

# WELCOME TO TECHNICAL TALK WITH RF

*Cybersecurity Awareness Month*

October 28, 2024





# TECHNICAL TALK WITH RF

Join the conversation at

[SLIDO.com](https://www.slido.com)

[#TechTalkRF](https://twitter.com/TechTalkRF)

# TECHNICAL TALK WITH RF

Follow us on



[Linkedin.com/company/reliabilityfirst-corporation](https://www.linkedin.com/company/reliabilityfirst-corporation)

A screenshot of the ReliabilityFirst Corporation LinkedIn profile. The header features a banner image of power lines at sunset. The profile name is "ReliabilityFirst Corporation" with a notification bell icon. Below the name, it states "RF works to maintain the reliability, security and resilience of the electric grid in the Mid-Atlantic region" and "Utilities · Cleveland, OH · 3,970 followers · 101 employees". A section indicates "Brian & 85 other connections work here" with buttons for "Following", "Invite", and "More". Navigation tabs include "Home", "My Company", "About", "Posts", "Jobs", and "People". The "Posts" tab is active, showing a post from "ReliabilityFirst Corporation" (3,970 followers, 2d) with the text: "ReliabilityFirst staff participated in our organization's annual Day of Giving last week. Thank you to [BOYS & GIRLS CLUB OF CLEVELAND](#), [Providence House](#), [Shoes and Clothes for Kids](#), [Arkansas Foodbank](#), and [City Mission](#) for having us as w...see more". The post includes two images: a group photo of staff in front of a building and a photo of a roof being worked on.

# TECH TALK REMINDERS

Please keep your information up-to-date

- CORES and Generation Verification Forms

Following an event, send EOP-004 or OE-417 forms to [disturbance@rfirst.org](mailto:disturbance@rfirst.org)

CIP-008-6 incident reports are sent to the [E-ISAC](#) and the [DHS CISA](#)

Check our [monthly CMEP update](#) and [newsletter](#):

- [2024 ERO Periodic Data Submittal schedule](#)
- Timing of Standard effectiveness

BES Cyber System Categorization (CIP-002-5.1a)

- Assess categorization (low, medium, or high) regularly and notify us of changes

CIP Evidence Request Tool V8.1 was released and is on NERC's [website](#)




# TECH TALK REMINDER

Are you getting our newsletter  
***First Things RFirst?***

- Sign up today [here](#) -

Also, make sure to check out  
our [2023 Impact Report](#)




**First Things RFirst**  
Expert analysis for a more reliable, secure and resilient electric grid, plus news and updates for RF stakeholders.

**June 2024**

---

**Insights & Analysis**


**ReliabilityFirst 2024 Summer Reliability Assessment**



RF's Summer Reliability Assessment projects the PJM and MISO areas to have adequate resources under normal demand, but if demand or resource outages are experienced beyond those projections, there is an increased likelihood that corrective actions would be needed. This risk is low in the PJM area, but it is elevated in the MISO area.

[Click here to read more](#)

**The Lighthouse: The challenges of Operational Technology cyber security**



Our modern civilization relies on Operational Technology (OT) to keep essential services working. The electric grid, pipelines, water treatment plants, transportation systems, and many more all depend on OT to deliver reliable services. Operating these systems securely comes with a host of cyber security challenges.

[Click here to read more](#)



**FORWARD TOGETHER.**

**2023 IMPACT REPORT**

# WELCOME TO TECHNICAL TALK WITH RF

*Cybersecurity Awareness Month*

October 28, 2024



# TECH TALK ANNOUNCEMENT



## Reliability Insights

### [Grid Enhancing Technologies](#)

NERC and the ERO Enterprise has launched Reliability Insights to inform stakeholders on issues related to reliability and security of the North American grid. These brief technical documents will provide an overview of a topic, identify any critical issues and potential reliability impacts. The first one (released October 15) focuses on [Grid Enhancing Technologies](#) and dynamic line ratings.



# TECH TALK ANNOUNCEMENT



## "Currently Compliant"

### Episode 6 | EOP-011-4 Implementation Plan

NERC released the sixth installment of its compliance podcast, "Currently Compliant." This episode features Derek Kassimer, NERC senior engineer, Compliance Assurance and focuses on the **EOP-011-4 Implementation Plan**.

EOP-011-4 - Emergency Operations applies to Balancing Authorities, Reliability Coordinators, and Transmission Operators, along with some Transmission Owners and Distribution Providers that are identified in their Transmission Operators' operating plan(s) to mitigate operating emergencies. The associated implementation plan has different phased-in compliance dates for certain sections, and this update should provide clarity around the dates that entities must begin to comply.





# TECH TALK ANNOUNCEMENT



## ERO Enterprise Webinar: Inverter-Based Resource Registration Initiative

November 13 | [Register](#)

This informational webinar is designed for Category 2 GO and GOPs, and will feature presentations from NERC, the Electricity Information Sharing Analysis Center ([E-ISAC](#)), and Regional Entity staff focused on various topics and activities underway, including:

- Milestones and Work Plan
- Registration Criteria Revisions: New Category 2 GO and GOP
- NERC Standards and Compliance Expectations
- ERO Identification/Registration Process for Category 2 GO and GOPs
- Communications Resources



# TECH TALK ANNOUNCEMENT



## NERC-NATF-EPRI Annual Transmission Planning and Modeling Workshop

**November 19-20, 2024 | [Register](#)**

Register now for the 2024 virtual annual transmission planning and modeling seminar featuring industry experts sharing valuable insights, best practices, and innovative strategies to address the evolving challenges in the field of electric power transmission.

The event will be held virtually, 1:00 pm to 5:00 pm eastern each day.



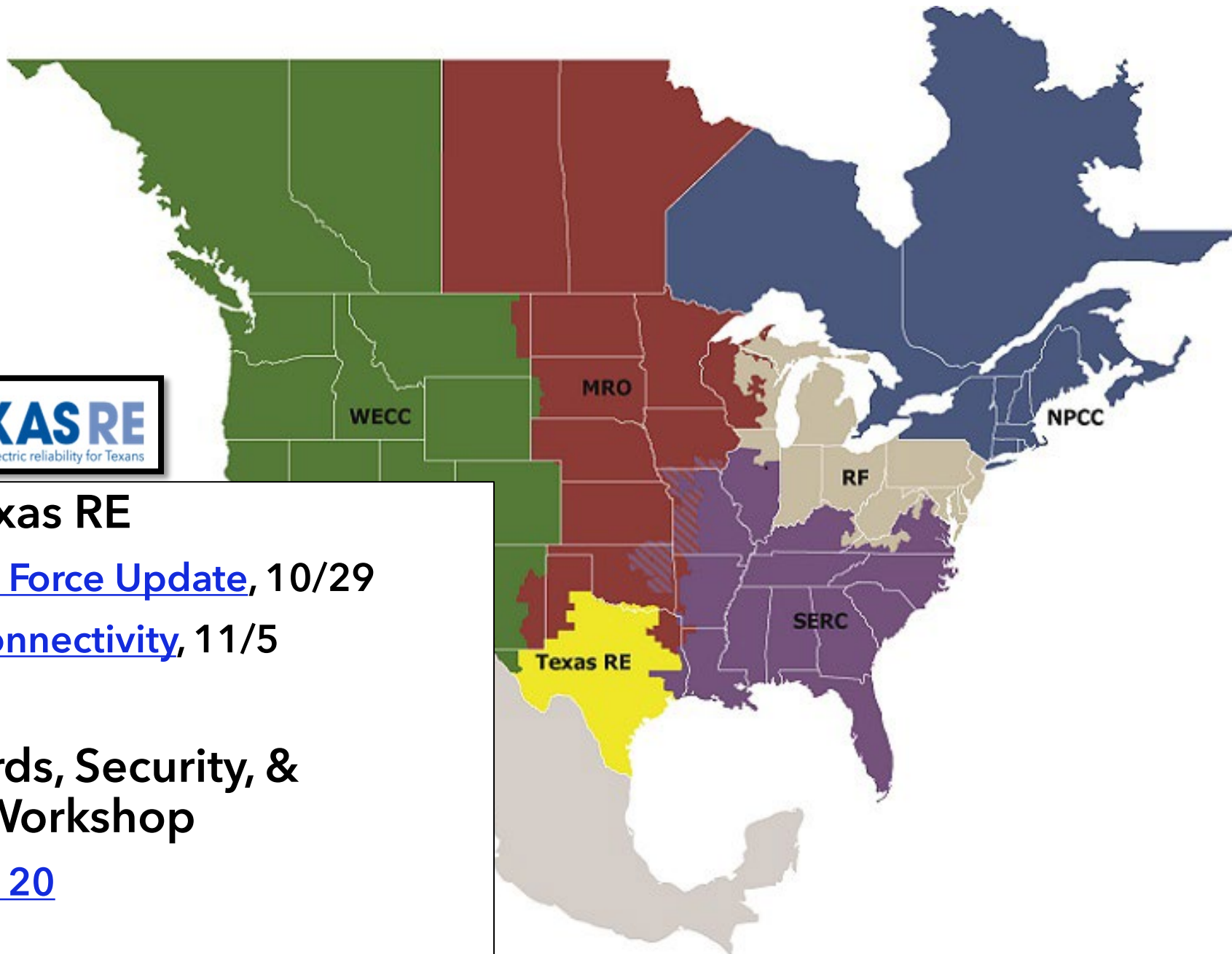


## Talk with Texas RE

- [6 GHz Task Force Update](#), 10/29
- [Remote Connectivity](#), 11/5

## Fall Standards, Security, & Reliability Workshop

- [November 20](#)





## Grid Fundamentals

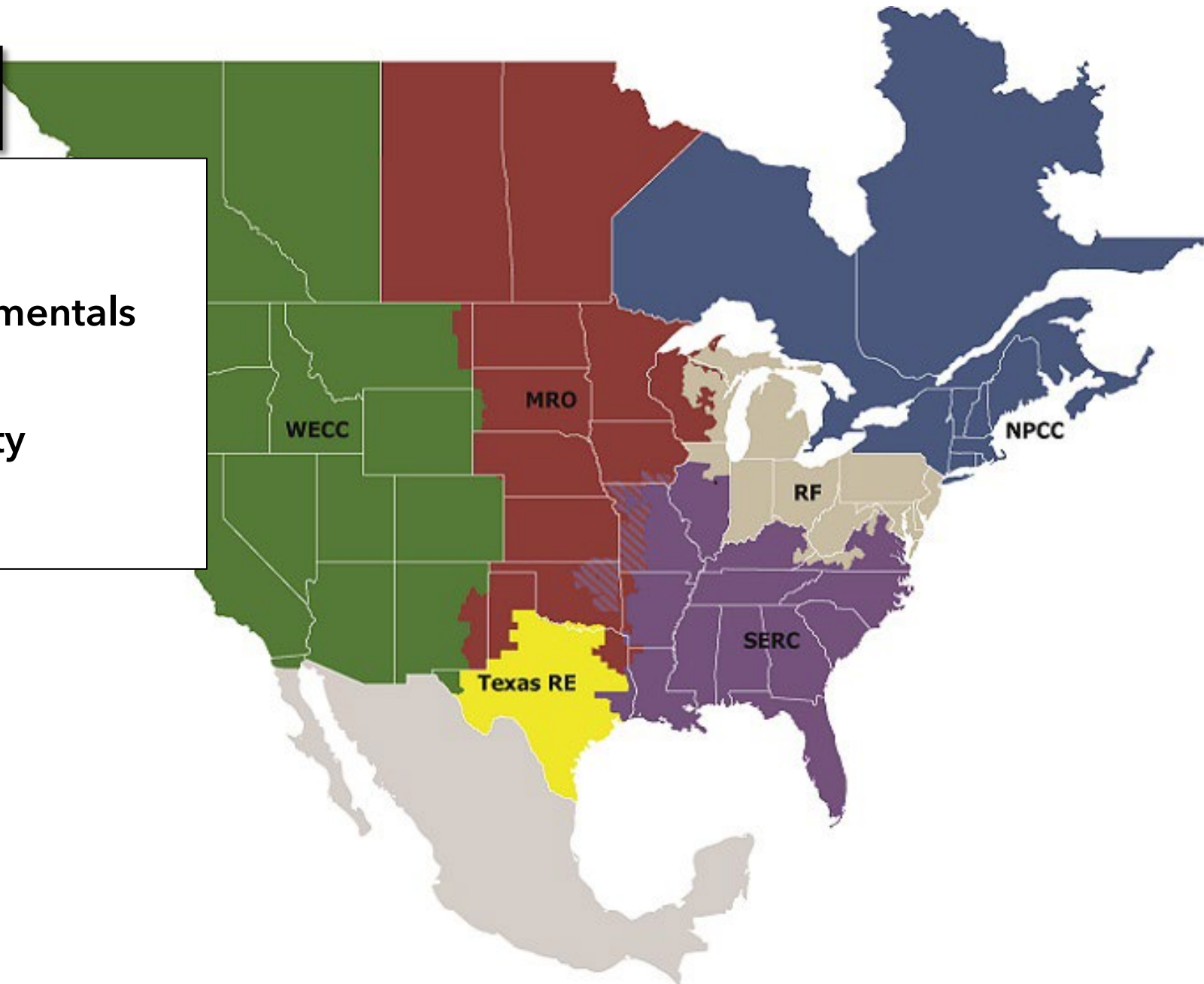
- [November 5-6](#)

## Compliance Fundamentals

- [November 14](#)

