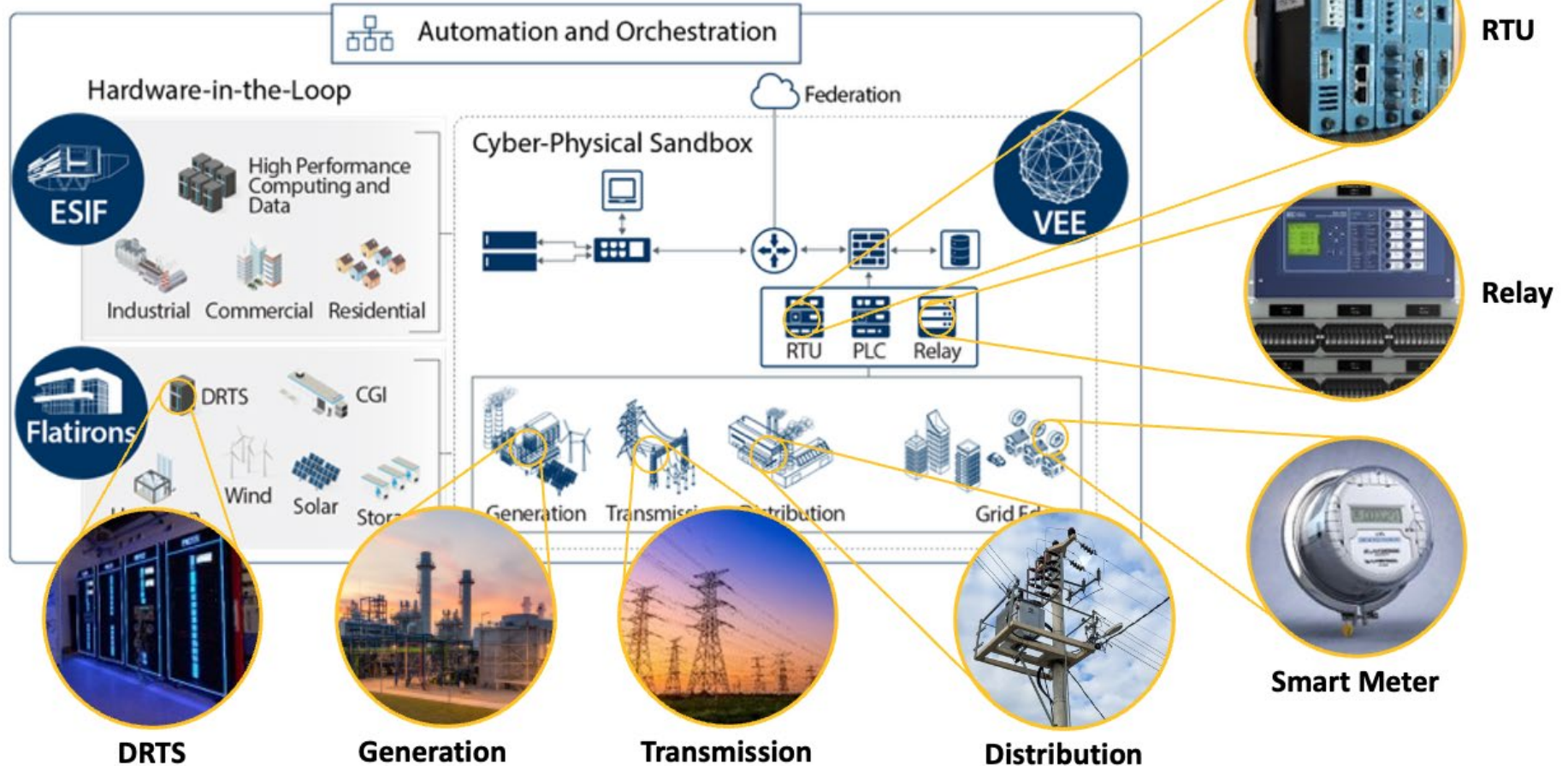


Federation

Cyber-Physical Sandbox



ARIES Cyber Range



A Unique, World-Class Capability

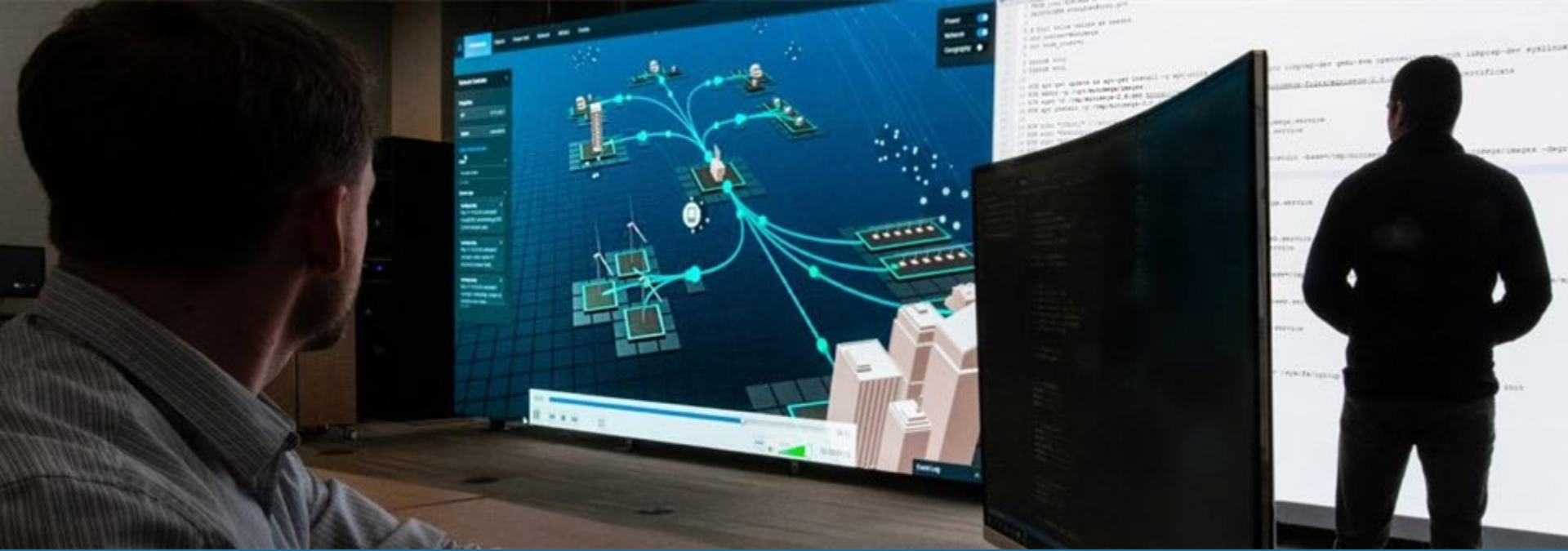
- Emulates **millions of diverse, distributed devices** in minutes
- Integrates **full-scale power system hardware** across ARIES
- Leverages **industry-validated**, high-fidelity reference architectures
- Deploys **threat-to-consequence modeling** for all-hazards analysis
- Federates **public cloud infrastructure**
- Yields **unmatched visualizations** showing cyber-physical interactions





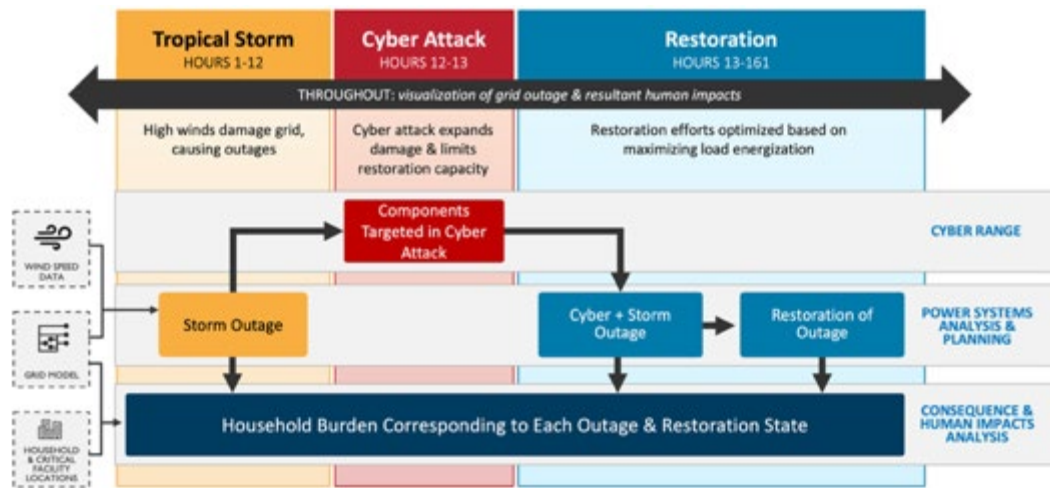
Questions the ARIES Cyber Range can help answer:

- Is my system **capable** of responding to and rapidly recovering from disruptions?
- Is my workforce **prepared** to respond to current and future risks?
- What **risks** do unverified software supply chains pose to the energy sector?
- How do we **quantify the benefits** of cyber-resilient distributed energy infrastructure?
- How should **cyber incident response change** in a more distributed and multi-stakeholder future?
- How **effective** will existing commercial tools be in a future with an exponential increase in the number of connected devices?
- How **big is the threat** of living-off-the-land attacks to advanced energy technologies?



Integration with the ARIES Cyber Range

Combined data from the DER-CF, the cyber range can help **merge the two complex cybersecurity topics of policy and technology** by providing an integrated way to interact with cybersecurity logs and alerts.



Threat-to-Consequence Demonstration

NREL's integrated compounding hazards risk analysis shows the outage impacts of a tropical storm, a cyberattack compounding impacts, and the restoration efforts needed to re-energize the grid and recover from widespread disruption.



Summary

- Utilities are subject to many types of **threats and vulnerabilities** and must plan accordingly.
- Risk quantification can help utilities **prioritize investments** in mitigation strategies.
- Cybersecurity governance helps an organization **detect, prevent, and respond to** cyber incidents.
- Cybersecurity assessments, like NREL's DER-CF, can help **monitor progress and identify gaps** in cybersecurity posture.

Thank You

www.nrel.gov

NREL/PR-5T00-95985

This work was authored by the National Renewable Energy Laboratory for the U.S. Department of Energy (DOE), operated under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Federal Energy Management Program. 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.

Photo from Getty 181828180





Megan Culler
Technical Director for Energy
Security

**Center for Security Digital Energy
Technology**



Smart Inverters, Dumb Risk Taking Control of IBR Security in the Digital Age

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

INL Idaho National Laboratory

IBR (It's Basically Risk)

Your Feature is My Vulnerability

A Capability-Focused Threat Brief

No One is Coming to Save You

The Case for Operator-Driven Defense in a Landscape of Growing Threats and Limited Oversight

Necessary but Not Sufficient

We can Tackle the Low-Hanging Fruit

Your Feature is My Vulnerability

A Capability-Focused Threat Brief

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy



Idaho National Laboratory

Digital Energy Transformation



- Dispatchability & Increasing Base Load



- AI in action



- Wide-scale sensing for optimized performance



- Increased control over energy use, consumer choice and bills



- Better management of existing assets



- Predictive maintenance for equipment



- More accurate forecasts

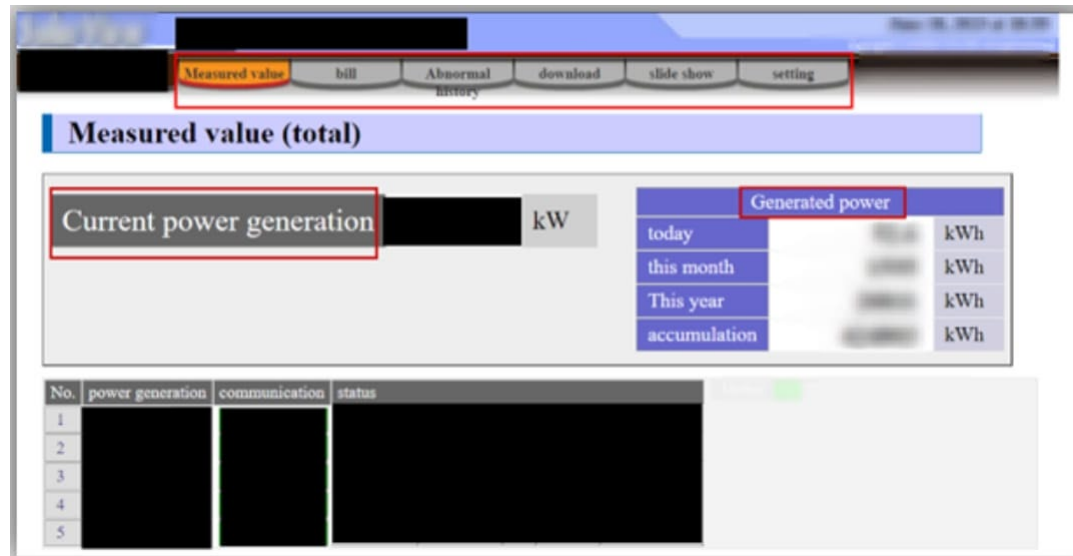


- Better supply chain management

Accessibility

Monitor your solar production from anywhere on the go!