## Reliability & Security Oversight Update

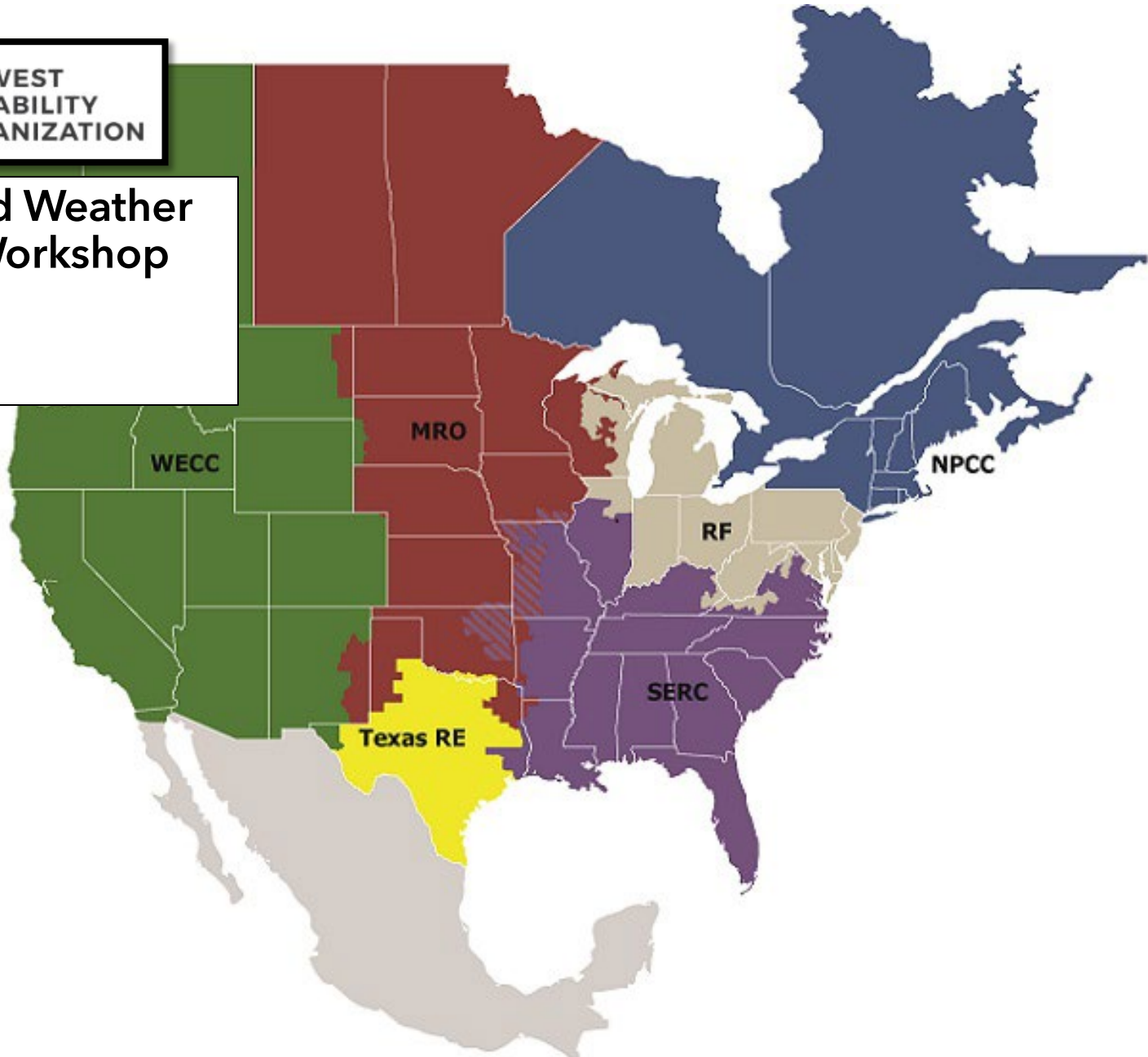
- [November 21](#)

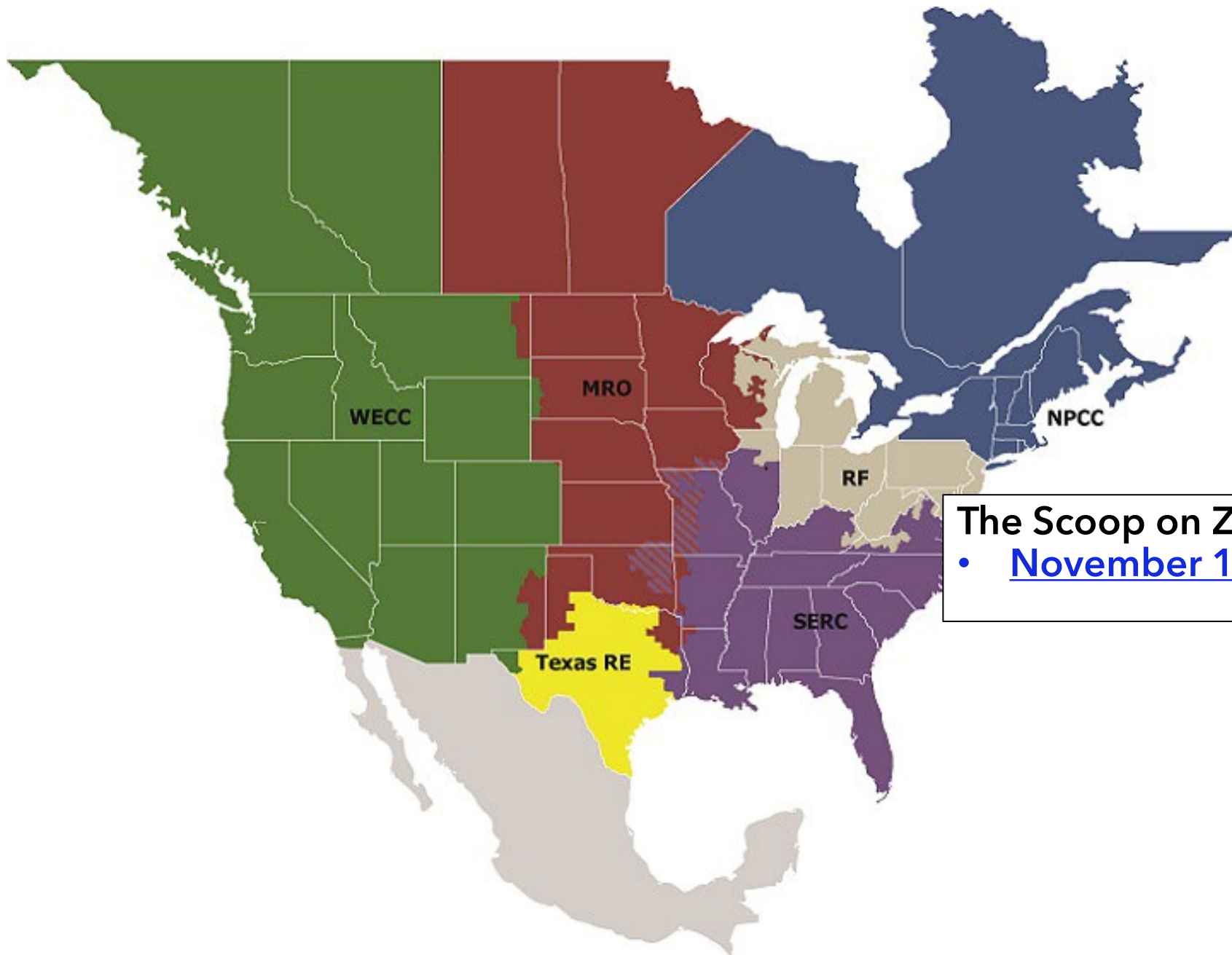




## 2024 MRO Cold Weather Preparedness Workshop

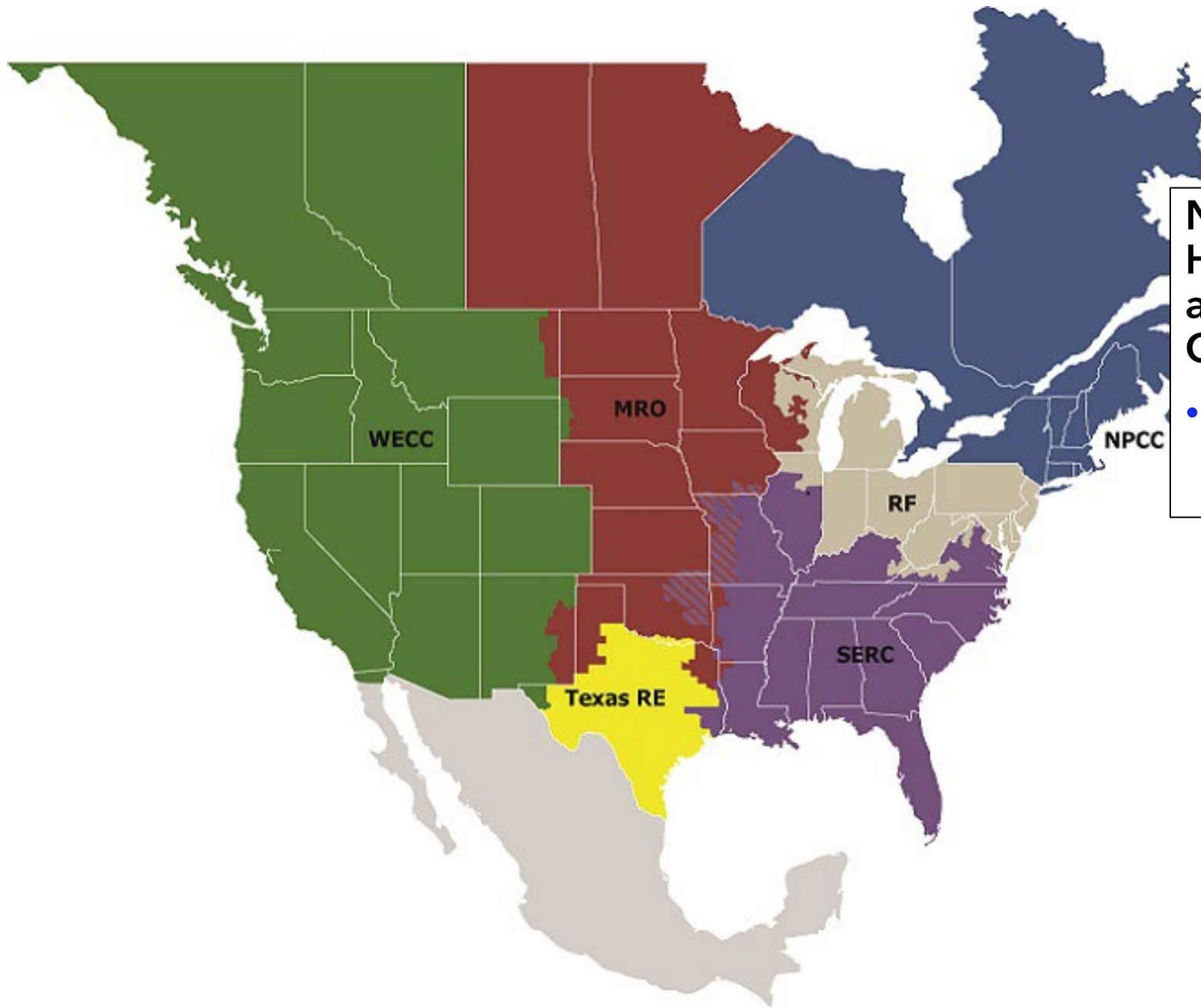
- [October 30](#)





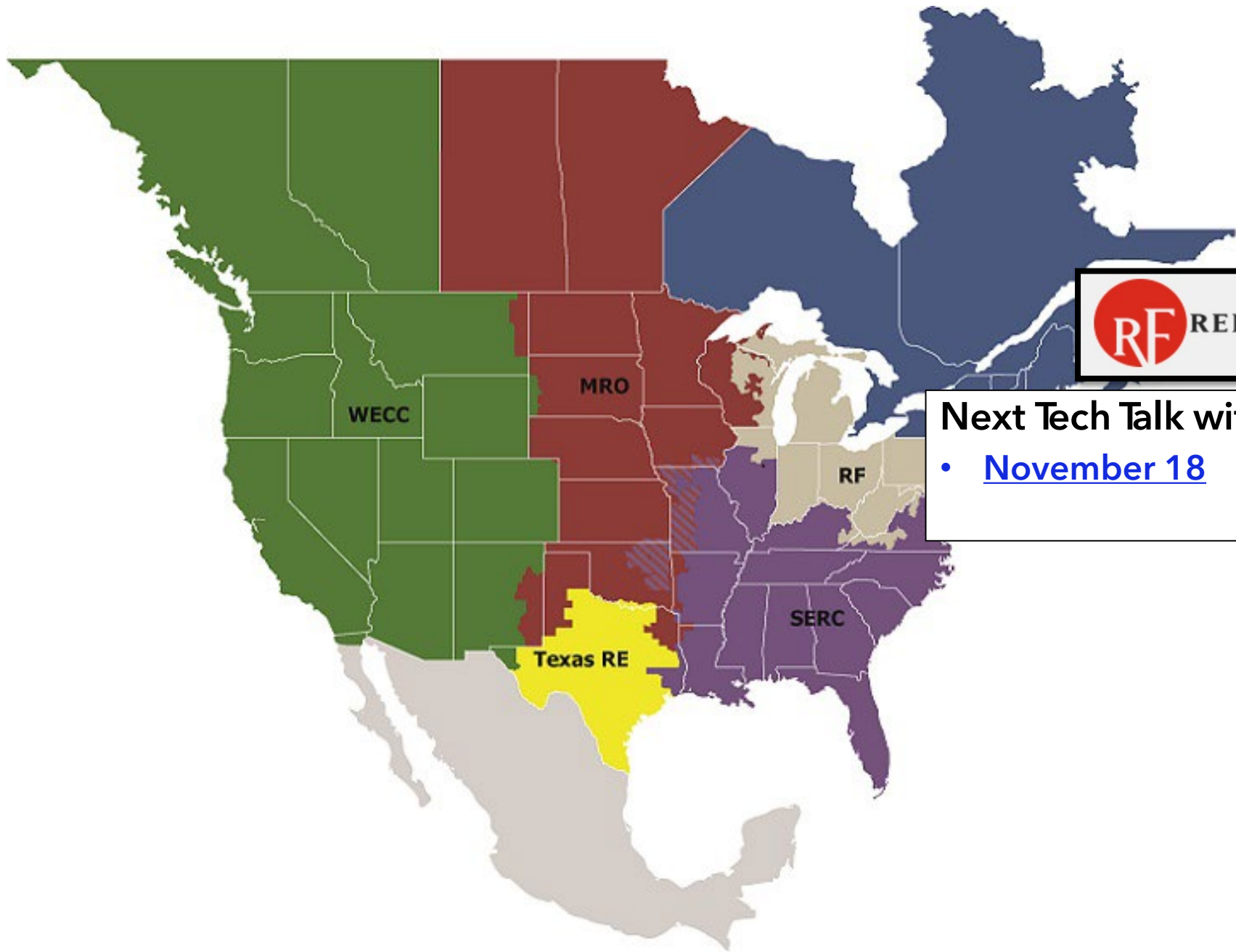
The Scoop on Zero Trust

- [November 12](#)



**NPCC Fall 2024  
Hybrid Compliance  
and Reliability  
Conference**

- [November 6 - 7](#)



**Next Tech Talk with RF**

- [November 18](#)



# TECH TALK REMINDER

*Tech Talk with RF* announcements are posted on our calendar on [www.rfirst.org](http://www.rfirst.org) under Calendar

October 2024

MON  
28

October 28 @ 2:00 pm - 3:30 pm

## Technical Talk with RF

Virtual (Webex)

Technical Talk with RF is a monthly webinar ReliabilityFirst hosts to discuss key reliability, resilience and security topics with our stakeholders.



CLICK HERE





# TECHNICAL TALK WITH RF

Join the conversation at

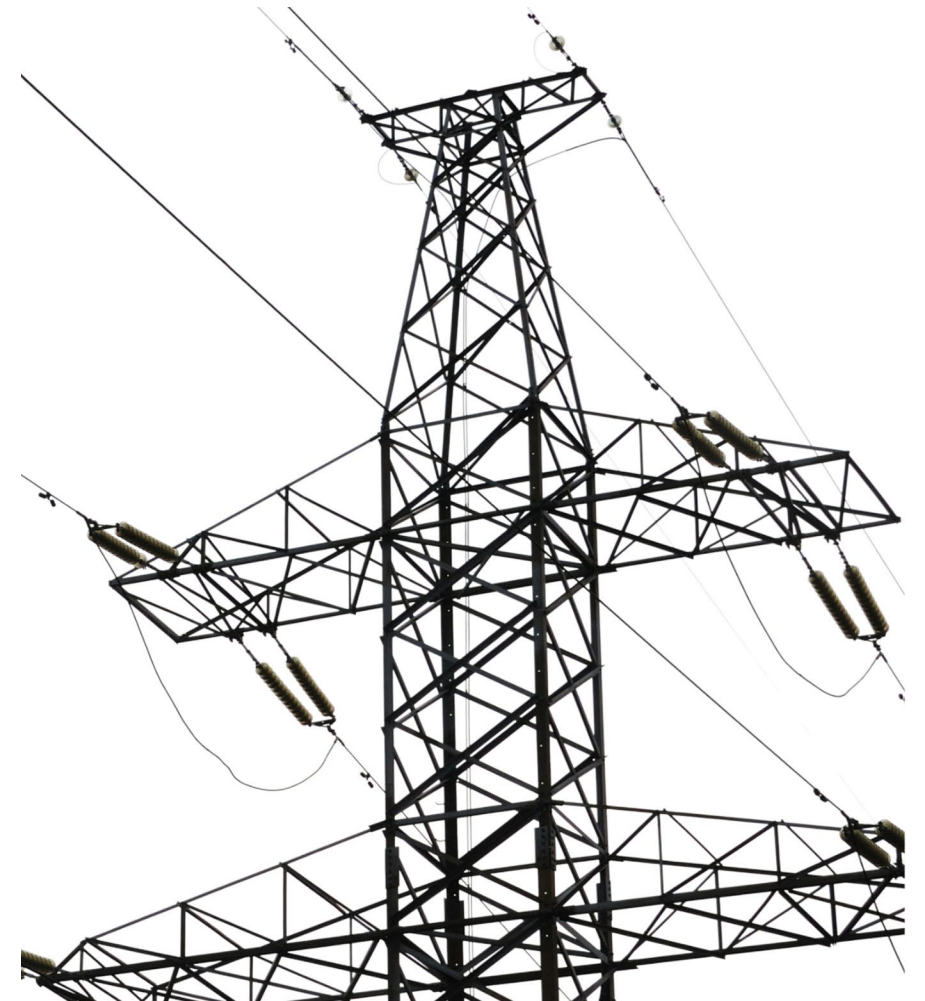
[SLIDO.com](https://www.slido.com)

[#TechTalkRF](https://twitter.com/TechTalkRF)

# Anti-Trust Statement

It is ReliabilityFirst's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct which violates, or which might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every ReliabilityFirst participant and employee who may in any way affect ReliabilityFirst's compliance with the antitrust laws to carry out this policy.



# AGENDA

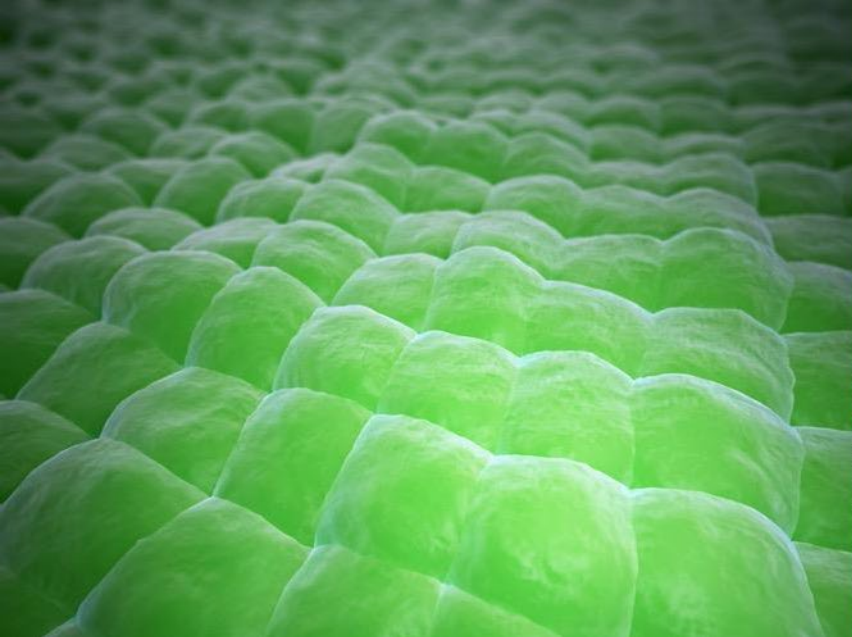
---

## CYBER SECURITY FOR CLEAN ENERGY RESOURCES

- **MEGAN CULLER**, POWER ENGINEER/RESEARCHER, IDAHO NATIONAL LABORATORY

## RISK REDUCTION THROUGH AUTOMATION

- **BRENT CASTAGNETTO**, MANAGING PARTNER, ARCHER SECURITY GROUP AND CO-FOUNDER, NOVASYNC



October 28, 2024

**Megan Culler**  
Infrastructure Security



# Cybersecurity for Clean Energy Resources

## ReliabilityFirst TechTalk

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

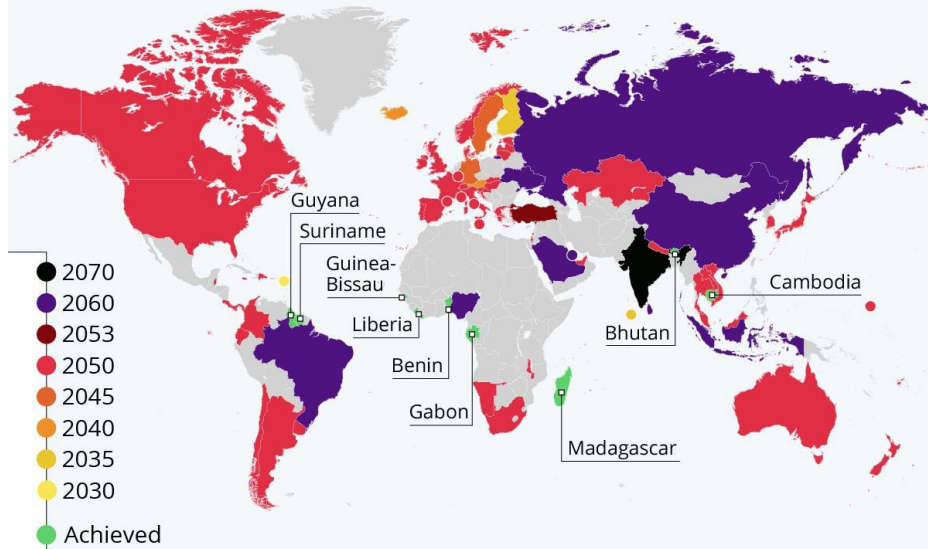


Idaho National Laboratory

# Energy Transition – Many Futures

## The Road to Net Zero

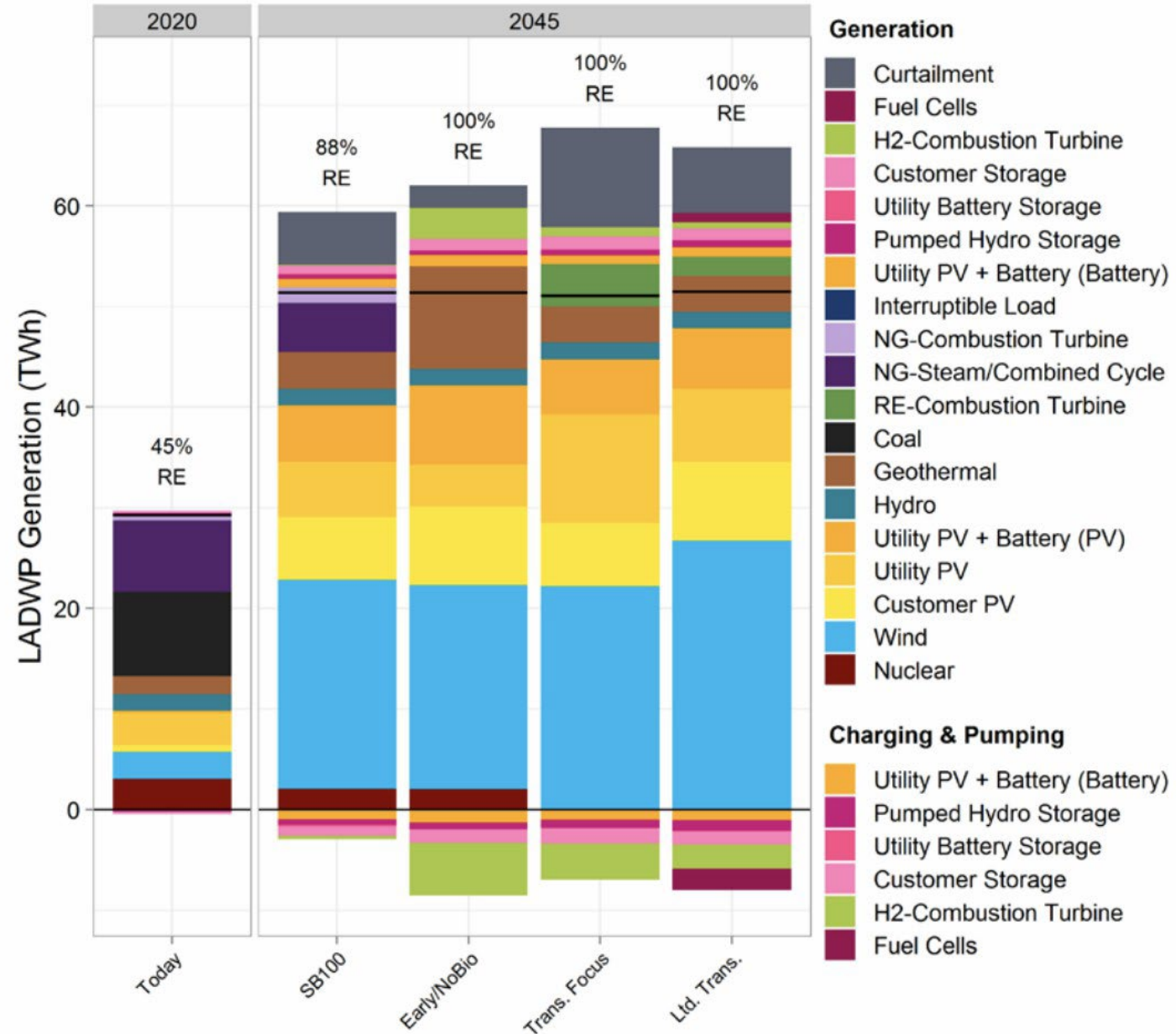
Countries with laws, policy documents or concrete timed pledges for carbon neutrality by target year



Source: Energy & Climate Intelligence Unit



- Cochran, Jaquelin, and Paul Denholm, eds. 2021. The Los Angeles 100% Renewable Energy Study. Golden, CO: National Renewable Energy Laboratory. NREL/TP-6A20-79444. <https://maps.nrel.gov/la100/>.

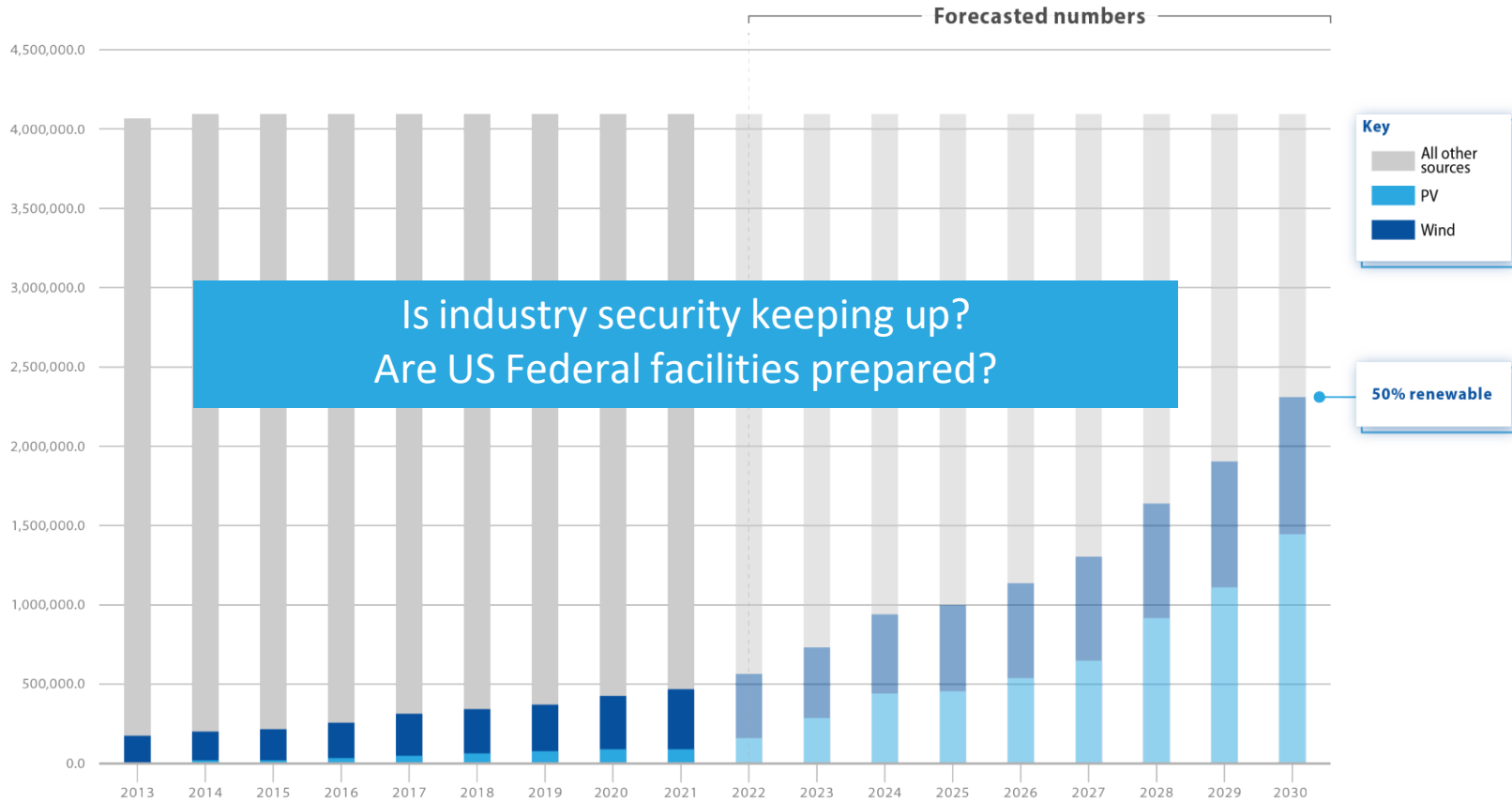


NREL LA100 Study

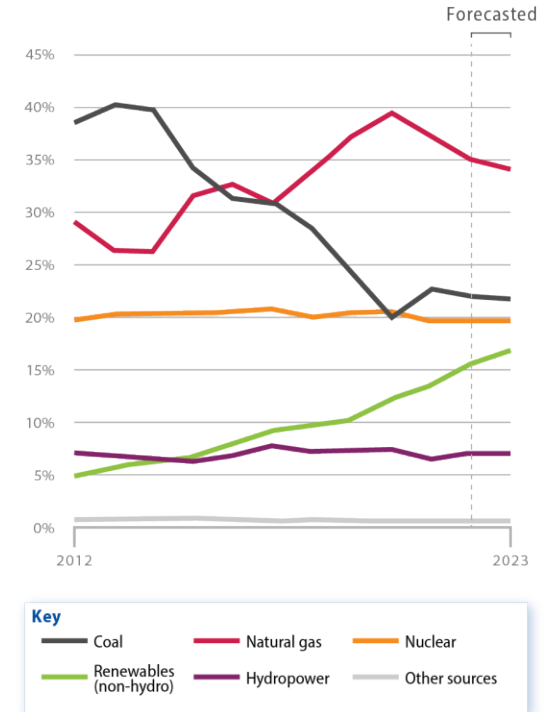
IDAHO NATIONAL LABORATORY

# To achieve high renewable energy targets of 50% by 2030, current trends will need to grow at a much higher rate.

US Total Electrical Energy (1000's MWh)