- Cyble researchers scanned web for solar PV devices and found over 134,000 products from various vendors accessible.
- Exposed assets may not be vulnerable or misconfigured, but some interfaces allow unauthenticated access.

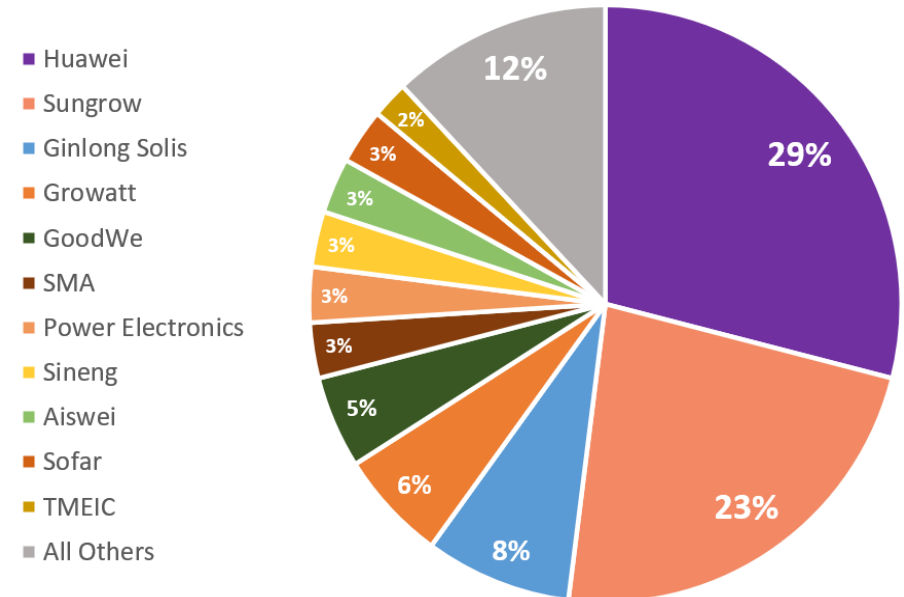
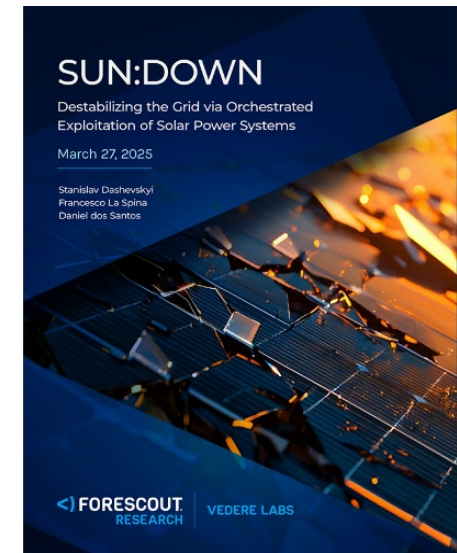


Solar Monitoring Apps



SUN:DOWN – Inverter Vulnerabilities

- Forescout's SUN:DOWN report highlighted critical vulnerabilities within SMA, Growatt, and Sungrow inverters
- SMA, Sungrow and Growatt provide a combined total of **approximately 32%** of **global inverters**
- Vulnerability disclosure summary:
 - 46 Total CVEs: Growatt accounted for 30 of these vulnerabilities, SMA for 1, and Sungrow for 15.
 - 39 of the vulnerabilities were related to web applications and Android applications (Mobile and web applications are not just used for residential inverters)
 - 7 of the vulnerabilities were related to an SMA gateway



Source: UnivDatos Market Insights | US Solar Inverter Market (2023-2030)

Smart & Fast Acting

Inverters provide critical grid services and rapid response capabilities

Rapid Response

- Fast ramping that matches natural gas in performance
- Avoided bulk outages through emergency dispatch
- Doubling installed capacity year over year

Reliable

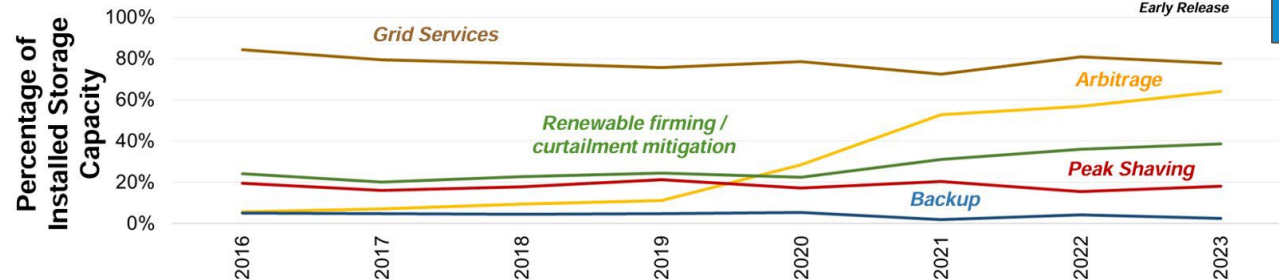
- HI – KES BESS project can serve 17% of Oahu's demand for 3 hours at peak load
- 17%+ of CA load is served by BESS
- TX and CA are 72% of deployed BESS, 62% of BESS in development

But fast acting **misbehaving** IBRs are a risk to stability



Breakdown of battery use-case for all batteries over time

Source: EIA 860 2023 Early Release



Source: EIA 860 2023 Early Release

IDAHO NATIONAL LABORATORY

Ease of User Interaction

Inverters are for everyone*!

*including adversaries

- Easy, convenient web-based interaction is often implemented with **insecure defaults, broad functionality** and **weak protections**
 - Adversaries like to use flows that exploit easy user interfaces (e.g., internet exposed inverter web UI's/cloud portals). This **increases** attacker surfaces and encourages risky behaviors.
 - Attackers who compromise UI can manipulate setpoints, volt/VAR control, remotely brick devices, etc.
- These insecure defaults and weak protections can include:
 - Weak or default authentication (e.g., inverters with default usernames/passwords)
 - Overexposed web interfaces (e.g., open internet for remote monitoring or control)
 - Simplified user controls
 - “One click functionality” for critical actions (e.g., inverter shutdown, firmware upgrade, grid-setting changes)
 - Poor Role-Based Access Control (RBAC) (e.g., all users share the same privileges)

Solar App Vulnerabilities – Weak Passwords

- Enphase Envoy

- CVE-2020-25754: Custom PAM module uses password derived from the MD5 hash of the username and serial number. Serial number can be retrieved by an unauthenticated remote user.
- CVE-2020-25753: Default admin password for certain versions set to the last 6 digits of the serial number, which can be retrieved by an unauthenticated remote user.
- CVE-2020-25752: Hardcoded web-panel login passwords for the installer and Enphase accounts. Users are unable to change these passwords
- CVE-2019-7676: Weak password vulnerability discovered in Envoy R3

- Contec SolarView

- CVE-2023-27512 use of hard-coded credentials may allow remote authenticated attacker to login with administrative privilege

- Fronius

- CVE-2019-19228: Solar inverter allows attackers to bypass authentication because the password is stored in a plaintext file

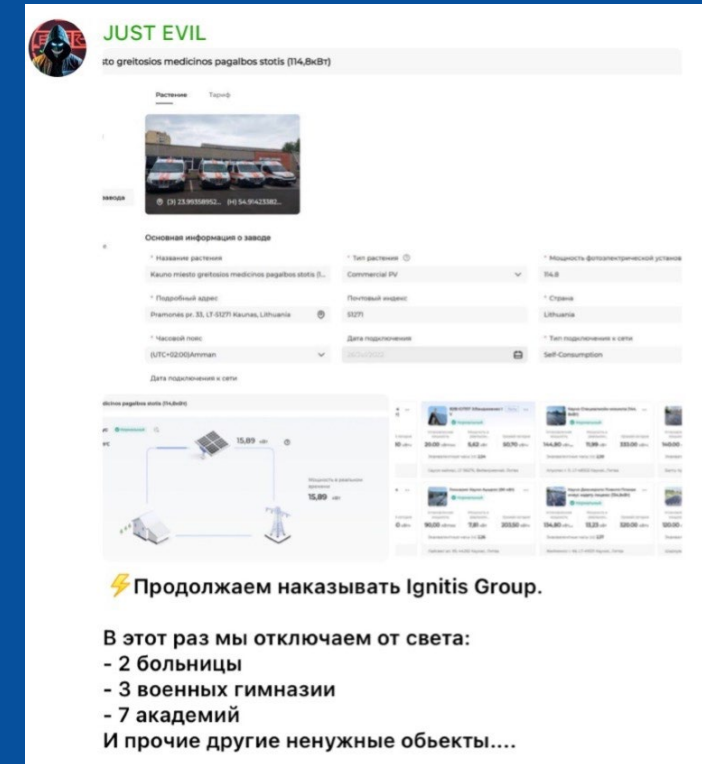
Takeaways for IBRs:


- Passwords should be unique, strong, and not related to other identifying information.
- Passwords should be encrypted for storage.



Alleged Attack on Lithuanian Solar Monitoring Systems (Sept. 2024)

- Pro-Russian hacktivist group Just Evil claimed to compromise PV monitoring solution used by the state-owned energy holding company Ignitis Group
- Claimed to access power monitoring dashboard of 22 Ignitis clients, including hospitals and military academies.
- **Believed that compromised credentials provided initial access.**
- Same group compromised EV charging control panel in February, demanded ransom.
- No operational impact from this incident, no ransom reported.





✓ **исправен**

Установленная мощность


104,80 кВт...

Мощность в реальном времени

11,70 кВт

Хороший контакт

264,30 кВт



✓ **исправен**

Установленная мощность


20,00 кВт

Мощность в реальном времени

5,62 кВт

Хороший контакт

50,70 кВт



✓ **исправен**

Установленная мощность


144,80 кВт...

Мощность в реальном времени

11,99 кВт

Хороший контакт

333,00 кВт



✓ **исправен**

Установленная мощность


140,00 кВт...

Мощность в реальном времени

12,00 кВт

Хороший контакт

349,20 кВт



✓ **исправен**

Установленная мощность


114,80 кВт...

Мощность в реальном времени

13,16 кВт

Хороший контакт

293,10 кВт



✓ **исправен**

Установленная мощность


90,00 кВт

Мощность в реальном времени

7,81 кВт

Хороший контакт

203,50 кВт



✓ **исправен**

Установленная мощность


134,80 кВт...

Мощность в реальном времени

13,23 кВт

Хороший контакт

320,00 кВт



✓ **исправен**

Установленная мощность

120,00 кВт...

Мощность в реальном времени

10,47 кВт

Хороший контакт

285,10 кВт

Cost Drivers & Market Pressures in IBRs

- **Key Cost Drivers**

- Hardware: semiconductors, inverters, transformers, etc.
- Manufacturing scale and supply chain concentration (especially PRC)
- Installation, permitting, and interconnection costs
- O&M costs remain lower than fossil but still tied to component reliability

- **Competitiveness & Government Support**

- Historically not cost-competitive without subsidies (e.g., state incentives)
- Tax credits & DOE programs helped bridge gap to make IBR deployment more feasible
- Current debates: shift toward OBBS, gradual reduction of credits

- **Cybersecurity & Cost**

- Cyber is seen as a cost adder meaning its **excluded** from early designs
- Market pressure = “First-to-Market” > “Secure-to-Market”
- Security retrofits increase lifecycle costs, harder to justify without mandates

- **Strategic Implications**

- PRC dominance in PV modules, inverters and BESS supply chain
- U.S. Market increasingly depending on Chinese-manufactured equipment
- Set up risk systemic exposure if cyber remains sidelined in cost discussions



BESS Supply Chain is highly dependent on non-domestic OEMs

Nearly 100% of battery material and over 70% of power electronic control systems for batteries are produced by the People's Republic of China (PRC). Nearly all BESS sites in the United States will have 1+ PRC-made component.