Annual US electric power sector generation by energy source



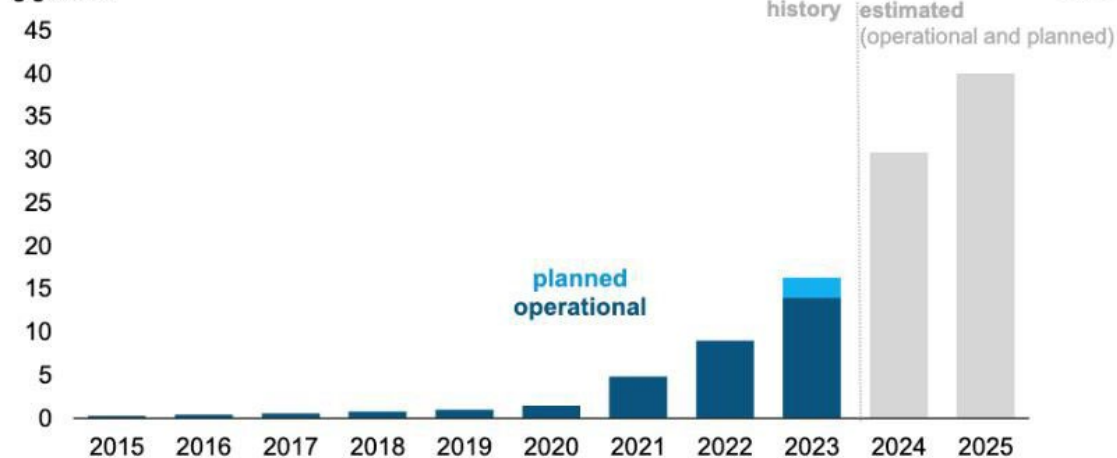
Source: U.S. Energy Information Administration, Short-Term Energy Outlook, January 2022

# How will we achieve this?

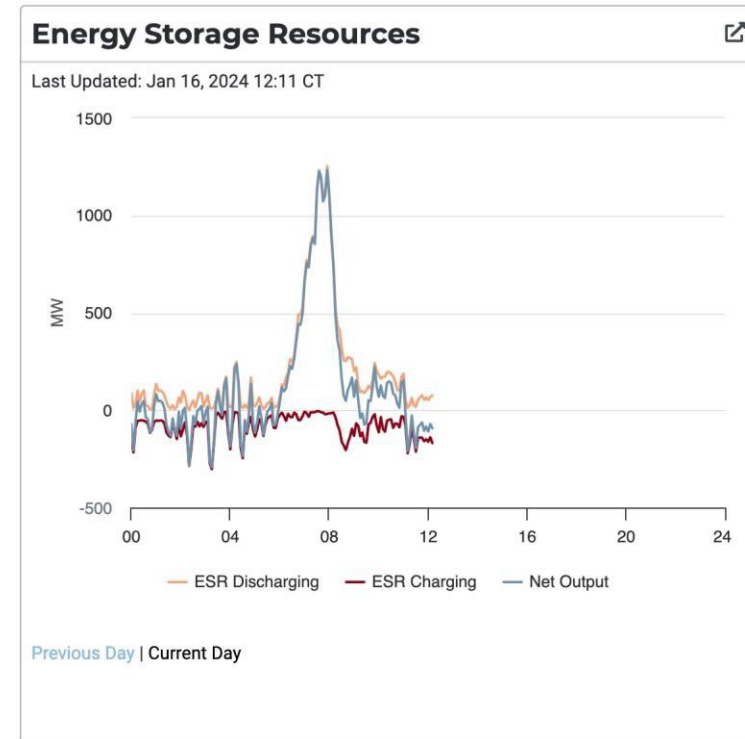
## Emerging energy markets are transforming...

- Batteries, BMS, IBR's are a core underpinning technology of the clean energy transformation
- The supply chain for batteries is overwhelmingly Chinese and is often re-branded by a US entity. There is no fast path to limiting battery investment in the US to a US-based or trustable provider.

Annual U.S. cumulative installed battery capacity (as of November 2023)  
gigawatts



Data source: U.S. Energy Information Administration, *Preliminary Monthly Electric Generator Inventory*, based on Form EIA-860M



- Utility-Scale batteries are increasingly operated by non-traditional utilities.
- Any batteries divested by U.S. utilities will end up serving grid interests from 3rd party entities.
- Many battery contracts which affect the next 5 years of installation have already been let.

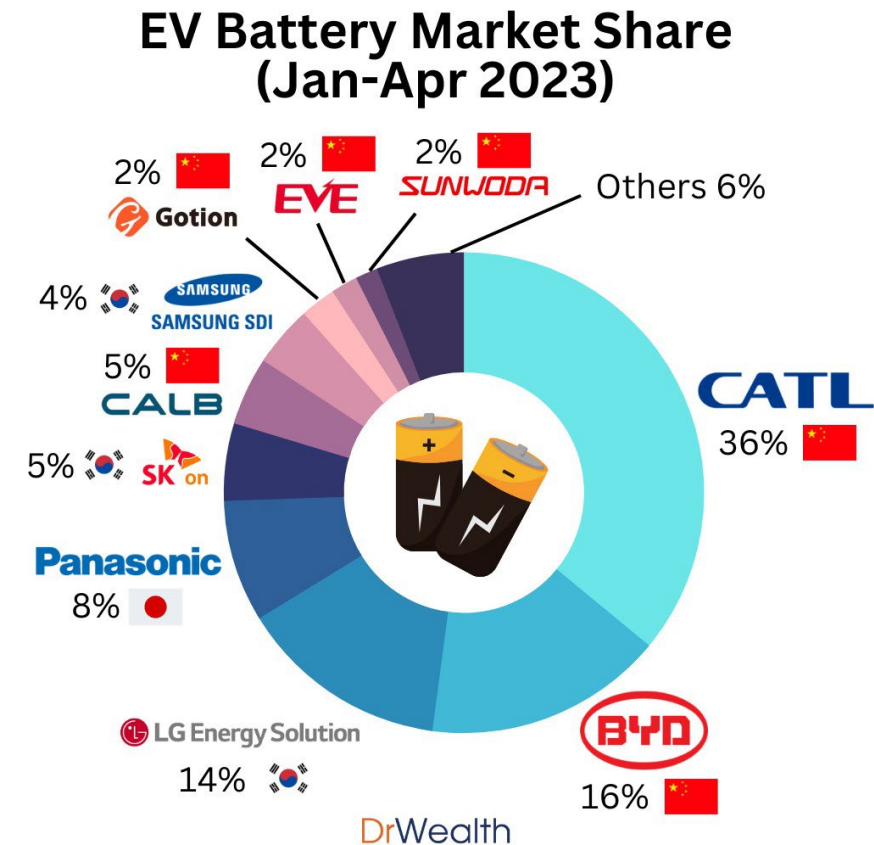


# The Current Landscape: Global Dependence on Foreign Landscape Battery Cells

In the U.S., the **top 5 country imports** of battery material as of Q2 FY23 are (note 2021 figures are provided in brackets):

- **China: 88%** (2021 = 80%)
- Hungary: 2%
- Japan: 1% (2021 = 3%)
- Poland: 3%
- South Korea: 3% (2021 = 9%)
- Malaysia: (2021 = 2%)

In the first four months of 2023, pictured are the six Chinese companies collectively controlled **62.5%** of the global EV battery market.



Problem: The penetration of CATL in the US is significant – its both integrated inside, and visible – and a major supply chain component for many

# Development Plan: How to Evaluate and Protect

(Operate large scale storage and other infrastructure with known higher risk items)



Problem: Concern over all battery/inverter supply chain from non domestic entities, request for analysis of size of problem, white paper, and mitigating strategy for utility and DOE



Mitigation menu/strategic training and workshops for consequence based/CIE approach, template & training



Key Injects: Procurement, Contracting, Design, Operations & maintenance,



Operate through, maintain the investment, resilience and reliability

# Digital Energy Ecosystem

## Changes in Digital Energy

- Growth of stakeholders →
- Growth of endpoints →
- Electrification of loads →
- Aggregation of DER →
- Increasing regulation →
- Digitization of monitoring →
- Digitization of control →
- Distribution of control →
- Smarter inverters →

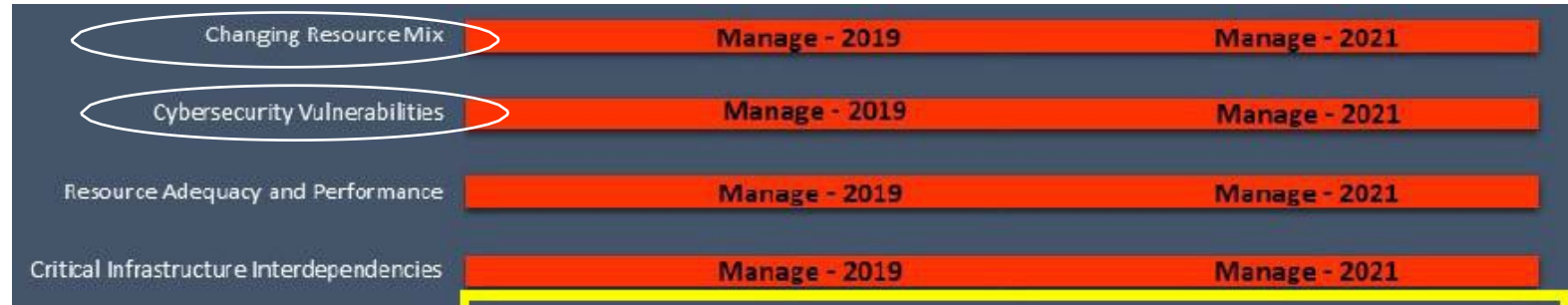
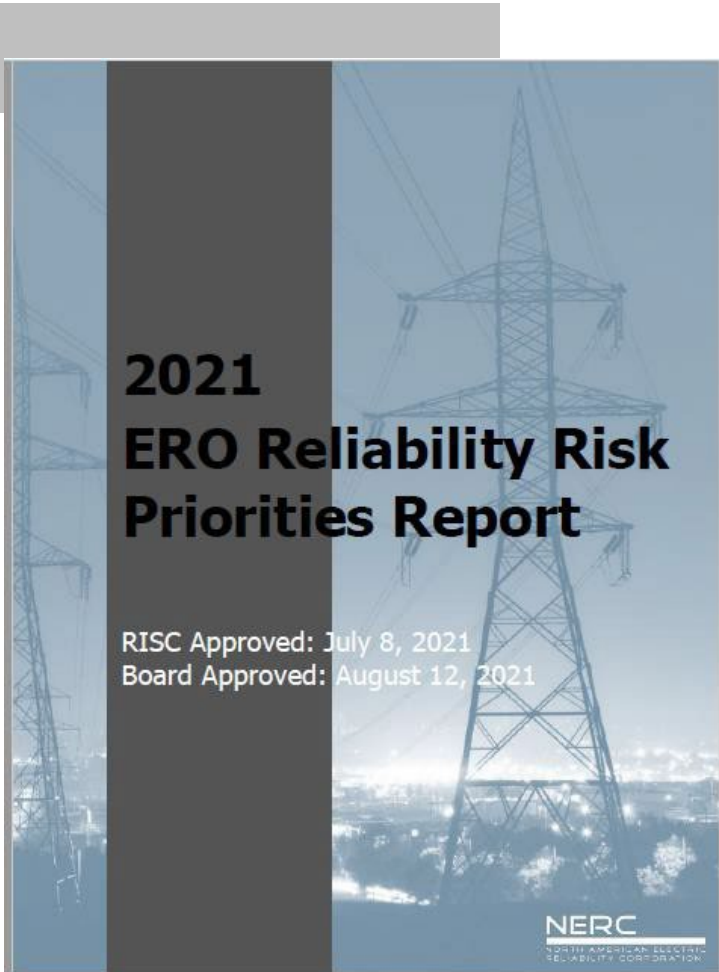
## Impact to cybersecurity

- Increase in attack surface
- Increase in attack surface, vulnerabilities
- Increase in potential impact
- Increase in potential impact
- Standards more widespread
- Explosion of data to process and store
- Need for resilience of critical functionality
- Management of roles and privileges
- Increase in attack surface