81+ battery/BESS suppliers with approved safety/standards

73+ named inverter manufacturers meet U.S. (safety/operational) standards

There are around 10 top integrators for PRC-made equipment

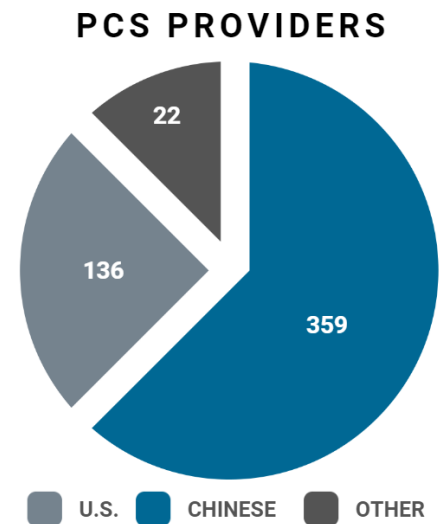
The integrator relationship has a significant influence on security factors, and can drastically change risk

~90–95% use PRC-manufactured equipment / material

70% are PRC owned/operated
90% have some manufacture in PRC

50% are PRC-owned integrators /
50% are U.S.-owned integrators

> 20 new players entered this market between 2021 – 2024

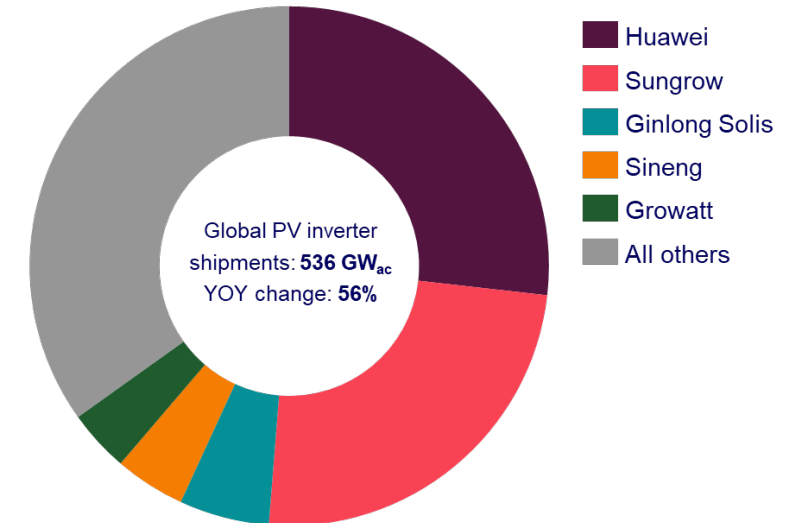


Market Reality and Diversity of Vendors - IBRs

- Market reality...
 - Global market is dominated by a handful of OEMs (Huawei, Sungrow, SMA, etc.)
 - The top 10 global PV inverter vendors accounted for **81%** of the market.
 - U.S. is **heavily** reliant on imports, especially from PRC based firms
 - Limited domestic production = shallow supply chain resilience

The lack of vendor diversity leads to systemic risk. A compromise of one dominant OEM can have nationwide grid consequences.

Global PV inverter market share rankings by shipment, 2023



Source: Wood Mackenzie

Rip and Replace vs. Secure Around and Through



- \$4B, 4 years to replace one US state's batteries alone
- \$12B for US Installed Supply Currently
- 70+ options currently for PRC BESS
- But what about quality and safety metrics?
- Huawei are still here, 5 years later
- Domestication of the Supply Chain
- Secure By Design
- Policy and Regulatory Solutions
- Cyber Informed Engineering Design
- Maintain demand signal

Maintenance Contracts & Persistent Connectivity

- **Why Persistent Communications Exist?**

- Firmware updates: ensure compliance, patch bugs, and enable new grid codes
- Performance monitoring: real-time diagnostics, predictive maintenance
- Warranty conditions: remote monitoring required to keep coverage
- Legitimate O&M needs: aggregators and OEMs require continuous telemetry

- **Cyber & Supply Chain Risks**

- Persistent links = persistent attack paths
- Vendors retain access long after commissioning = “always on backdoors”
- Firmware pipeline is high-value target (e.g., Deye inverter incident – attackers leveraged weakly secured firmware signing and updates channels)
- OEM-controlled updates bypass local operators > loss of autonomy and risk of malicious updates
- Warranties incentivize keeping comms open = operators trade security for financial protection

- **Strategic Implication**

- Supply chain dependence = foreign vendors retain long-term access
- Trust in firmware provenance & update channels become critical
- Increases systemic exposure if compromised at scale

Deye inverters disabled (Nov. 15, 2025)

- Deye-branded inverters in the U.S. were bricked with the message “This inverter is not allowed use at Pakistan/USA/UK.”
- Sol-Ark has exclusive rights to sell Deye inverters in the U.S., but other companies have sold them (a breach to which Sol-Ark has responded with lawsuits)
- Unclear why shutdown occurred.
- Sol-Ark claimed no tie to shutdown – offered discounted replacement inverters to affected individuals.
- Deye provided update 2 weeks later – claimed products that do not meet UL standards not authorized in US, and automatic check disabled inverters accordingly
 - Deye does not directly export or sell Deye brand inverters to US or allow resell. Therefore, Deye is currently unable to provide technical support for inverters in the U.S. market.

Takeaways:

- Consider implications of remote firmware updates.

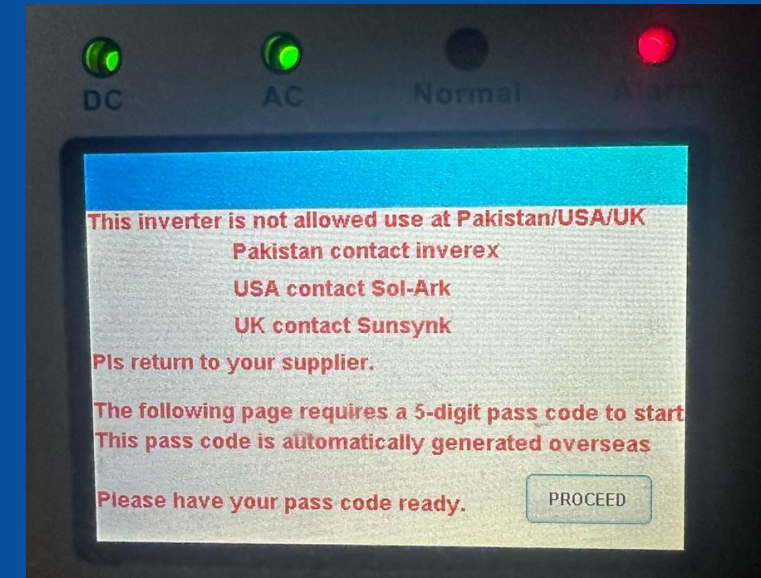


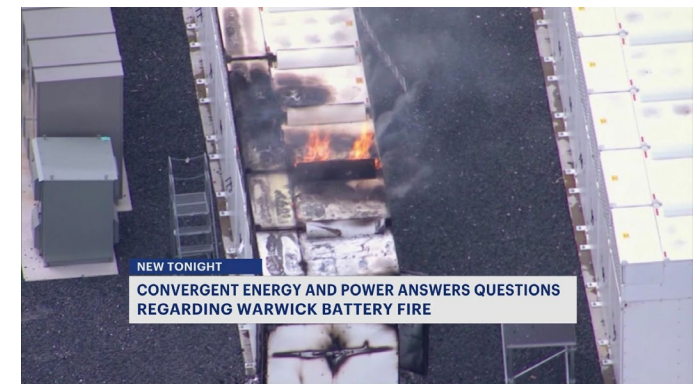
Image shows evidence of error message on bricked Deye inverter

Potential Impacts of Attacks on Batteries - Asset Health, Site Damage, Environment

- Site (uncontrolled) Fire
- Loss of preventative/proactive disconnect
- Damage to Battery Components & Site
- Damage to Battery Site Capacity
- Environmental Discharge / Damage



Moss Landing Fire June 2025



Warwick Battery Fire Oct 2023

Likelihood vs Difficulty point: Single Site - Medium, Mass Event – Low L Very High D

Potential Impacts of Attacks on Batteries - Loss of visibility

- Loss of status monitoring
- Loss of capacity monitoring
- Loss of activation or inactivation control
- Loss of physical access alarms



- Attack against the ViaSat KA-SAT network
 - Russian state-sponsored actors in attack coordinated with invasion of Ukraine
- DoS caused by an attacker exploiting a VPN appliance misconfiguration
 - Allowed for rewriting of flash on customer modems
 - Required replacement devices
- Caused loss of remote monitoring of 5,800 ENERCON wind turbines

Likelihood vs Difficulty point: Mass Event – high L, Med D

Potential Impacts of Attacks on Batteries - Electric Grid/Bulk Impact

- Loss of Control (doing the opposite)
- Power system stability & ancillary services
- Emergency Dispatch failure/loss of load
- Reputational damage
- Uncontrolled re-energization
- Loss of life
- Financial Loss

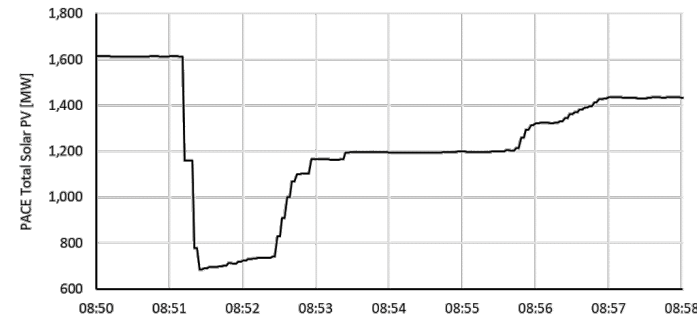
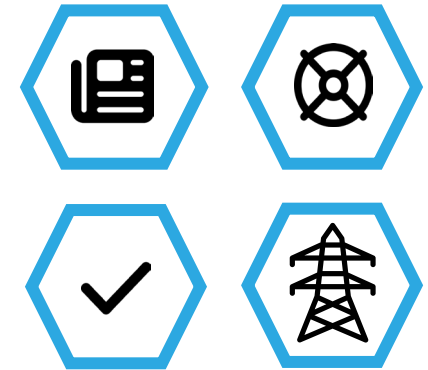


Figure I.2: PACE BPS-Connected Solar PV during Disturbance

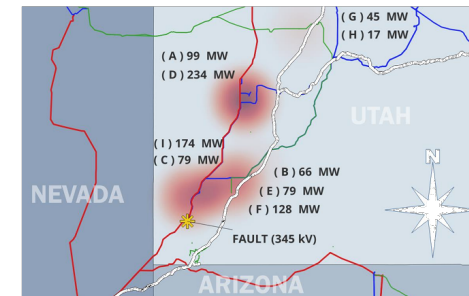


Figure I.3: Map of Fault Location and Affected Solar PV Facilities

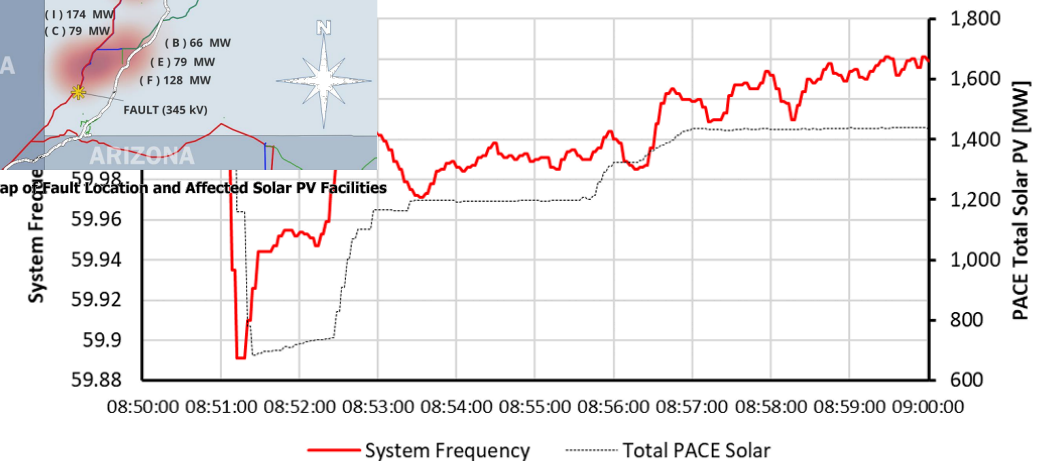


Figure I.4: WECC System Frequency

Likelihood vs Difficulty point: Mass Event – Low L, Very High D

Overall Attack Trends

- Notable increase in attacks targeting inverter based resources at large
- No strong evidence that IBR being targeted because they're IBRs or for operational impact
 - Active exploitation of vulnerabilities uses devices for computing power for other attacks
- Ransomware and data breaches continue to be some of most common attacks.
 - Ransomware remains a top cyber threat across sectors
 - Targets include utilities, manufacturers, and service providers
 - Median payment in energy, oil & gas, and utilities ransomware events was \$2.5M (Sophos)
- Operational impact seen most as denial-of-service.
 - Level of impact depends on stakeholder affected and criticality of assets.
- Attacks targeting third parties (OEMs, maintenance, etc.)
- APT activity detected before OT attack executed



No One is Coming to Save You

The Case for Operator-Driven Defense in a Landscape of Growing Threats and Limited Oversight






Are IBRs truly a low impact asset?

INSURANCE JOURNAL

NewsMagazinesResearchJobs

 **ACADEMY of INSURANCE** *Live webinars every week!*

Hacking Rooftop Solar Is a Way to Break Europe's Power Grid
December 12, 2024 by Eamon Farhat

Bloomberg All it takes is one hacker and a batch of faulty solar panels to threaten the safety of Europe's electric grid.

**Envirotec**
TECHNOLOGY IN THE ENVIRONMENT

- Advertisement -

 **Adler & Allan** DSEAR risk assessments for safe, compliant hazardous area operations.  [Learn more](#)

Home

NewsRenewablesSolar

Cybersecurity vulnerabilities in solar power could be used to attack the grid and cause blackouts

March, 2025




BUSINESS | GLOBAL ISSUES

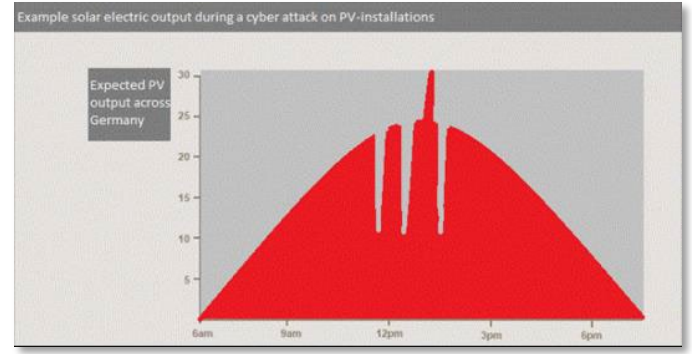
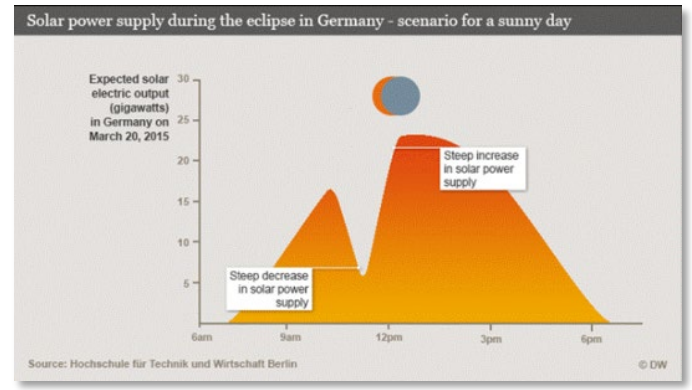
How hackers capture your solar panels and cause grid havoc

Mathis Richtmann
02/27/2025

The global push towards smart-energy production adds new vulnerabilities to national power grids. DW spoke to hackers who've exposed security gaps in rooftop installations and solar power plants around the world.



The transition to renewable energy relies on digital networks that can be targeted by hackers



Horus Scenario (c. 2017)

WHY 2025 - Horus Scenario 2.0

Practical analysis

- Tampering through API's
 - 2024 Solarman, Full control over other's devices.
 - 2025 SMA, RCE on cloud server
 - 2025 Vangelis Stykas: Gridlock
 - Solarman, Full control over other's devices.
 - Sunsynk, Full compromised cloud
 - Growat, Full compromised cloud
 - Solax, Full compromised cloud
 - Ingecon, Full compromised cloud
 - Foxess, Full compromised cloud
- Most of the above, also had backdoor access for manual.
- And did not respond to CVD after 3 years of trying.

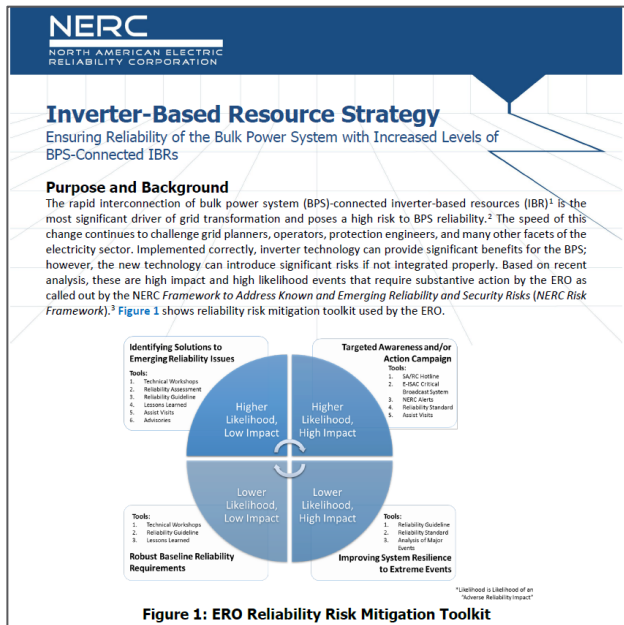
MORE VIDEOS

14:29 / 25:36

YouTube

Horus Scenario 2.0 (2025)

IBR Assets and NERC CIP Applicability



- IBRs have historically not been within scope of Bulk Power, though “dispersed power” producing resources that does sweep larger scale assets/farms into scope.
- Recent reliability failures and grid trends resulted in a specific initiative to bring more renewable assets into scope.
- Most IBR assets are **not subject** to NERC jurisdiction, so NERC CIP compliance requirements would not apply (or any cybersecurity regulation).
 - GO-IBR applies to generation assets >20MVA connected at 60 kV
- The requirements for initial implementation are limited to *operational* standards.
- Cybersecurity / CIP requirements will **not be** applicable to these lower threshold assets.

Who is not subject to NERC CIP? (some examples)

Developers

- Unless they are also the operator

EPCs

- If a customer is a registered entity, they would be responsible for defining the applicable requirements for the EPC

Product vendors

- Manufacturers, integrators, etc. are not registered entities.
- They could receive design requirements from a registered entity customer

Service providers

- Maintainers
- Cybersecurity solution providers
- Data monitoring and optimization

Smart loads

- Data centers and other large commercial or industrial loads participate in demand response and could impact the grid

Note: All of these could have legitimate business functions that would require them to have temporary or permanent physical or cyber access to systems.

Stakeholders in IBR Operation Vary Widely

Key Challenges with Growth

- Aggregators are growing but **lack** clear **oversight**
 - Aggregators typically outside of NERC CIP scope (especially when behind-the-meter)
 - DERs lack standardized cybersecurity baselines
- Little to no network monitoring within IBRs
- Lack of federal-level incident reporting for IBR cyber events
- No mandatory software checks for aggregator services
- Vulnerability management is often ignored
 - Partially because its difficult for utilities and aggregators to keep up
- Third-party and foreign component dependencies
- Patch Management
 - Inverter vendors rarely push timely patches; customers often unaware of risks

Aggregator/ Integrator/ Developer Incentivization

Or lack thereof

- **Lack of Regulatory Control**
 - Limited oversight of aggregator or developer cyber obligations
 - No uniform baseline for secure integration into grid services
- **Lack of Financial Incentives**
 - Security = cost with no direct ROI for developers/aggregators
 - Incentivized to deploy quickly, **not** securely
- **Site Sales and Handoffs**
 - Developers often build then sell portfolio of sites to asset owners
 - Integration responsibility shifts with little continuity of security posture
 - Weak accountability across lifecycle stages

Necessary but Not Sufficient

We Can Tackle the Low-Hanging Fruit

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy



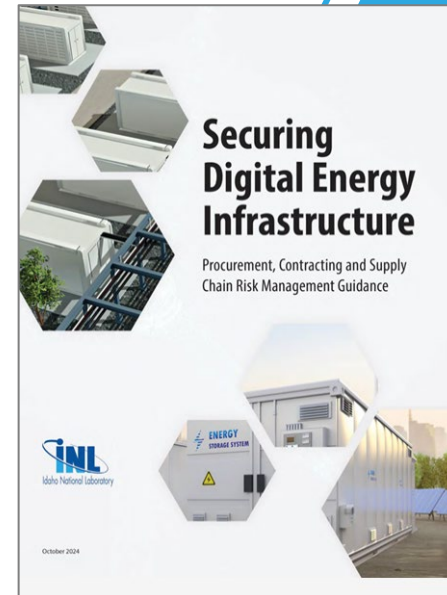
Idaho National Laboratory

You can demand accountability

Contract teeth: Configuration, Design Requirements & Supply Chain

- Firewall and Firmware DMZs
- Don't put it on the internet
- US Based O&M
- Monitor it
- External sensing for highest consequence scenarios
- Make contracts and procurement your friend

Better configurations could mitigate ~70 to 80% of the biggest consequences



Equipment can be inspected

Inspection is not just physical. It's about uncovering hidden dependencies in warranties, documentation, and vendor obligation.

- **Warranty Requirements**

- Some warranties mandate OEM connectivity (creates hidden obligations)
- Inspect whether warranty terms force persistent comms or remote access

- **Documentation Gaps**

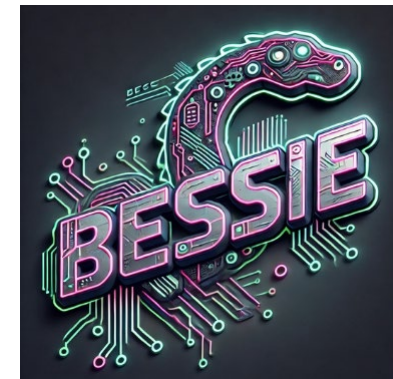
- Direct OEM connections may not be clearly documented in manuals
- Look for undocumented ports, cloud endpoints, or hidden firmware behavior
- Weak or inconsistent records complicate operator oversight
- Take photos of serial numbers, ports, cabling, comms, modules, labels, etc.
 - Helps verify against OEMs specs and warranty claims
 - Supports audit trails and post-inspection analysis

Monitor your OT

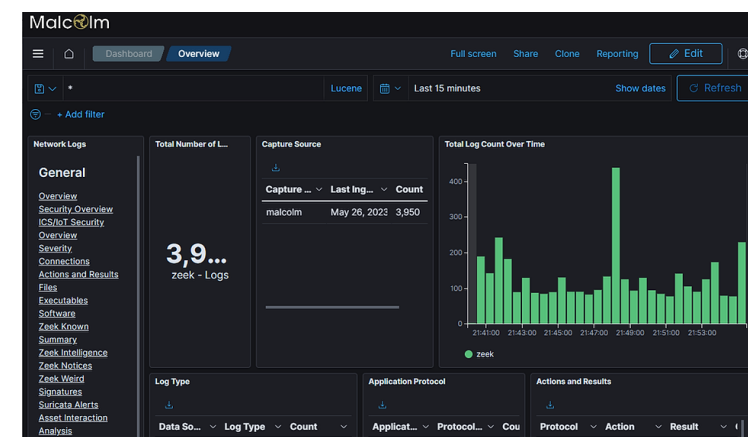
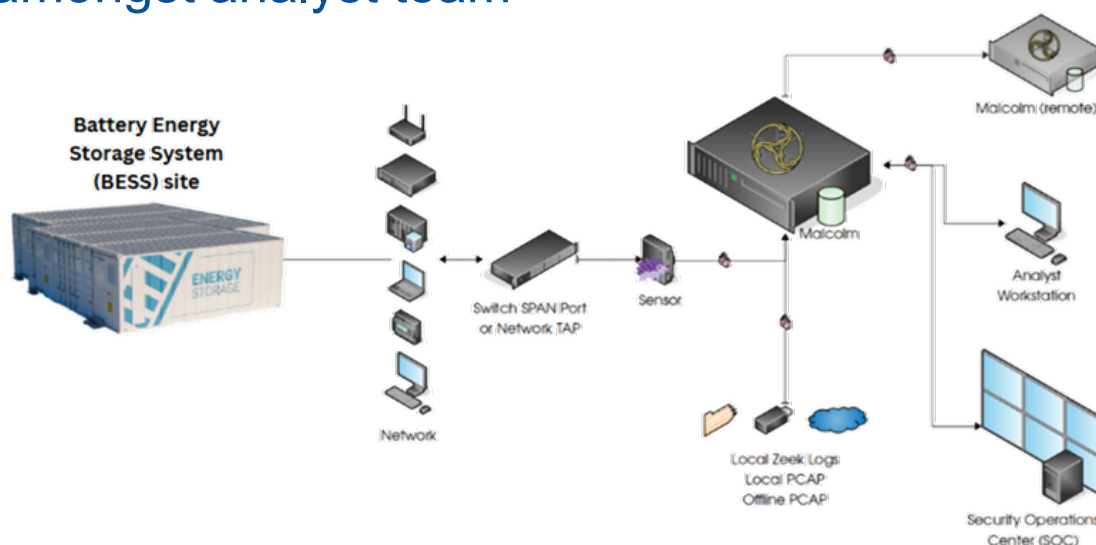
Don't forget about the grid edge

Network Hunt Kit Features:

- Highly scalable **passive network monitoring**, analysis, and threat detection
- Robust server hardware + virtualization for flexibility in use
- Industrialized network sensors for harsh physical environments
- Variety of tools for traditional **endpoint-based collection and analysis**
- Server-based applications facilitate a common, **real-time view** of data for all analysts
- Collaboration and case management tools enable task **coordination and sharing** amongst analyst team



BESSIE Hunt Kit Backpack



Malcolm Tool Dashboard

Vendor Risk Assessment

Asset inventories and layers of maturity

- Who makes it?
- Where's it coming from?
- What are their financial interests?
- What is it connected to?
- Where is the data going?
- What are the subcomponents?
- Is an SBOM available?