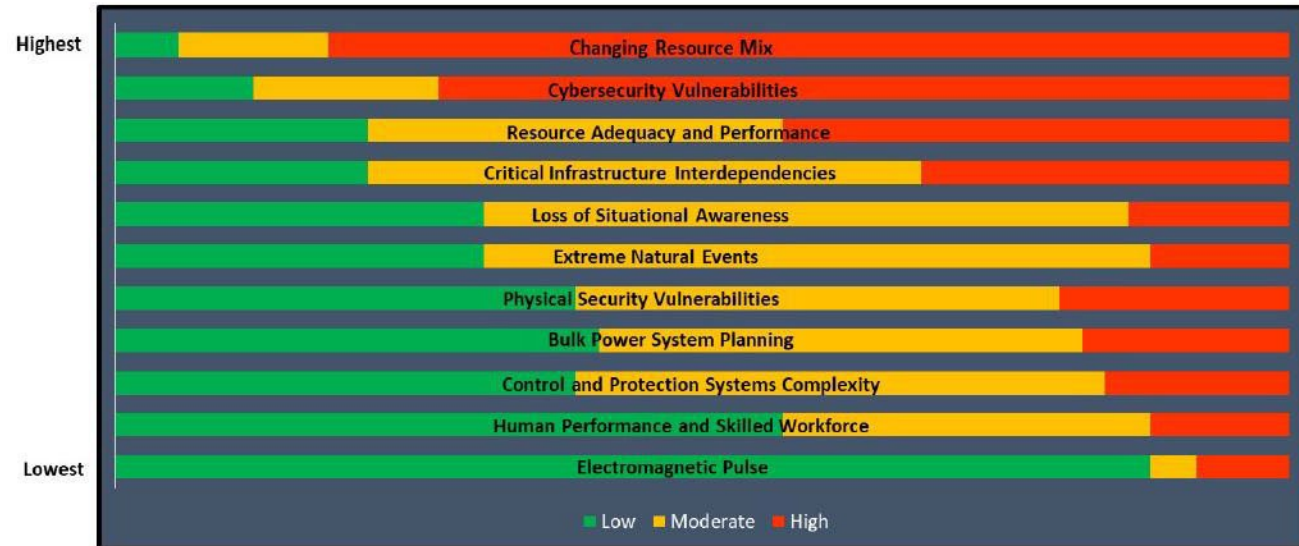
# Risk for the Grid

## Changing Resource Mix and Cybersecurity are the highest Ranked Risks

NERC Reliability - Risk



### Risk Ranking

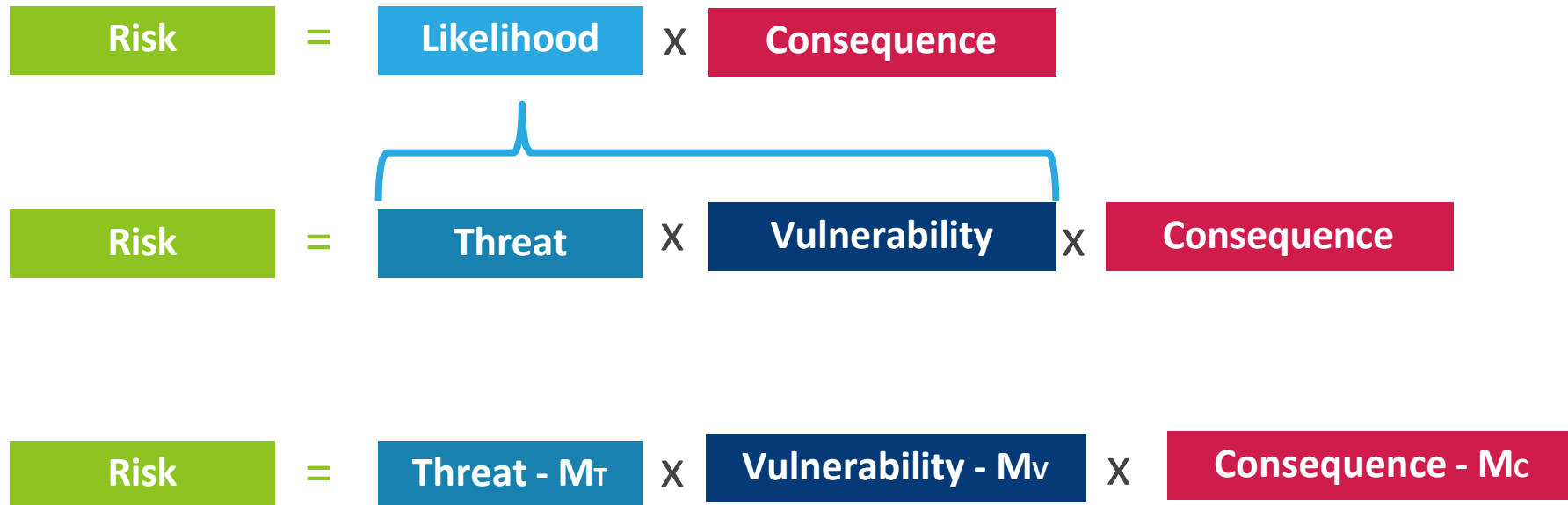


# Recent Renewable Energy Cyber Attacks



- Increased renewable sector influence
- Primary U.S. adversaries
  - China
  - Russia
  - Iran
  - North Korea
- Development of more sophisticated attacks

# Risk Management Architecture



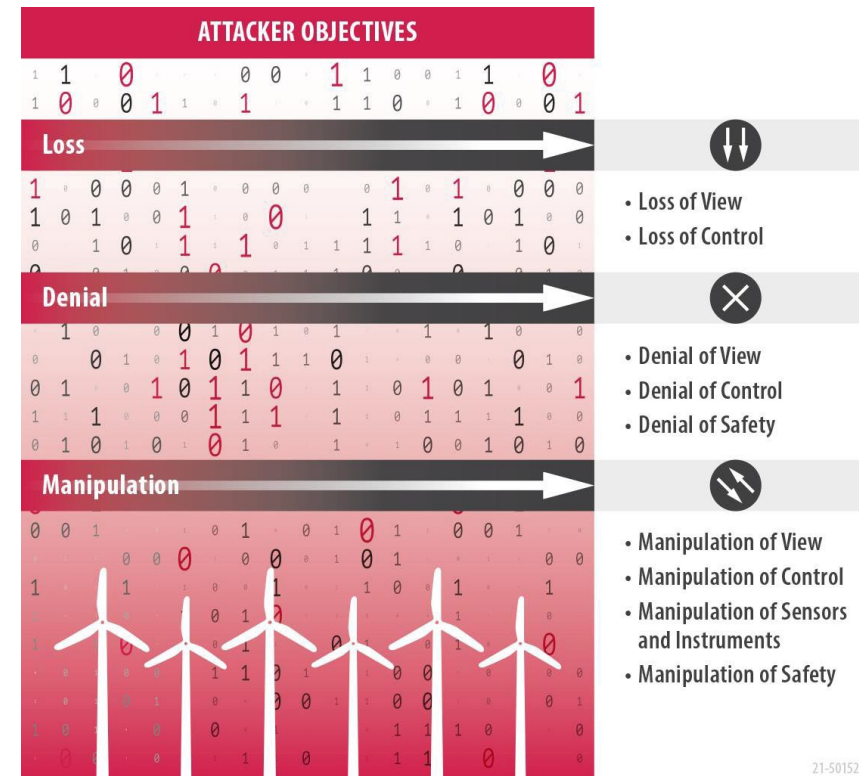
- Risk management comes from mitigating each element individually
- Cyber resilience measures can apply to any element

# Risk Management Architecture: Threats



- **Intent:** may be intentional (driven by a particular objective) or unintentional
- **Capability:** skills and funding
- **Opportunity:** Access to a target

Capability	Example
Hacker	Spower Firewall DoS attacker
Insider	AWEA technician
Organized group	Russian cybercrime or ransomware gangs
Hostile nation-state or terrorist	Nation-state sponsored APT



21-50152

# Examples of Internal Threat Actors & Known Incidents

## AOO

- Disgruntled employee
- Phishing victim

## OEM

- (March 2022) Nordex SE hit by ransomware
- (Nov. 2023) Vestas hit by ransomware

## Utility

- (May 2023) Danish utilities compromised by coordinated attack, forcing islanded operations

## Maintainers

- (2018) U.S. technician accidentally downloaded malware from hotel, later plugged into wind plant network and turbines stopped working.

## Integrators & other third-parties

- SaaS providers
- Data collectors
- Installers
- Developers



# Examples of External Threat Actors & Known Incidents

## Benign external actors

- Landowners
- Land tenants
- Land staff
- General public

## Activist groups

- (2019) Anti-wind protestors in Hawaii disrupt construction
- Rise in eco-terrorist attacks in Europe

## Criminal organizations

- Ransomware groups affected 3 wind companies within 6 months
- Exploiting known vulnerabilities for DoS or financial gain
- Ex: (2019) IPP sPower affected by denial-of-service on comms equipment

## Nation-state actors

- Reconnaissance activity and advanced persistent threats (APTs)
- Russian attack on SATCOM infrastructure affected 5800 turbines
- Chinese espionage targeting offshore wind in Strait of Taiwan and India

# Ransomware Attacks

- Vestas (November 2021)
  - Cyber incident reported (Group using Lockbit 2.0 took credit)
  - IT systems shut down across multiple business units
  - Data stolen, some personal data publicly released
  - Ransom not paid (“failed in attempt to extort”)
- Nordex SE (April 2022)
  - Conti ransomware
  - IT systems and remote access to managed turbines shut down
- Deutsche Windtechnik AG (April 2022)
  - Controlled shut down of remote monitoring for turbines
  - Regular activity restored within 3 days
  - Evidence found of Conti ransomware on IT systems
- Canadian Solar (September 2022)
  - Lockbit ransomware
  - Demanded payment to recover data, threatened to leak data

## Takeaways for renewables:

- Track reliance on third-party services and OEM access
- Ransomware continues to be prevalent, and indirectly impacts OT



# Attack Vectors

## Physical Access

- Physical device access
  - Takes time to respond to intrusions



## Cyber Access

- VPN exploitation
- Wireless
- Temporary access points
- Pivoting from enterprise network



## Transient Access

- Authorized external devices
- Infected technician equipment



## sPower Denial-of-Service (March 15, 2019)

- Utah-based independent power producer sPower
- Known vulnerability exploited in Cisco firewall
  - Forced firewalls to reboot repeatedly
  - 5-minute interruptions occurred repeatedly over 12-hour period
- Disabled communication to generation sites
  - Loss of view to field equipment and generation sites
- Did not affect power generation
  - Thought to be a test or scan
  - Adversaries may not have known what they were affecting

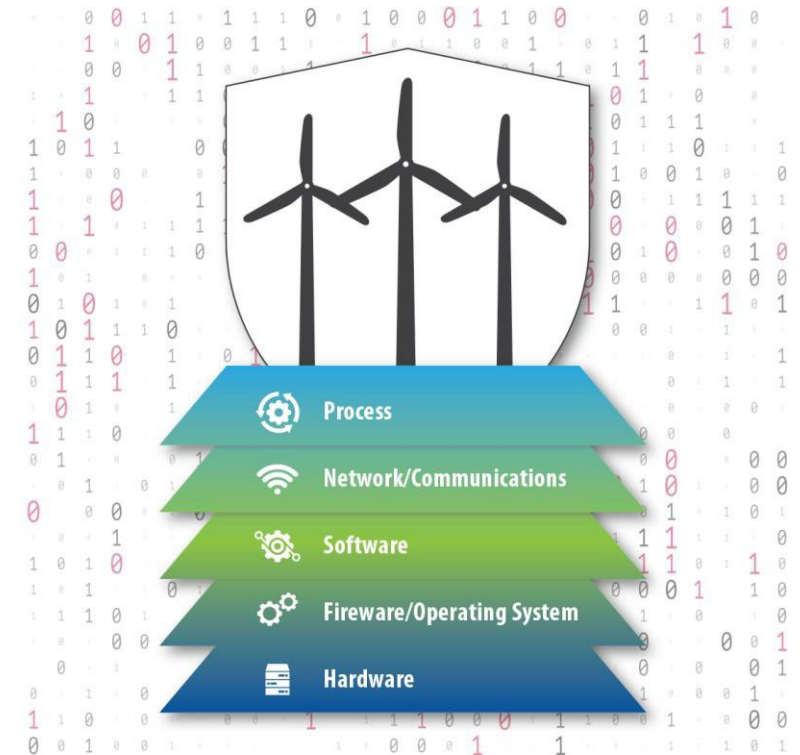
### Takeaways for renewables:

- Effective patch management strategies key
- Limit exposure of internet facing devices
- Note prevalence of IT infrastructure in the OT environment



# Risk Management Architecture: Vulnerabilities

- **Vulnerability:** a weakness which can be exploited by an adversary to gain unauthorized access to or perform unauthorized actions on a system
- May be a flaw in either design or implementation
- Can occur at any layer of the system
- Renewable examples:
  - XZERES 442SR CSFR
  - NovaWind Turbine HMI vulnerability
  - CONTEC, SMA, Enphase web vulnerabilities



# 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 renewables:

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

The Enphase logo consists of a stylized orange 'e' symbol followed by the word 'ENPHASE' in a bold, black, sans-serif font.The Fronius logo features the word 'Fronius' in a white, italicized, sans-serif font, set against a red oval background.The Contec logo includes a green circular icon with a white target-like pattern, followed by the word 'CONTEC' in a bold, black, sans-serif font.

# Solar App Vulnerabilities +

- Enphase Envoy vulnerabilities (2023)
  - ICSA-23-171-01 & ICSA-23-171-02
  - Enphase Envoy is a communications gateway that transmits home solar energy system performance data to the MyEnlighten portal
  - Wired connection to microinverter, connected through user’s router or cell modem to MyEnlighten
  - Used for monitoring and automatic software updates
  - Control features include power export limiting and zero-export applications
  - OS Command Injection in the gateway allows root access
- CONTEC vulnerabilities (2023)
  - CVE-2022-29303 unauthenticated and remote command injection vulnerability
  - Less than 1/3 of internet-facing SolarView systems patched against this vuln.
  - CVE-2023-23333 command injection vulnerability affecting downloader PHP webpage
  - CVE-2022-44354 file upload vulnerability enabling webshell
- Growatt solar panels
  - Independent researcher found that by changing the “plant ID” or “serial number” in web requests allowed access to anyone’s inverter
  - Worst consequence was switching off the inverter
  - Growatt fixed the issue, but disclosure process was difficult.

## Takeaways for renewables:

- Web portals seen with several simple vulnerabilities.
- Potential high impact through command injection.