One Big Beautiful Bill (OB BB)

New FEOC Definitions

General goal: prevent Chinese companies from claiming IRA tax credits and reduce reliance on China for supply chains of critical energy technologies

Prohibited Foreign Entities (PFE)

Specified Foreign Entity

- Chinese military companies operating in the U.S.
- An entity that is subject to Uyghur Forced Labor Prevention Act restrictions
- A battery-producing entity that is ineligible for DoD contracts, as identified by FY21 NDAA
- Foreign-controlled entity*

Foreign-Influenced Entity

- Can directly or indirectly appoint a covered officer*
- Has 25% ownership over the entity
- Owns, in aggregate, alongside to the Specified Foreign Entities at least 40% of the entity
- Holds, in aggregate, at least 15% of debt of the entity
- Made a payment to a SFE that allows a SFE to exercise “effective control”* over a qualified facility, energy storage technology, or eligible component (for some credits)

*These definitions create two new FEOC categories in addition to the IRA FEOC definitions



Change your gd passwords
That's it. That's the slide.



Change your gd passwords

Okay fine, there's more.

- Change default passwords.
- Ensure there are no hardcoded passwords
- Make sure passwords are not stored in plaintext.
- Require strong passwords
 - Check against known breached password lists
- Consider periodic changes to passwords
- Enforce RBAC
 - Different accounts for maintainers, engineers, operators, etc.
- Avoid password reuse across devices

Use Inverter Features with Confidence

Accessibility

- Get it off the public internet – use private subnets, VPNs, and firewalls.
- Use available tools to check exposure (war driving sites, Shodan, etc.)
- Require passwords for access to web portals.

Fast-Acting

- Time delays in code
- Add noise to the system
- Monitor settings for changes
- Inspect firmware updates

Ease of Access

- Change default passwords
- Require strong passwords
- Ensure commissioning or site handoff policies

Affordability

- Include a vendor risk assessment as part of the procurement process
- Implement strong contracting T&Cs to enforce shared responsibility for cyber

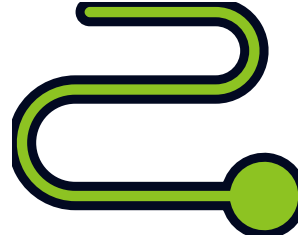
Maintenance

- On-site escort requirements
- Firmware and hardware inspection
- Vuln management programs

We have technical and policy solutions, we need to use them



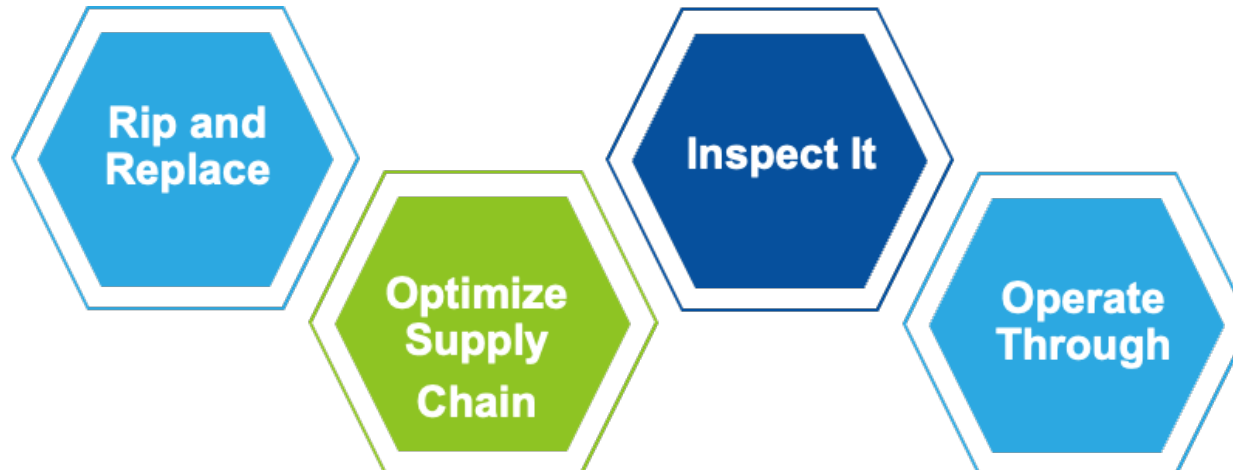
Solutions, analysis, and research **MUST** take a system-of-systems approach to reduce risk




There is no fast path to limiting suppliers domestically



Most direct approach is implementing a cyber-informed engineering approach to secure systems and mitigate risk

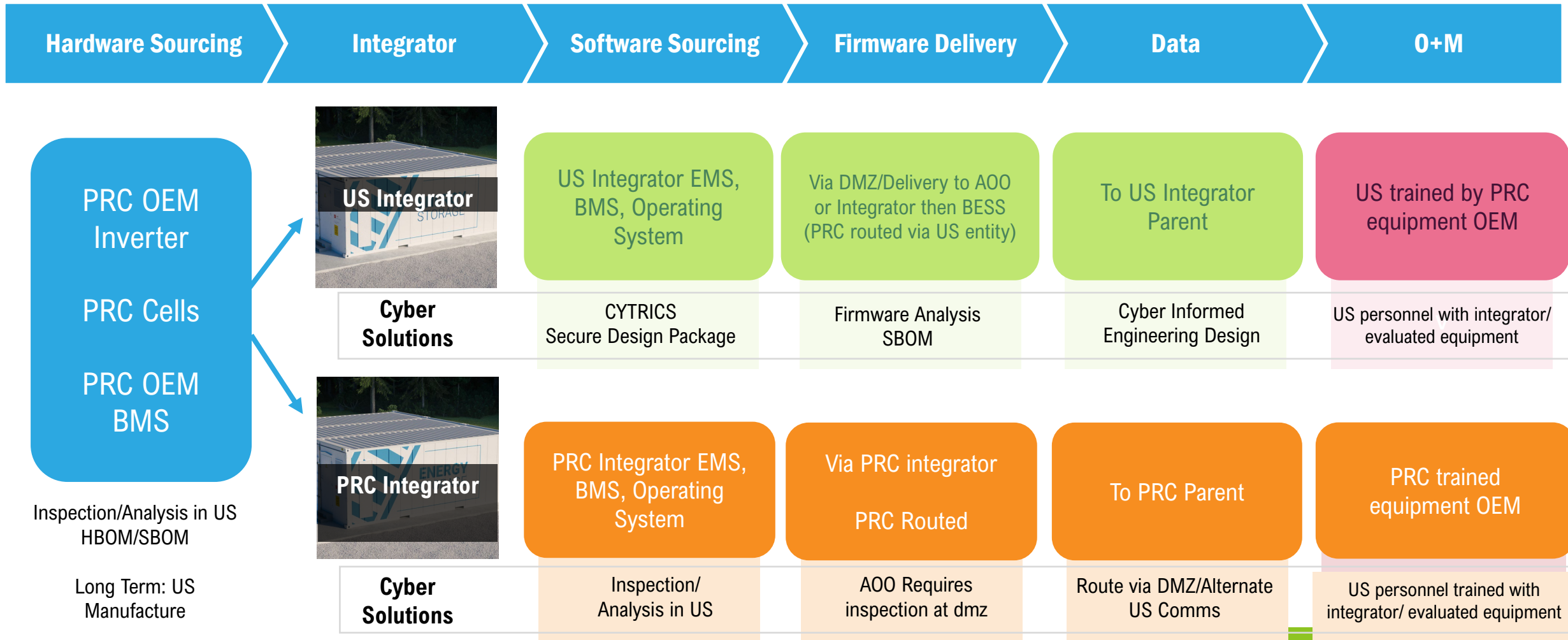


Menu of Solutions Along the Integrator Scale of Risk

			
	All FEOC, High Risk, More PRC Control & Connection, Less Ability to Evaluate	May Have Non-FEOC Equipment, Emerging Tech Relationships, Financial Ownership	Less Risk, All U.S. Connection, Higher Ability to Evaluate
Policy Solutions	Right to inspect/evaluate for vulnerability and control Tariffs	Develop U.S. Integrator & international cybersecure manufacture agreements	U.S. supply chain incentives for power electronics
Technical Solutions	<ul style="list-style-type: none"> • Procurement/contract guide • SBOM/HBOM Escrow • Configuration & inspection • OT monitoring & specific detections for PRC controller/actors • CIE design 	<ul style="list-style-type: none"> • Configuration & inspection • Secure by design for U.S.-made software • Secure comms • Vulnerability assessment program • Data Diodes 	<ul style="list-style-type: none"> • Secure comms • Secure by design • CIE design • Hunt & IR • Vuln assessment prioritization
Coordination Required From:	U.S. AOO, Buyer of PRC Product	U.S. AOO, U.S. Integrator, International OEM	U.S. AOO, Integrator, U.S. OEM

What's on the inside, and the outside counts

The integrator relationship has a significant influence on security factors, and can drastically change risk



Cyber Informed Engineering Design Guide for BESS and Microgrids

1

ANALYZE SYSTEM SERVICES

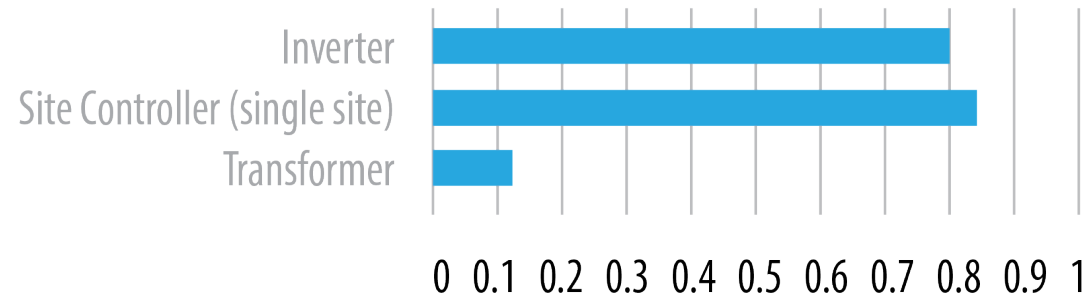
2

ANALYZE CONSEQUENCES

3

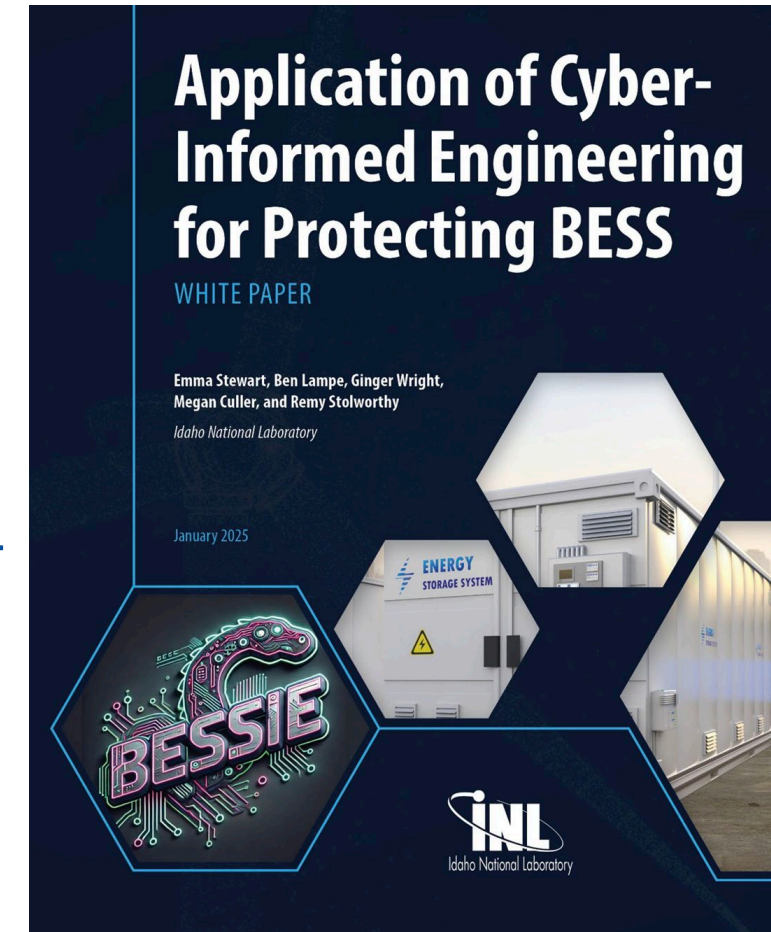
ANALYZE CIE MITIGATIONS

CRITICALITY OF BESS COMPONENTS



Goal: Help asset owners design their BESS integrations securely
3 industry partners have tested and used the process successfully

- Successful Case Study with US BESS Company: Business case for utilizing CIE in US integrated manufacture



Mitigations: Exercise and Incident Response

- Plum Island/Liberty Eclipse with BESS integrated
- GridEx
- SunSplat now ARES for Inverter Vuln Report
- IR Guide with specific BESS integrated options (ICS4ICS)
- Working with fire and incident responders



Putting Solutions Into Practice

GDO Technical Assistance for Digital Assurance

- Partnering to **rapidly deploy technical cyber and supply chain solutions** to federal awardees and enhance their hunt capabilities
- **15+ deployments to utilities and energy providers** – deploy solutions affecting \$20B of infrastructure in the next two years
- **Location prioritization and tiered solutions**
- **Prioritize** across 1,700 inverters/PCS for assessment
- **Cohorts of integrators** and 3rd party providers for key technologies
- **CIE Tool + Training** – CIE BAT and CIE MAT
- **Procurement and Contracting Guide** – training online to 56 federal awardees, in use by grant awardees and solution providers, trade association
- **Recommending changes to procurement strategies** – e.g. allow inspection

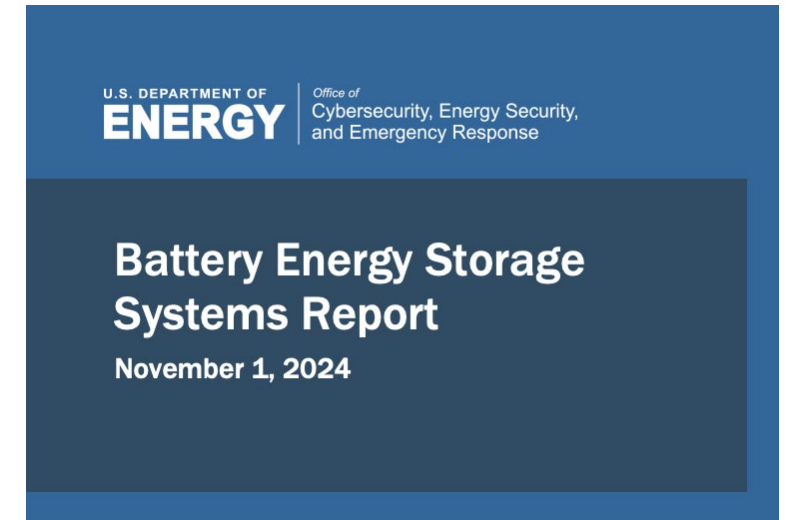
Summary

- The adoption of digital and emerging sources is increasing across all critical infrastructure sectors, such as hospitals, communication systems, water, transportation, military installations, and large loads
- The presence of adversarial entity suppliers in the supply chain is a significant concern, but not going away
- Solutions extend to many scenarios – not just IBR
- We can fix this, both in the short and long term
- Policy and Technical mitigations need to align

- 1 Force inspection and assessment**
- 2 Rationalize regulation and oversight around the “new school”**
- 3 Configure it right!**
- 4 We can safely integrate this equipment, we don’t have a choice, we need the right structure and services to do it (we just need to use them)**

Links Programs and Info

- <https://csdet.inl.gov/bess/>
- <https://www.energy.gov/ceser/articles/new-ceser-report-offers-supply-chain-mitigation-strategies-battery-storage-systems>
- **Cyber Informed Engineering** – <https://www.energy.gov/ceser/cyber-informed-engineering>
 - Products in IBR, Interconnection, Microgrids and BESS to guide secure configuration
- **Cyber Testing for Resilient Industrial Control Systems (CYTRICS)** – <https://cytrics.inl.gov/>
 - Equipment assessment strategy
- **Energy Cyber Sense** - <https://www.energy.gov/ceser/energy-cyber-sense-program>
 - Principles Targeted as Guidelines for IBR & BESS Manufacture
 - Analysis and Assessment Combined
- **Cyber Labeling (Inverters)** - <https://energy.sandia.gov/programs/electric-grid/cyber-security-for-electric-infrastructure/cyber-labeling-research-initiative/>
- **Liberty Eclipse** – <https://www.energy.gov/ceser/liberty-eclipse>
 - Battery Assessments in GMLC
- **CyberStrike (STORMCLOUD)** – <https://inl.gov/national-security/cyberstrike/>
- **Energy Threat Analysis Center (ETAC)** – <https://www.energy.gov/ceser/energy-threat-analysis-center-0>
- **CESER OT Defender** – <https://otdefender.inl.gov/>





Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.

GO IBR Initiative

Generator owner/Generator operator of inverter-based resources

- Purpose: identify and address challenges of IBR as penetration of these resources continues to increase
- FERC issued order in 2022 directing NERC to identify and register owners and operators of currently unregistered bulk power system-connected IBRs.
- NERC determined that majority of unregistered IBR nameplate capacity is made of resources 20 MW or larger
 - Study found that IBRs accounted for over 15% total nameplate capacity on BPS in 2021, but only 84% of nameplate capacity of IBRs were registered with NERC.
- GO-IBR is a new registered entity function that includes IBRs that
 - (1) have an aggregate nameplate capacity between 20-75 MVA and connected at a voltage greater than 100 kV
 - (2) have an aggregate nameplate capacity of greater than 20 MVA and interconnected at a voltage less than 100 kV.
 - Definition does not include IBRs on distribution system or DERs

GO-IBR Initiative

- New registration requirements expected to result in ~98% of BPS-connected IBRs being subject to NERC Reliability Standards.
- 2024 focused on revisions of registration-related sections of its Rules of Procedure
- 2025 will focus on approach for identifying applicable Reliability Standards, including sub-set lists, for newly identified GO-IBRs
- 2026 will complete registration activities for GO-IBRs, including technology transition and training, onboarding checklists, and notification letters to new GO-IBRs with information on registration and compliance responsibilities

Limitations of GO-IBR

- While new registration requirements are expected to cover 98% of BPS-connected IBRs by nameplate capacity, the number of devices that is not covered may represent a far larger portion of devices than 2%.
 - The individual DER do not impact the BPS and will not be covered by IBR-GO, but there are still a lot of these devices and a lot of stakeholders interacting with these devices.
- Not yet clear what Reliability Standards will be applicable to GO-IBRs (may be NERC low, or a subset)



RF CIP Low Impact Workshop - Dragos

Jeremy Korger
jkorger@dragos.com
Associate Principal Solutions Architect

Agenda

1. High Level Overview
2. Free Resources
3. Threat Brief
4. Dragos Platform
5. Neighborhood Keeper
6. Open Q&A

<https://www.dragos.com/cybersecurity-solutions/industrial-cybersecurity-compliance/nerc-cip/>



DRAGOS

Safeguarding Civilization

The Most Effective OT Security Tech Platform

Expertise integrated into software to reduce OT risk

A Community-Focused Mission

Skills, communications, & resources to strengthen the collective defense

Expert OT Intelligence & Service Resources

OT expert analysts, threat hunters, & responders to help you win the fight.

The background is a dark, industrial scene featuring a complex network of pipes, scaffolding, and large storage tanks. A semi-transparent dark rectangle is centered over the image, containing the text. The text is in a light green, sans-serif font. The overall aesthetic is technical and modern.

Free Resources

RECOMMENDATIONS

<https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/>



THE FIVE ICS
CYBER SECURITY
CRITICAL
CONTROLS

- 01 ICS Incident Response Plan
- 02 Defensible Architecture
- 03 ICS Network Monitoring Visibility
- 04 Secure Remote Access
- 05 Risk-based Vulnerability Management

Introducing the Community Defense Program

The Dragos Community Defense Program (CDP) gives under-resourced utility providers (with under \$100M in annual revenue) [free access to the Dragos Platform](#), which provides clients the foundation for building their cybersecurity program and reducing operational technology (OT) cyber risk.

Free OT cybersecurity software technology

Dragos Platform and other key resources such as Dragos Academy, OT CERT, Neighborhood Keeper | CDP Threat Hunting

For small water, electric, and natural oil/gas providers

<\$100m USD annual revenue in Canada & the United States

To help reduce risk of cyber events a multitude of resources are provided

- Inventory management
- Detect and hunt threats
- Manage vulnerabilities
- Respond to incidents

Register at:

[Dragos.com/community-defense-program](https://dragos.com/community-defense-program)

Email us at:

CDPinfo@dragos.com

Community: Dragos OT-CERT



OT-CERT
OPERATIONAL TECHNOLOGY
CYBER EMERGENCY READINESS TEAM

**1,600
members**

**60
countries**

OT-CERT is the Operational Technology – Cyber Emergency Readiness Team dedicated to addressing the OT resource gaps that exist in industrial infrastructure.

For more information:
<https://www.dragos.com/community/ot-cert/>



2025 OT / ICS CYBERSECURITY REPORT

A Year in Review: Industrial Threats
& Strategic Recommendations

→ **DOWNLOAD NOW**

dragos.com/year-in-review



The background is a dark, atmospheric photograph of an industrial complex, possibly a refinery or chemical plant. It features tall distillation columns, storage tanks, and piping. A semi-transparent black rectangle is centered on the image, containing the title 'Threat Brief' in a light green, sans-serif font. The entire image is overlaid with a network of thin, glowing green lines and dots, suggesting a digital or cyber theme.

Threat Brief

TWO NEW DRAGOS THREAT GROUPS




YEAR FIRST
DISCOVERED



THREAT GROUP UPDATE: VOLTZITE



**VOLTZITE**
SINCE 2023

ADVERSARY:

- + Overlap with Volt Typhoon and BRONZE SILHOUETTE

CAPABILITIES:

- + Heavy use of living off the land techniques
- + Slow steady reconnaissance to evade detection
- + Use of Fast Reverse Proxy, multiple web shells

VICTIM:


- + Targets the electric sector across the United States, Guam

INFRASTRUCTURE:

- + Uses internet-facing SOHO networking equipment for communications

ICS IMPACT:

- + Loss of Confidentiality, Theft of Operational Information
- + Espionage and persistent access



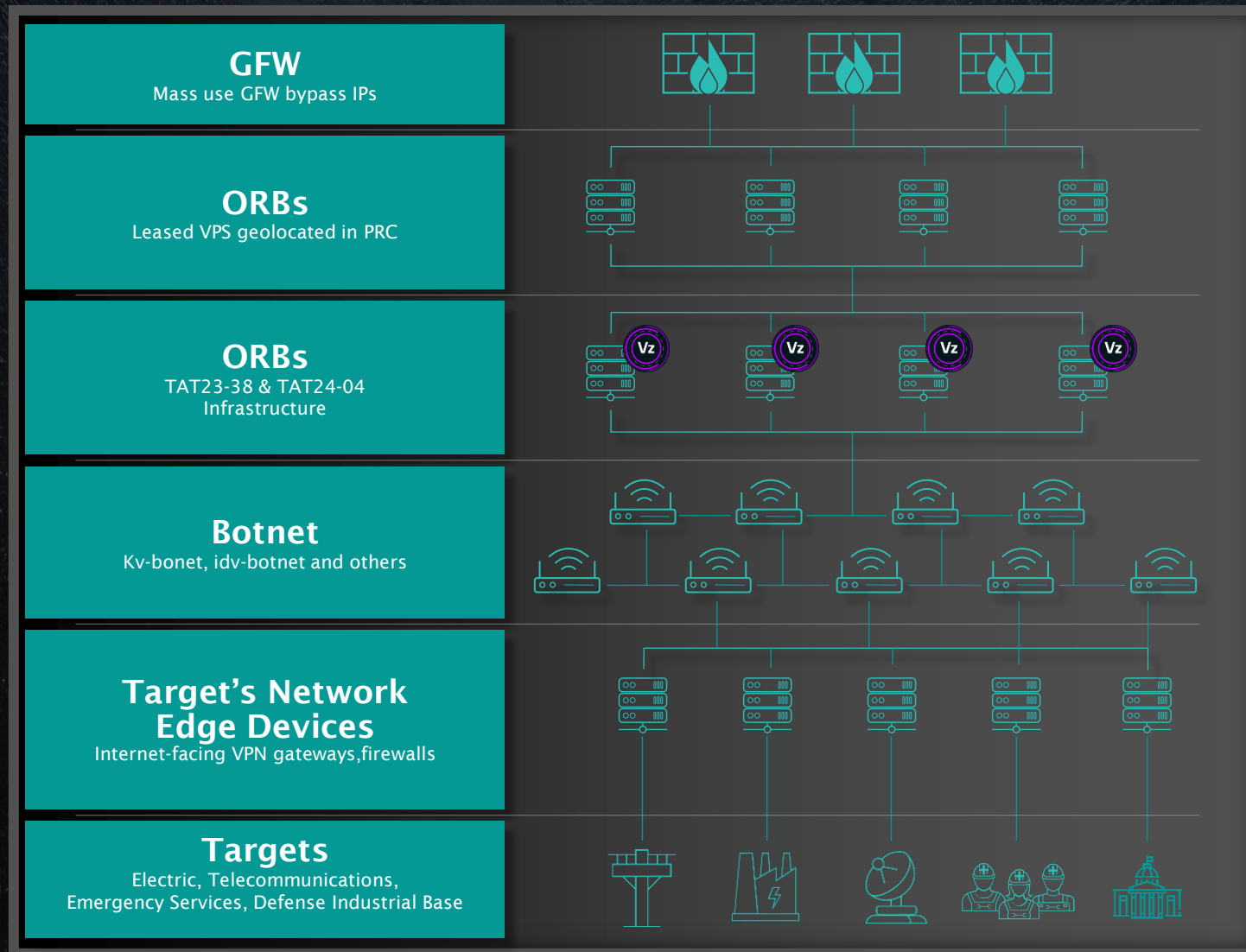
“[Chinese government-linked hackers have burrowed into U.S. critical infrastructure and are waiting] ‘for just the right moment to deal a devastating blow.’”