**TOTAL RESULTS** 615

**TOP PORTS**

Port	Count
80	460
8010	38
81	19
8000	19
8080	11

**TOP ORGANIZATIONS**

Organization	Count
Open Computer Network	235
ASAHI Net,Inc.	96
NIFTY Corporation	31
BIGLOBE Inc.	26
GMO Internet,Inc.	26

**TOTAL RESULTS** 425

**TOP PORTS**

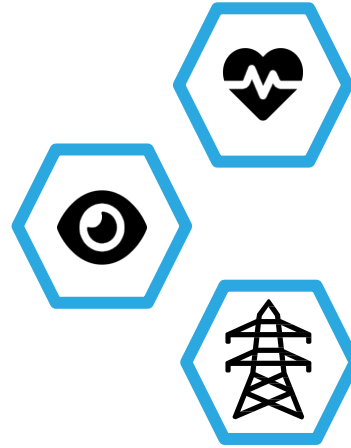
Port	Count
80	328
8010	35
81	10
8000	9
50000	6

**TOP ORGANIZATIONS**

Organization	Count
Open Computer Network	156
ASAHI Net,Inc.	78
BIGLOBE Inc.	24
NIFTY Corporation	21
GMO Internet,Inc.	20

# Risk Management Architecture: Consequences

- Asset health and damage
- Loss of remote monitoring
- Power system stability



*Critical failures can lead to severe physical damage.*

- Ancillary services
- Power dispatch
- Reputational damage





## ViaSat Denial-of-Service (February 24, 2022)

- 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
  - Made the modems unable to access the network
  - Required replacement devices
- Caused loss of remote monitoring of 5,800 ENERCON wind turbines
  - 1217 wind farms, 10GW generation capacity
  - Customers relied on ENERCON's infrastructure – no backup links
  - Took almost two months to bring 95% of turbines back online

## Takeaways for renewables:

- Risk associated with reliance on third-party infrastructure
- Renewables may be a casualty, even if not a direct target



# Center for Securing the Digital Energy Transformation (CSDET)

## Clean Energy



Energy Delivery



Cybersecurity



Communications

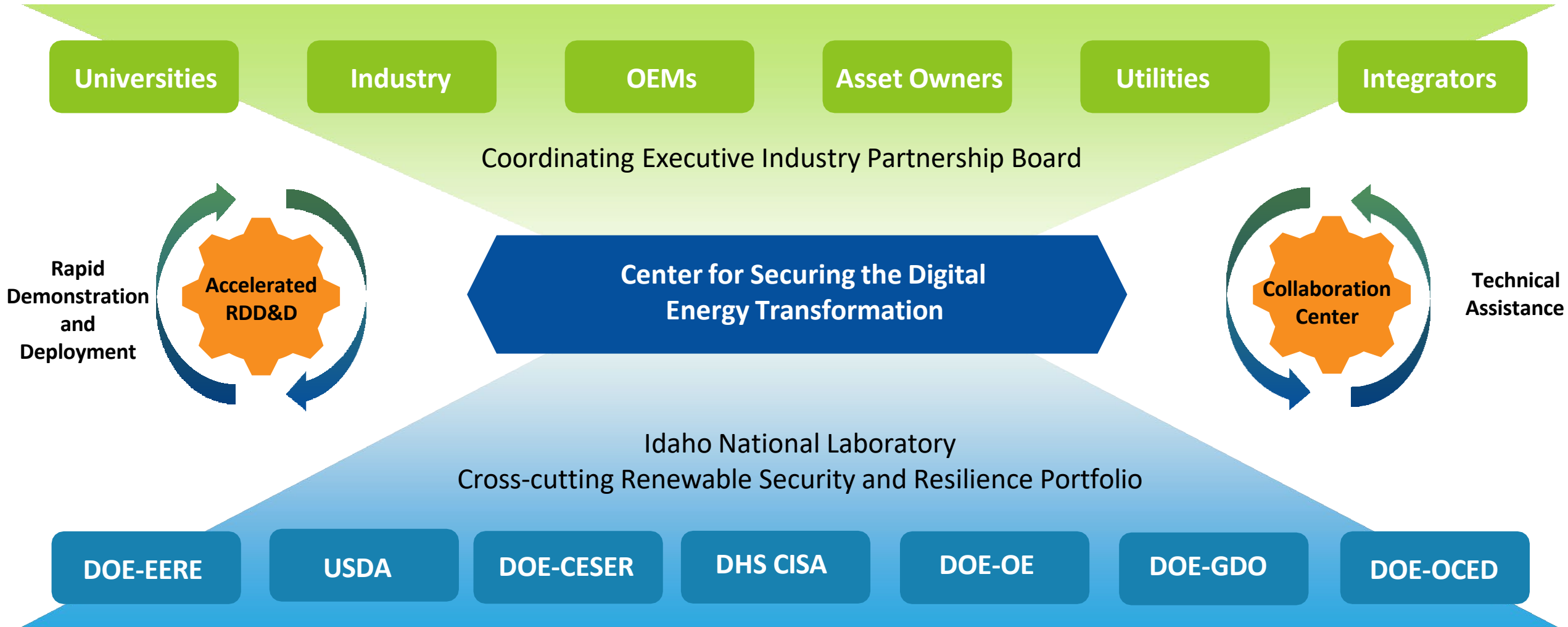
## Why Now / Why INL?

- Energy transition snowball is rolling
- Grid's traditional view of renewable threats is not accurate
- Few work in the intersection of security, grid and renewables with cross agency capabilities
- NERC ordered to develop **IBR Performance Standards** – those will include security
- **Standards harmonization** for DER and **WH Task Force** on Renewable Security
- DOE OE EAC recommendations on **inverter security**
- **Interconnection** rules and queue

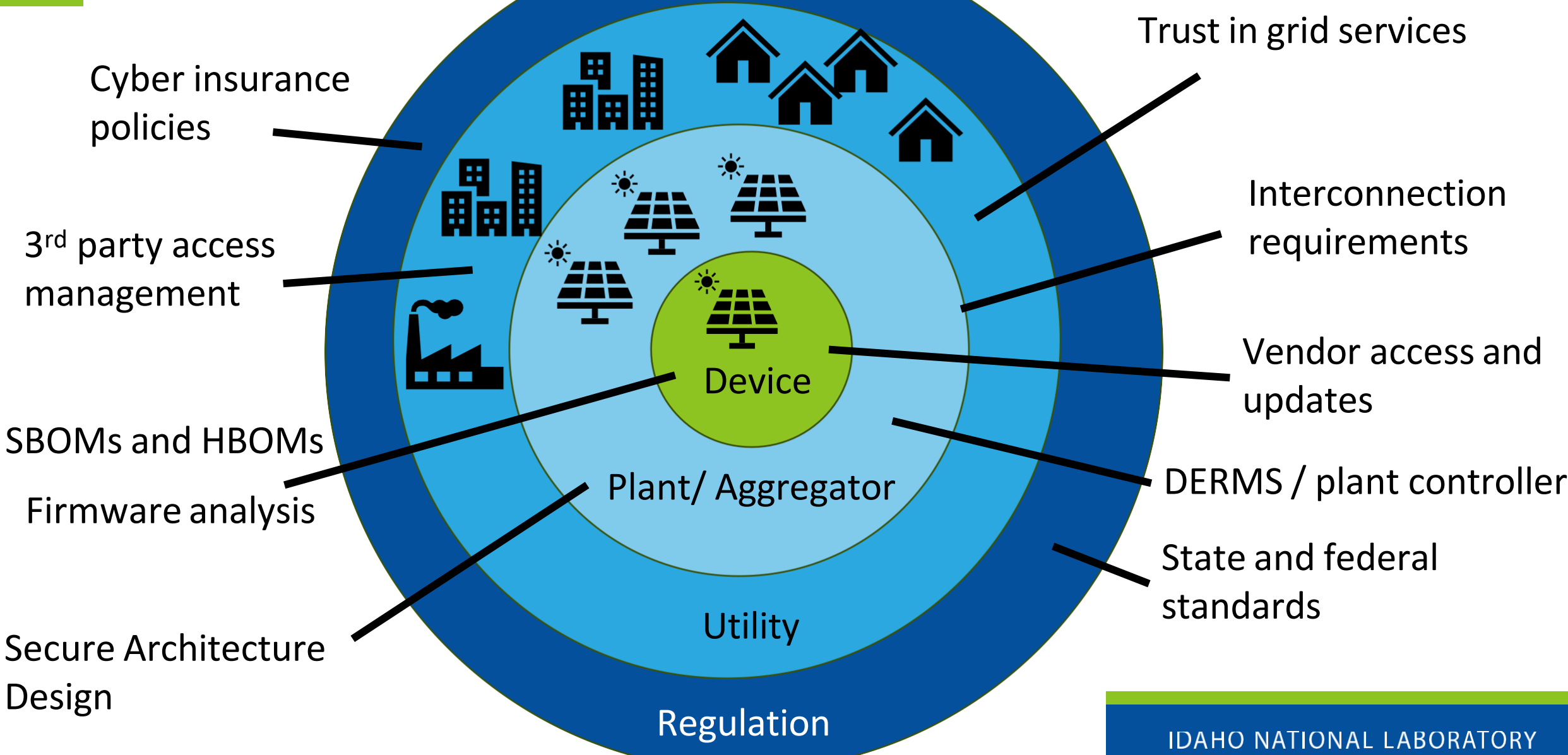
# Impact Model



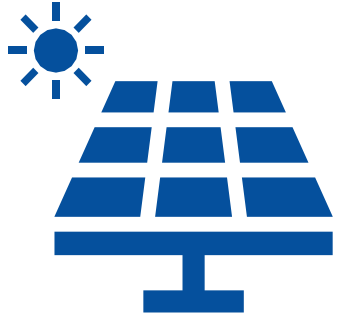
# Coordination & Collaboration Model



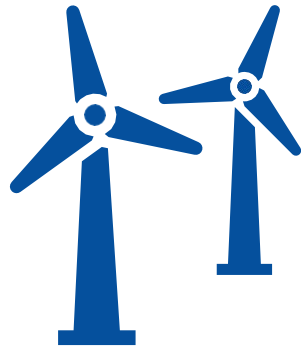
# Where do we start?



# Device level: Why do different technologies require different cybersecurity considerations?



- Wide range of vendors with varying maturity
- Diverse stakeholder ecosystem



- Smaller number of large vendors, higher vendor maturity
- Lots of physically moving parts
- Physical access to remote areas feasible



- Bi-directional power flow
- Typically more controls



- Smart device connections
- Load control vs. generation



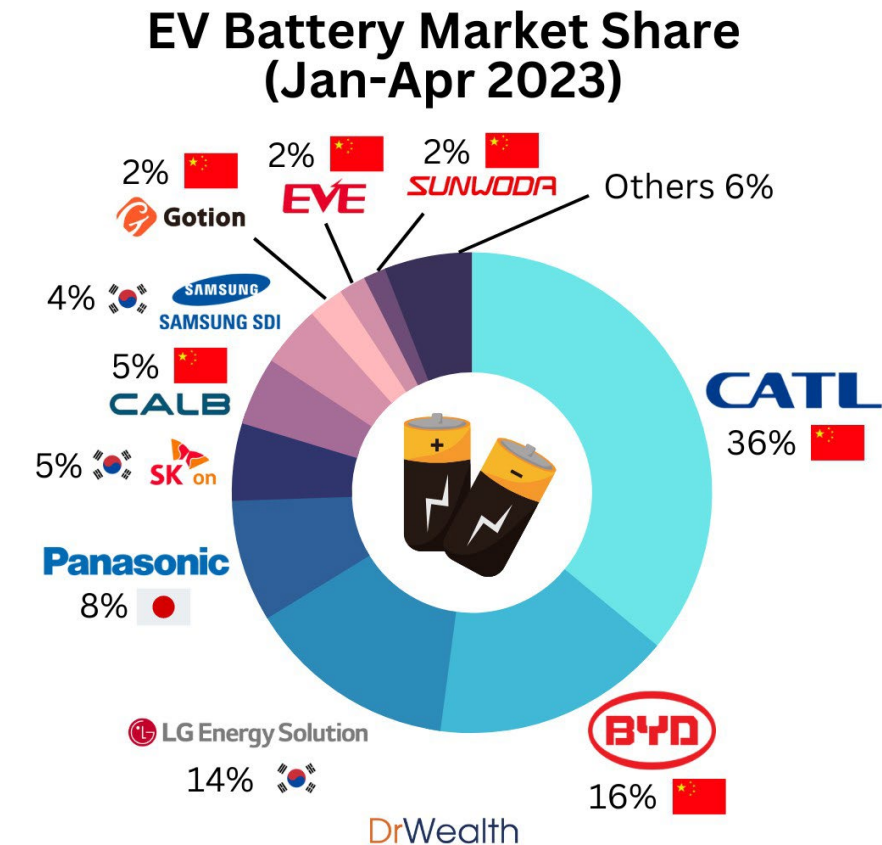
- Privacy and personal data considerations
- Direct cross-sector impacts

# The Current Landscape: Global Dependence on Foreign Landscape Battery Cells (Supply Chain... where we are at today)

In the U.S., the **top 5 country imports** of battery material as of Q2 FY23 are (note 2021 figures are provided in brackets):

- **China: 88%** (2021 = 80%)
- Hungary: 2%
- Japan: 1% (2021 = 3%)
- Poland: 3%
- South Korea: 3% (2021 = 9%)
- Malaysia: (2021 = 2%)

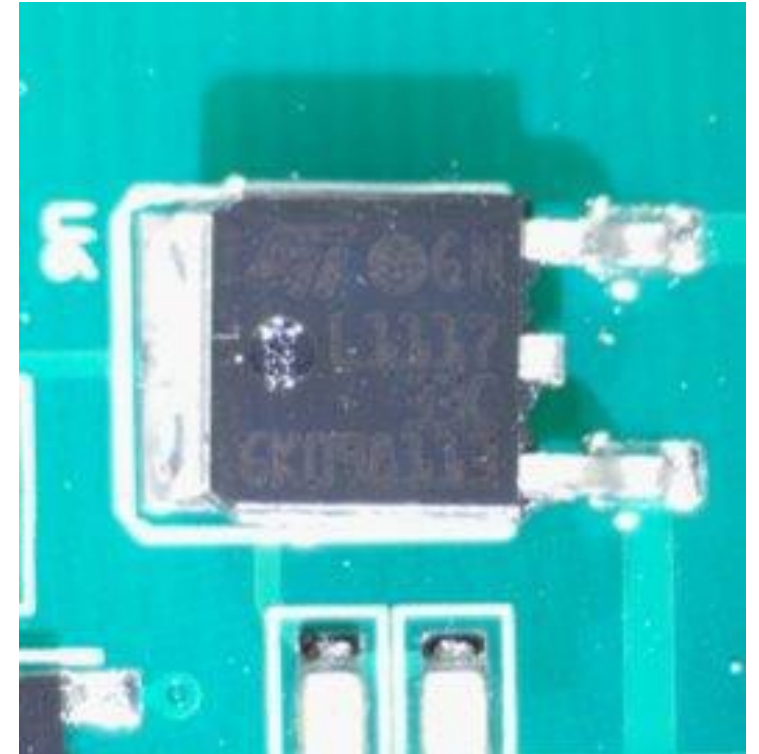
In the first four months of 2023, pictured are the six Chinese companies collectively controlled **62.5%** of the global EV battery market.