Volt Typhoon has successfully gained access to numerous American companies in telecommunications, energy, water and other critical sectors, with 23 pipeline operators targeted

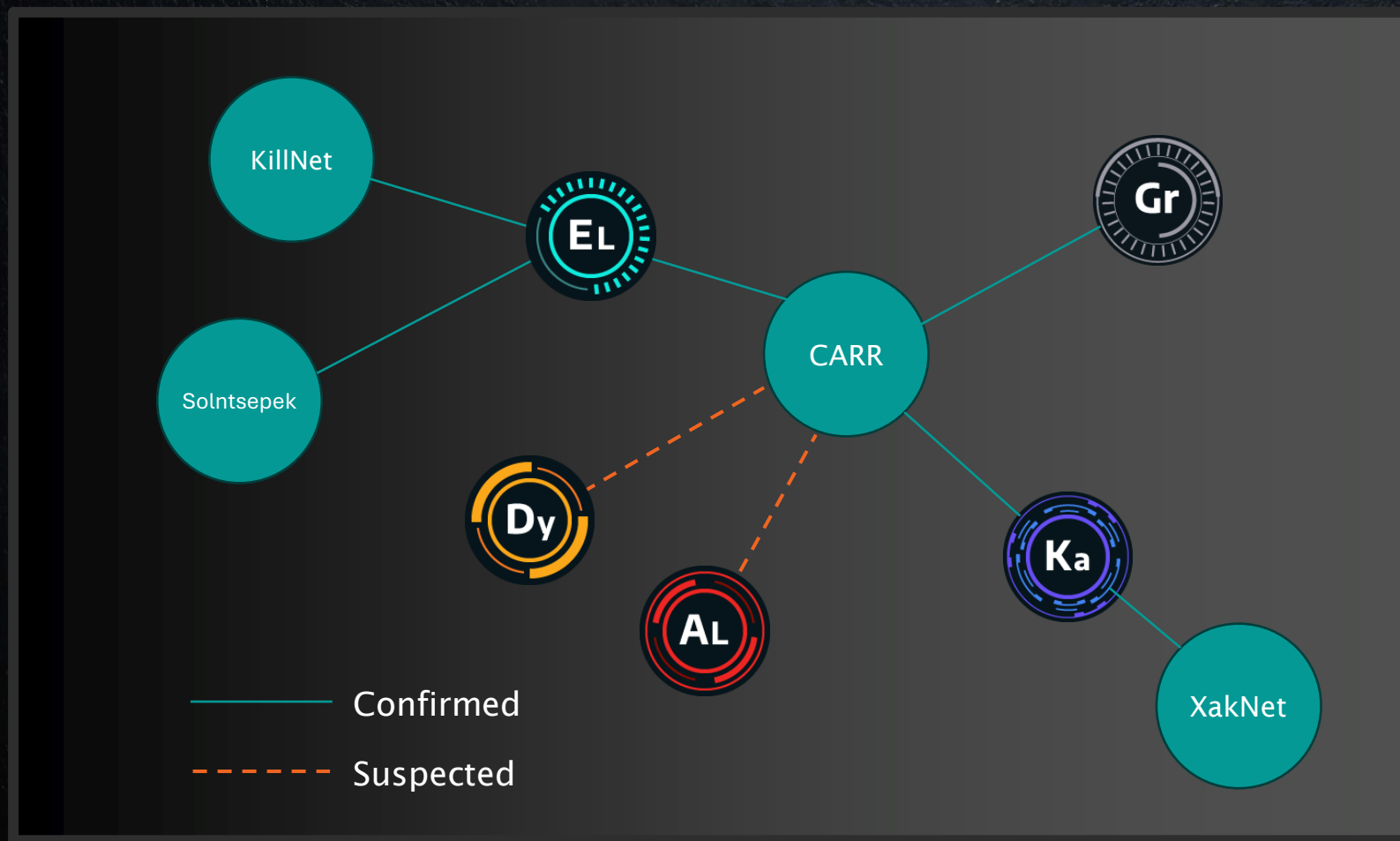
“The CCP’s dangerous actions—China’s multi-pronged assault on our national and economic security—make it the defining threat of our generation.”

- US FBI Director Christopher Wray

VOLTZITE BOTNET



CONVERGENCE OF HACKTIVISM & STATE-SPONSORED THREATS



Shared Infrastructure



Intelligence Sharing



Victim Overlaps

NEW THREAT GROUP: BAUXITE

STAGE 2: ICS ACTIONS AGAINST EASY-TO-ACCESS TARGETS



BAUXITE
SINCE 2023

ADVERSARY:

- + Overlaps with CyberAv3ngers

CAPABILITIES:

- + Uses publicly known exploits
- + Consumes Security Advisories from OT/ICS OEMs
- + Leverages tools built into Kali Linux
- + Linux Backdoor with C2 over MQTT

VICTIM:

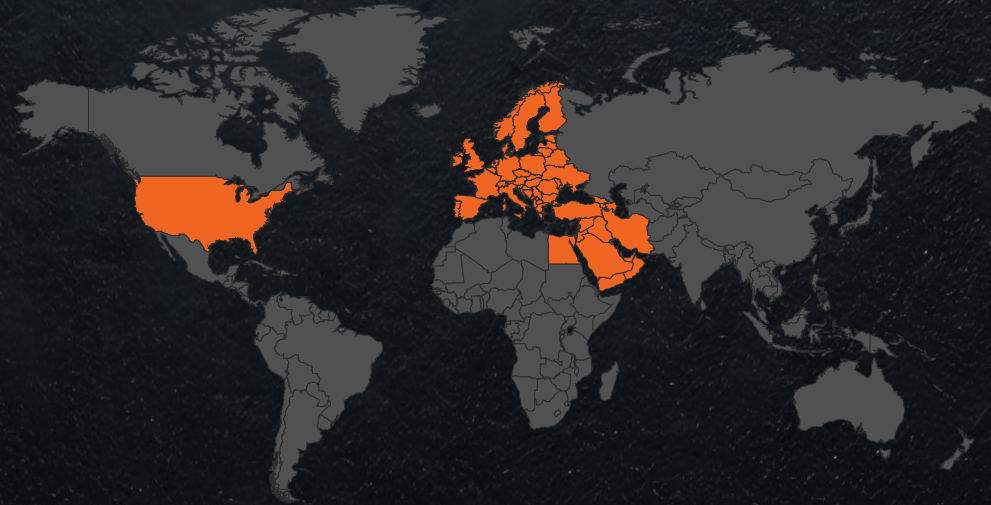
- + Global impact, victims in the U.S., Australia, U.K., and Israel

INFRASTRUCTURE:

- + Use/reuse of bulletproof hosting providers & owned infrastructure
- + Different infrastructure for CNA/CNE, Scanning & Research

ICS IMPACT:

- + ICS Cyber Kill Chain Stage 2
- + Denial of Control, Loss of Availability, Loss of Control, Loss of Productivity and Revenue, Loss of View



BAUXITE is capable of modifying ladder logic in PLCs & deploying custom backdoors in ICS equipment. Associated with the manipulation of Unitronics PLCs.

Focused on critical manufacturing, government, and professional services, aviation.

Uses compromised victim infrastructure/identity for operations against other targets.



Oil &
Natural Gas



Electric



Water &
Wastewater



Food &
Beverage



Chemical
Manufacturing

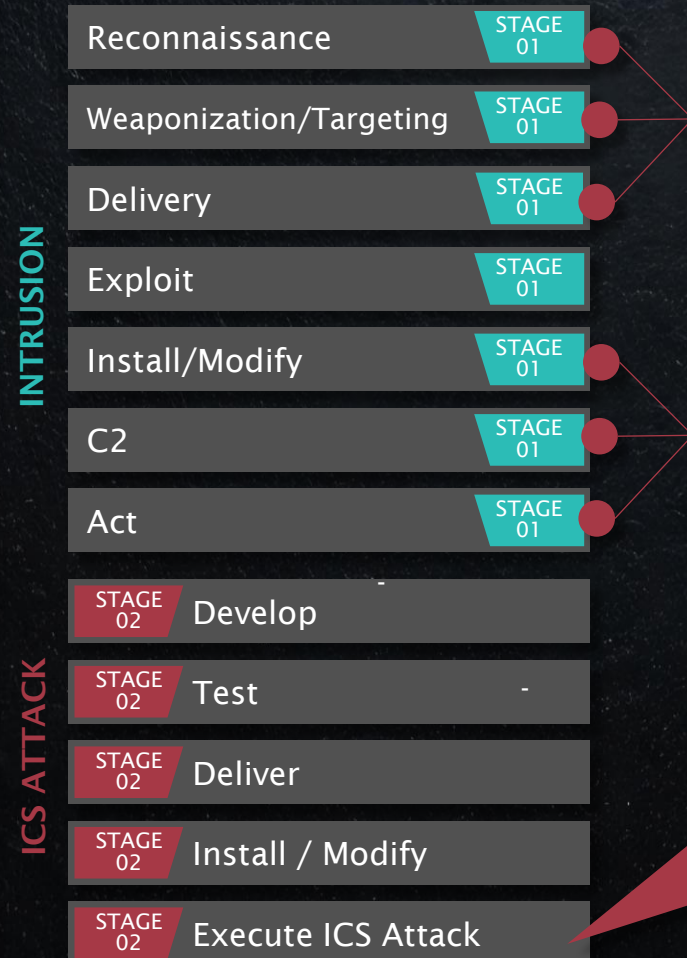
BAUXITE: STAGE 2 ICS ATTACK



100%
of observed
BAUXITE
targets were
accessible from
the internet

100%
of ICS attack
activity used
SSH for initial
access

ICS CYBER KILL CHAIN



CAPABILITIES

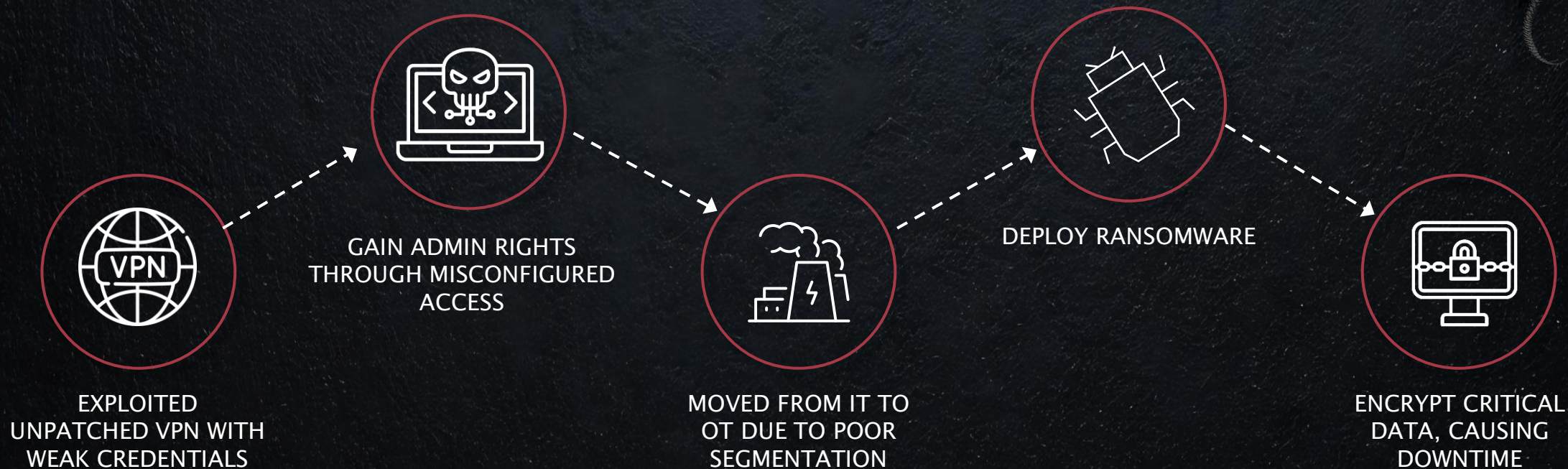
Targets Internet Facing Devices (VPN, Firewalls, PLCs)
Access via brute Force SSH with custom scripts & binaries
Delivers with webpages, SSL, & web pages

Installs malware like IOCONTROL, changes router configs
Establish backdoors with persistent SSH connects
Creates C2 link with Cloudflare infrastructure

STAGE 2

Denial-of-Service (DoS) attacks against PLCs and HMIs, ladder logic manipulation. Potential for wiping firmware on affected devices.