# Device-level Research: HBOM Enumeration

## Solar inverter example

- Identifiers pulled directly from individual component
  - Identifier
  - Pin package
  - Vendor
- Identifiers from researching individual component
  - Pin package
  - Description
  - Vendor
  - Model
  - Official Name

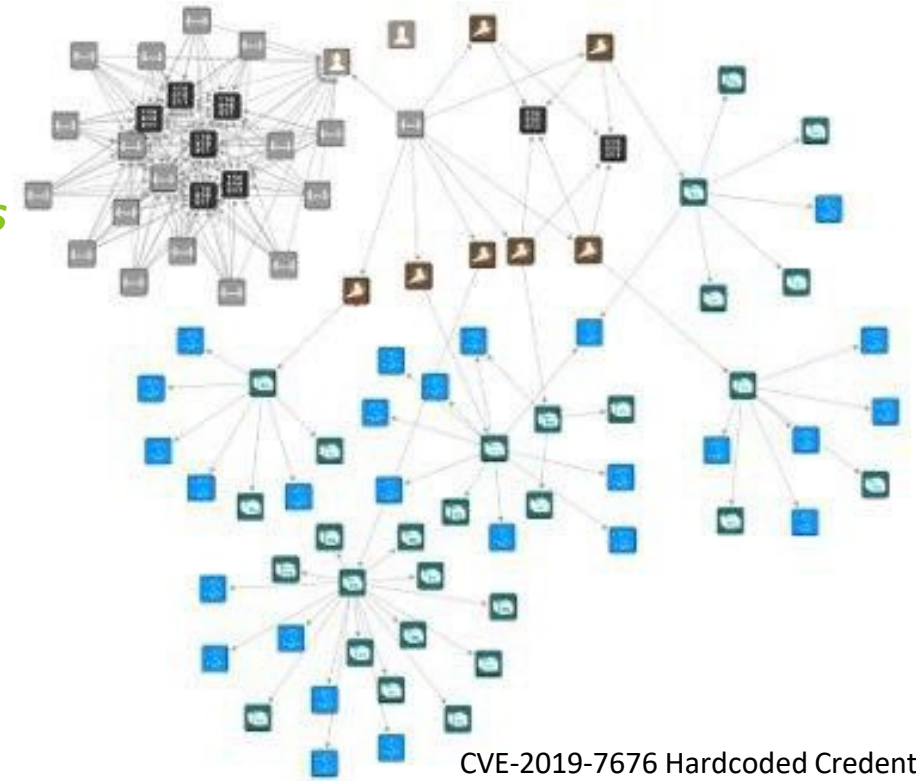




# Device-level Research: Automated firmware analysis and enumeration of common weaknesses and attack patterns



*Most common weaknesses*  
*Most used attack patterns*



STIX Objects	Pre	Delta	Post-WAVgraph
Relationships	2,213	+935	3,148
Weaknesses (CWEs - group)	0	+129	129
ATTACK/CAPEC - Patterns	0	+167	167
Vulnerabilities (CVE)	32	+0	32
Known Exploits (KEV)	0	+0	0
Software (CPEs - software)	103	+112	215*
Infrastructure	238	+0	238
Identity	32	+0	32
Note	10	+0	10
Total	2,628	+1,343	3,971

CVE-2019-7676 Hardcoded Credentials  
 CVE-2019-7677 XSS  
 CVE-2019-7678 Directory Transversal  
 CVE-2020-25752 Hardcoded Credentials  
 CVE-2020-25753 Weak Default Password  
 CVE-2020-25753 Weak Password Hash  
 CVE-2020-25755 Arbitrary Command Execution

# Procurement Guidance for BESS



## Overview of the BESS Procurement Guide

The battery energy storage system (BESS) Procurement Guide provides comprehensive guidance informed by industry best practices to BESS Consumers on how to incorporate cybersecurity requirements into the procurement process to enhance both BESS supply chain security as well as SCRM programs.

This BESS Procurement Guide will help entities integrating digital energy infrastructure accomplish the task of quickly developing and maturing cybersecurity supply chain risk management programs and maximize their ability to manage non-domestic equipment appropriately.

### SUPPLY CHAIN SECURITY FOR BESS AND IBER BESS, Inverter-based resources (IBR), and other

Name  
208-xxx-xxxx  
[lower.case@inl.gov](mailto:lower.case@inl.gov)  
[www.inl.gov](http://www.inl.gov)



energy sector digital equipment could present, and are perceived to present, security risks due to the nature of their architectures, such as persistent communications, organizational challenges with foreign ownership, and unknown spiderwebs of components. Many of these challenges can be aided with enhanced SCRM focused on procurement processes and contract terms.

Through procurement guidance that integrates SCRM considerations, organizations can mitigate supply chain risks from the start. Some of the guidance focuses on eliminating risk, while other guidance introduces risk transfer, requiring other stakeholders to take on some of the responsibilities of ensuring security of components throughout their lifecycles.

plays a critical role in the effective management of BESS, IBR, and other energy sector digital system supply chain cybersecurity risks by implementing cybersecurity considerations as part of the vendor selection and purchase processes, the organization sets a standard for vendor security maturity to ensure suppliers have also prioritized security.

Some key cybersecurity challenges present in the majority of digital equipment include:

- Remote monitoring and control capabilities, expanding adversary attack surface.
- Remote software and firmware update capabilities, which allow suppliers to quickly deploy patches, but also exposes the equipment to the potential of malicious firmware uploads.
- Reliance of critical systems on the software and firmware in digital equipment.
- Capability to rapidly change the functionality or behavior of devices through malicious or error-filled code updates.
- Proliferation of stakeholders who need, or claim to need, access to digital devices and their data.

**BESS Vendor Risk Assessment** – This section contains a basic risk analysis and impact factors, decision trees for initial evaluation, and risk assessment methodology guidelines. It includes content for the BESS vendor assessment in the context of organizational risk, discussing cyber supply chain security risk considerations specific to BESS, IBR, and energy digital equipment. The methodology provides guidance for classifying service and product suppliers into three tiers corresponding to low, medium and high risk.

**BESS Procurement Agreement Terms** – This section provides sample terms and conditions for vendor agreements to mitigate security and supply chain risks associated with procurement of digital assets and services, including software and hardware bill of materials requirements. The sample terms cover topics including disclosure of security events, incident response, vulnerability disclosure, access to systems, and more. Supplier management controls to ensure cyber SCRM processes are effectively integrated by both suppliers and the organization.

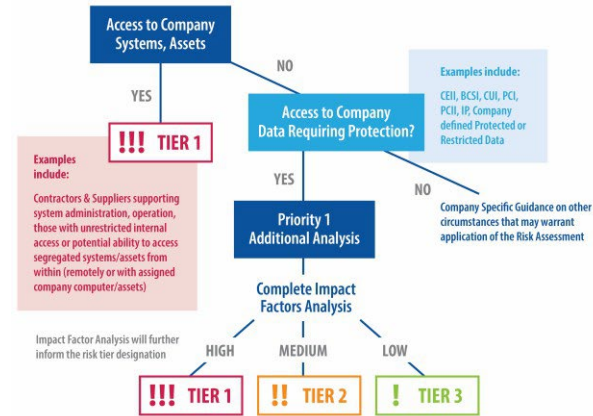
For additional information on INL Digital Assurance project initiatives and other available resources visit the [Center for Securing the Digital Energy Transition](http://Center for Securing the Digital Energy Transition).



## Final Selection Approval & Supplier Communications

## SERVICES SUPPLIER ANALYSIS

Illustrative: Sample Initial Analysis Risk Decision Tree for Services Suppliers



Impact Factor Analysis should include the following in addition to company specific considerations:

- Operations – Grid
- Operations – Internal
- Operations – Business Systems (IT, Finance, Billing)
- Reliability – Grid systems, and more.
- Security – Cyber, Physical

Determination of Initial Risk Tier guides Decisions about the application of Risk Assessment & security specific procurement terms.

- TIER 1 HIGH RISK** Complete full Risk Assessment for Tier 1 Suppliers & use all applicable Cybersecurity & Supply Chain procurement terms (based on company risk profile and preferences).
- TIER 2 MEDIUM RISK** Complete full or partial Risk Assessment for Tier 2 Suppliers & use any applicable Cybersecurity & Supply Chain procurement terms (based on company risk profile and preferences).
- TIER 3 LOW RISK** Complete partial Risk Assessment for Tier 3 Suppliers if warranted & use any applicable Cybersecurity & Supply Chain procurement terms (based on company risk profile and preferences).

Some organizations may create "Tier 1, 2, 3" categories for the Cybersecurity & Supply Chain Risk Procurement Terms to be included to provide additional guidance.

Ex: Risk decision tree for services suppliers

## Plant/Aggregator level

- Focus on one technology type
- Responsible for production
- Managing responses collectively to the utility
- Update and patch management

# Device-level Research: Pentesting of storage controller in microgrid application

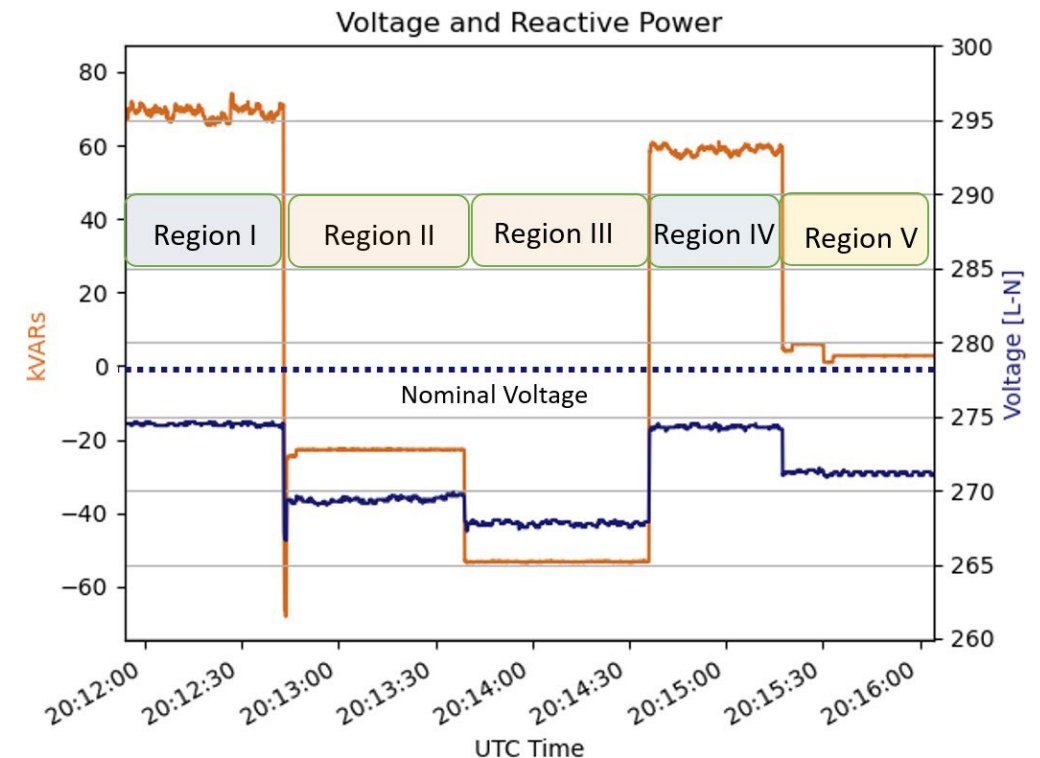
- Plum Island Microgrid Test Bed
  - GMLC project added renewables, storage and sensors to the existing Plum Island experimental microgrid, originally constructed to support the DARPA RADICS program
  - Equipment added included: Two 100kVA grid-forming batteries, 20kW solar PV, power meters with PMU and oscillography capture functionality, data logging and visualization system



# Device-level Research: Pentesting of storage controller in microgrid application

- API Manipulation assumes adversary has full network access and credentials, and operates BESS with malicious intent

Command	Outcome
Volt-Var setpoint manipulation	Inverted Volt-Var curves were allowed, and could be used to have adverse effects on local voltage
Setting direct power timeouts to low values	Adversarial use of the timeouts could cause the direct power modes to turn off after short periods of time
Manipulation of direct power setpoints	Direct power setpoints (and similar settings) could be modified to change the battery output adversarially.
Manipulation of power modes (including off)	Changing the battery mode could have adverse impacts, particularly by changing islanding modes or engaging total shutdown.
Simultaneous commands	Code was written to execute commands simultaneously on both batteries, doubling the impact of any adversarial commands.



Malicious Volt-VAR setpoints cause the voltage to dip even lower when the baseline is already below nominal voltage

# Cyber – Manual Fuzzing

Action	Successful execution?	Notes
Mixed protocols	Yes	Modbus and authenticated commands were accepted simultaneously. Adversary can use Modbus to circumvent any protections provided by authentication/encryption.
No token	Partial	READ requests successful, WRITE requests returned inadequate access rights error
Incorrect token	No	Invalid bearer token error
No certificate	Partial	If no certificate provided, SSL certificate verification error returned. However, if verification is disabled, both READ and WRITE requests are successful
Incorrect certificate	Partial	If a session has already been established, incorrect certificate does not matter. If new session is being established, incorrect certificate raises SSL Max retries exceed error
Invalid parameter names	No	READ and WRITE requests to endpoints or schema names that do not exist return “404 page not found” and “400 invalid character” errors respectively
Invalid parameter values	No	Interface requires that parameter types align with what is expected.
Control parameters outside documented limits	Partial	Most parameter tested were limited to the documented bounds. However, some values had no bounds and were instead limited by the device physics. Other values had bounds, but the enforced limits did not align with the documented limits.

- Modbus is always enabled, so protections can always be circumvented
- Authentication still allows some unexpected behaviors that could lead to broken confidentiality
- API parameters must be matched
- Most documented limits were enforced, some were not, which could potentially cause unexpected behaviors

# Hardening Wind Energy Systems from Cyber Threats

## Scalable, Actionable Decision Support to Advance Cybersecurity for Wind Asset Owners

### Project Description

In alignment with the WETO Cybersecurity Roadmap, this project provides actionable and strategic decision support to prioritize the needs, based upon real world analysis and evaluation, and use of security hardening technologies to secure wind energy systems. Specific recommendations include secure reference architectures, technology suitability and benefit will be provided to the wind industry.