WHAT CAN GO WRONG: RANSOMWARE



HOW TO FIX IT

Patch VPN vulnerabilities, enforce MFA

Restrict admin privileges, monitor access

Implement strict IT/OT segmentation

Deploy OT-native threat & anomaly detection

Conduct TTX, establish offline backups

The background is a dark, industrial scene featuring a refinery or chemical plant. It includes tall distillation columns, storage tanks, and complex piping. A semi-transparent dark rectangle is centered over the image, containing the text. Faint, glowing green lines and circular patterns are overlaid on the background, suggesting a digital or technological theme.

Dragos Platform

Key Challenges Managing OT Cyber Risk



UNDERSTANDING THE OT ENVIRONMENT

What assets do I have? How does it change?
What systems talk to other systems?
What external connections do my OT systems have?



VULNERABILITIES

Which vulns should I care about?
What are alternative mitigations?



THREAT DETECTION

Am I compromised?
What do I do about it?



IT-OT CYBER GAP

How can I get OT security expertise?
Who should I partner with?

OT CYBER THREAT INTELLIGENCE TEAM

Engage and Educate the Community:

Intelligence Team creating Reports, answering RFI's, and embedding in orgs with Concierge Analysts

Codify the Knowledge Into Technology:

Platform Analytics
Threats & Vulnerabilities

Dragos Technology Platform

Neighborhood Keeper Collective Defense

OT Watch – Managed Threat Hunting

Network Segmentation & Access Path Analysis

Risk-based Vulnerability Management

Multi-layer Threat Detection

Response Playbooks & Digital Forensics

OT Network Monitoring and Deep Packet Inspection
Asset Discovery & Inventory | Forensic Logging

OT CYBER SERVICES TEAM

Partnering with Customers on Their Journey:

Proactive Assessments, TTX'es, Architecture Reviews, Compromise Assessments, Pentesting, & Incident Response

Codify the Knowledge Into Technology:

Expertise
Features, Dashboards, Playbooks built by practitioners for practitioners

How Dragos Platform Works

Level 3
Level 2
Level 1

Collect Data in Levels 1-3 of Purdue Model

- Sensors, Edge Collectors, File Ingest
- Analyze North-South & East-West traffic
- Analyze Firewall and Switch Configurations
- Passive-first approach (Active options)

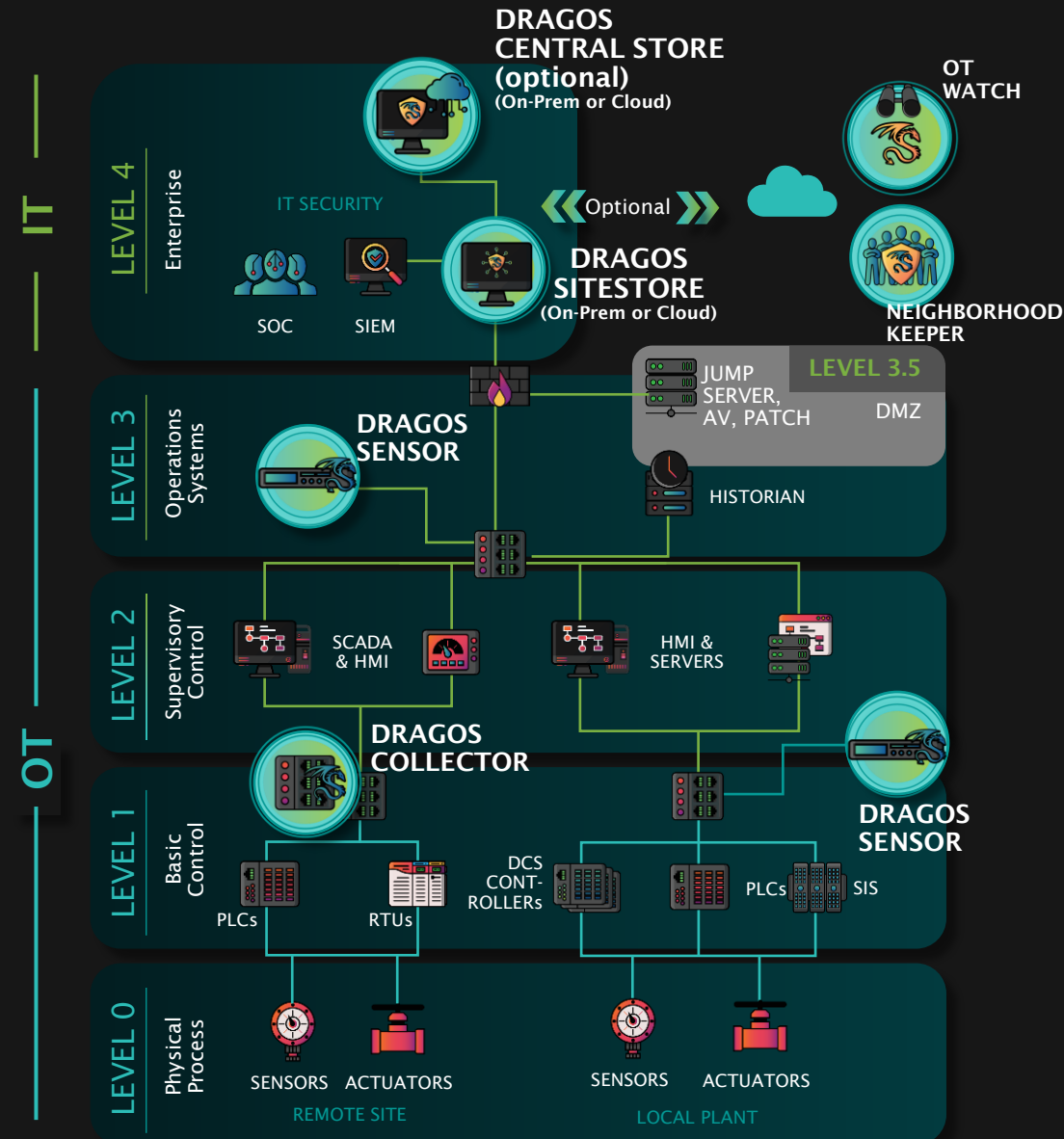
Monitor Your Environment via SiteStore

- Asset discovery, inventory, & profiles
- Risk-based vulnerabilities
- High-fidelity threat detections
- Response Playbooks

Integrate into Security Processes

Threats
Vulns
Intel

- Alerts flow into SIEM & SOC Tools
- Asset groups & alerts inform Firewalls
- Vulnerabilities flow to service management
- Visibility for Operations Teams for Root Cause Analysis and Operational Resilience



The background is a dark, atmospheric photograph of an industrial complex, possibly a refinery or chemical plant. It features tall distillation columns, storage tanks, and piping. Overlaid on this image are faint, glowing green lines and circular patterns that suggest a digital or data-driven theme. In the center, a black rectangular box with a thin green border contains the title text.

Dragos Platform Demo

The background is a dark, industrial scene featuring a large cooling tower on the left and several large storage tanks on the right. A semi-transparent dark rectangle is centered over the image, containing the text. The text is in a light green, sans-serif font. The entire image has a dark, muted color palette with some yellow-green highlights from the background elements.

Neighborhood Keeper

COMMUNITY CHALLENGES



LIMITED ICS/OT VISIBILITY



DEFENDING IN ISOLATION



INFORMATION LATENCY

“For these reasons and more, the industry has been working to assess adversary capabilities through a keyhole, rather than through a deeper collection and broader field of vision.”



NEIGHBORHOOD KEEPER

COMMUNITY VISIBILITY & COLLECTIVE DEFENSE FOR OT THREATS

A free, opt-in program for
Dragos Platform customers

Anonymously shared ICS threat
intelligence at
machine speed between asset
owners and community defenders

See aggregated threat, asset, and
vulnerability data from across Dragos
Platforms customers in your industry



NEIGHBORHOOD KEEPER - INSIGHTS

All identifiable and sensitive data stays on-prem with the customer

Non-sensitive, non-identifiable insights are shared with Neighborhood Keeper

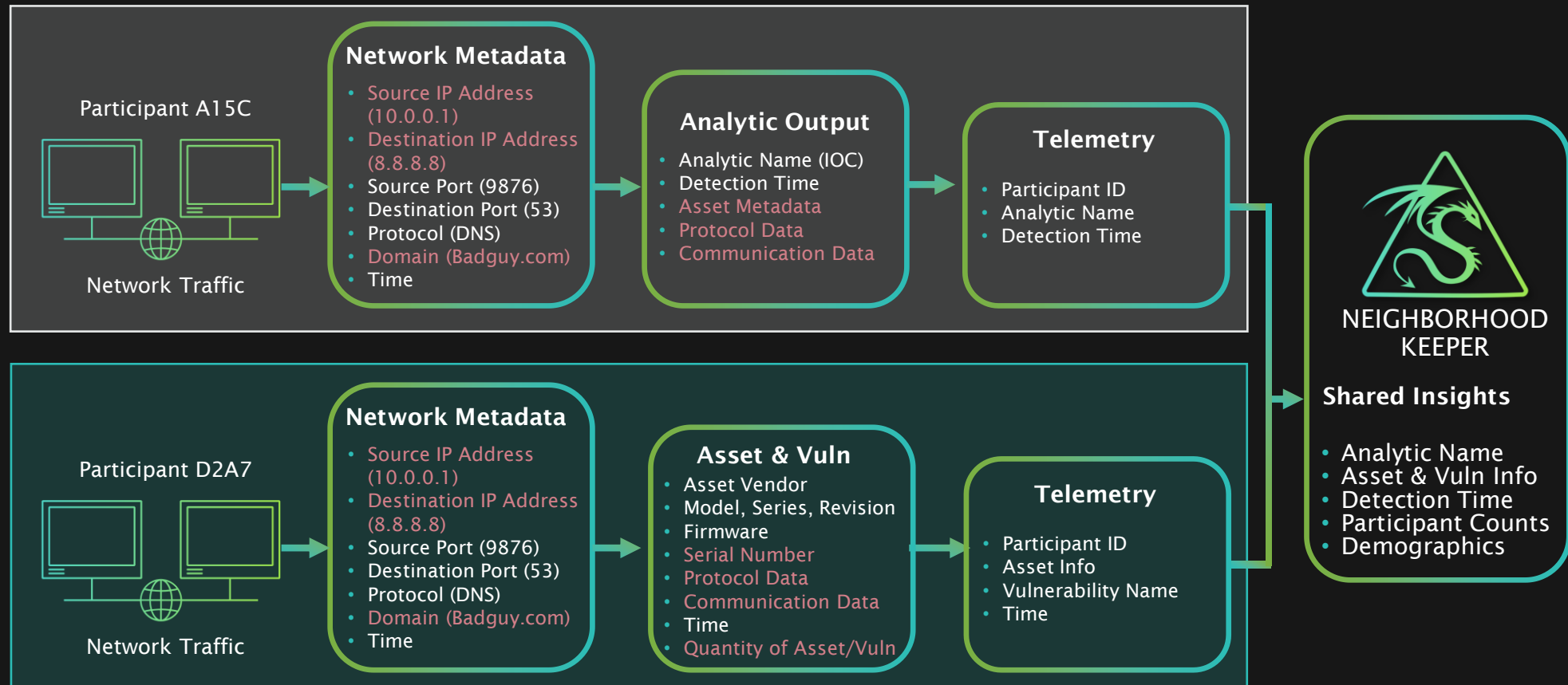
An example would be:
“Detection 3 fired at Utility 2”

The participant's name, identity, etc. are technologically irreversible from the data



NEIGHBORHOOD KEEPER – INSIGHTS IN-DEPTH

Aggregated metadata is sent to Neighborhood Keeper for analysis



Rockwell Automation ControlLogix Vulnerability

A State-Actor Developed Capability Prior to Employment by the Adversary



US Government Agency Identifies New Rockwell Automation ControlLogix Vulnerability being researched by a state-actor for use in operations



FIRMWARE REVERSE
ENGINEERING

100101001
010011010
101010101
100101011

PCAP
ANALYSIS



ANALYTICS
DEVELOPMENT

Dragos OT Cyber Threat Intelligence Team Works with USG Agency and Rockwell to reverse engineer the capability and develop detections



Dragos Deploys Analytics to Neighborhood Keeper & OTWatch for Asset Prevalence & Signs of Active Exploitation to provide insights to USG and early protections for customers



Dragos
Platform

Dragos Deploys Detection Analytics to Platform via a Knowledge Pack

- Dragos Briefs Customers Prior to Public Announcement
- Rockwell Announces Vulnerability
- Dragos Educates Broader Community on Vulnerability, Impact, & Mitigation

Collective response happened PRIOR to an attack taking place.
Success for all of us.

The background is a dark, atmospheric image of an industrial facility, possibly a refinery or chemical plant, with various structures, pipes, and storage tanks. A semi-transparent dark rectangle is centered over the image, containing the title text. A thin, glowing green rectangular border frames the text area. Faint, glowing green lines and dots are scattered across the background, suggesting a digital or data-driven theme.

Neighborhood Keeper Demo



Open Q&A “Ask Me Anything”