### Lab Partners



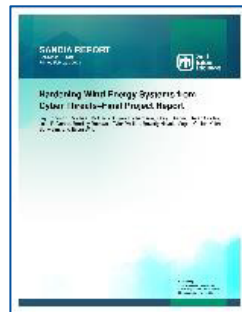
### Industry & Open-Source Partners



### Key Outcomes



Video demonstrating cybersecurity tools for wind



Technical report with all project details



Industry flier, featured in POWER magazine



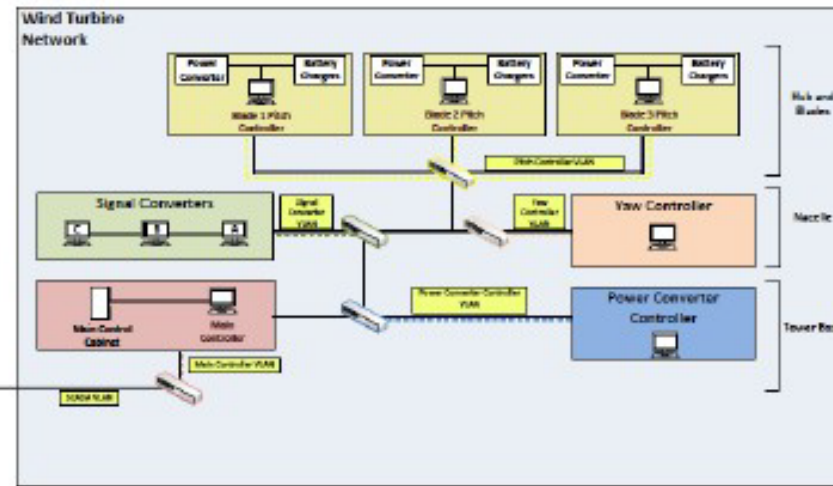
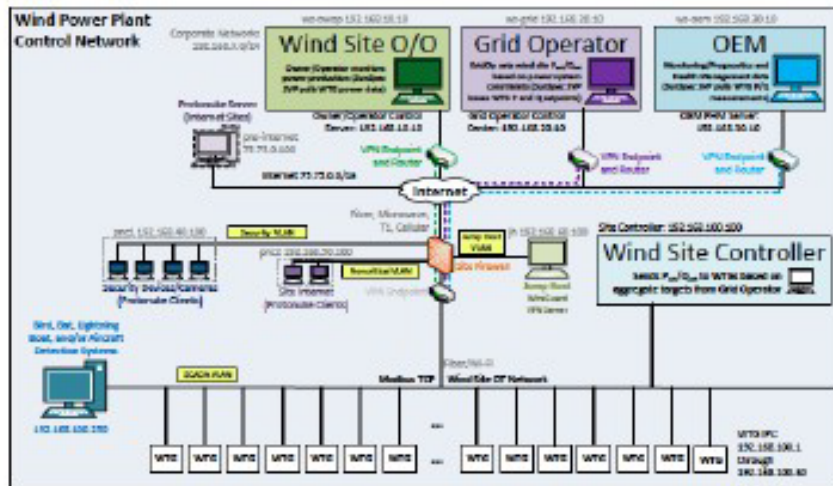
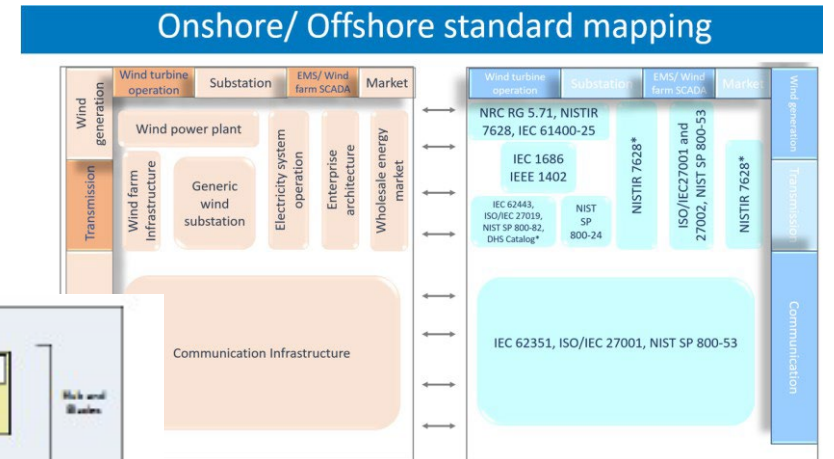
IEEE Access Journal Paper

### Value Proposition

- ✓ Recommendations to confirm need and prioritize investment
- ✓ Criteria for evaluating cyber risk,
- ✓ Enable a secure reference architecture

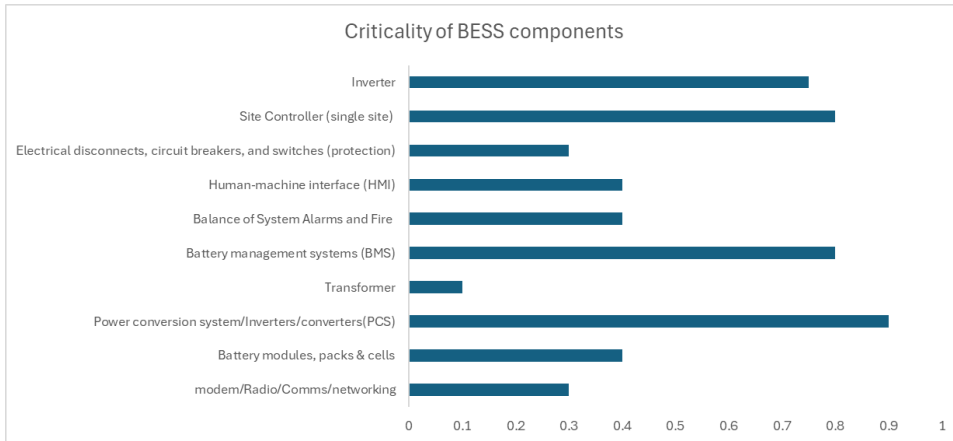
# Offshore Wind Cybersecurity

- Reference architecture for offshore wind systems and associated transmission networks
- Cybersecurity assessment of architecture

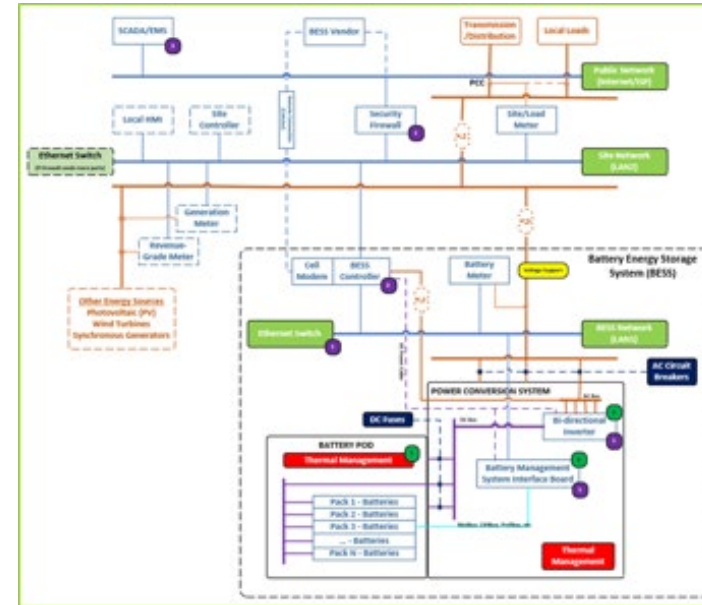




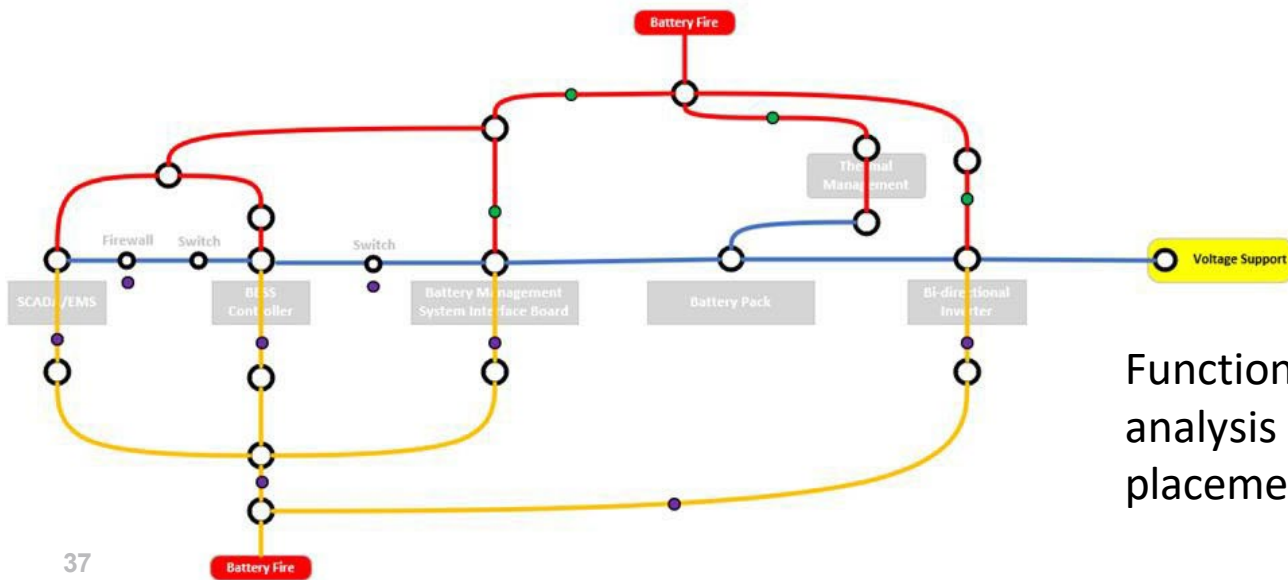
# CIE Design Guide for BESS and Microgrids



Criticality of BESS Components: Consequence of mis-operation

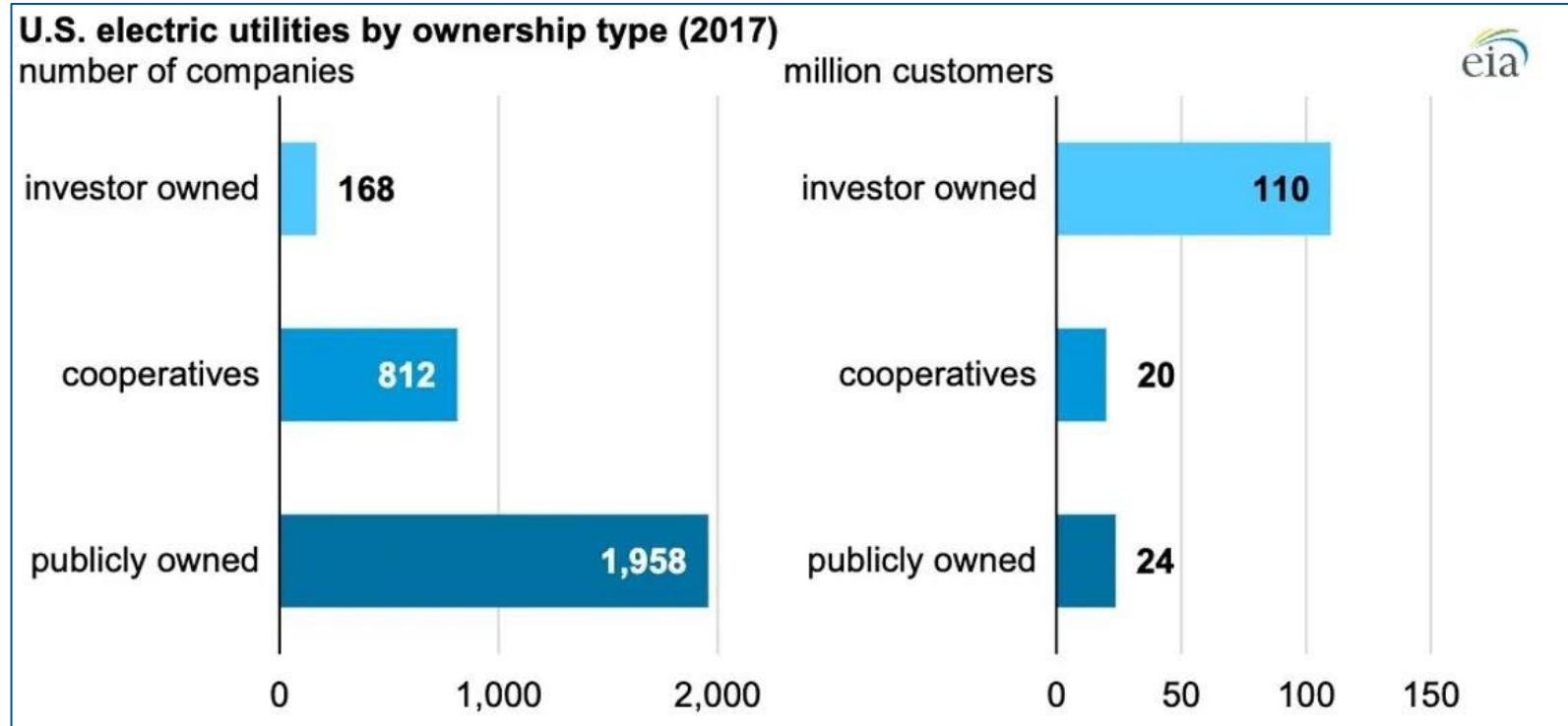


BESS Reference Architecture for system definition used in risk assessment



Function consequence analysis & mitigation placement

# Utility level



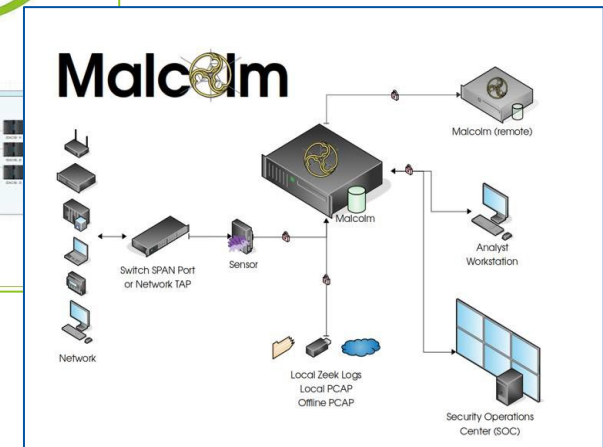
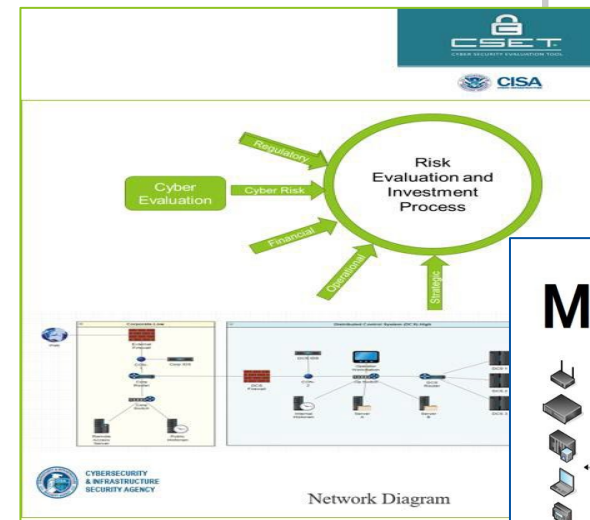
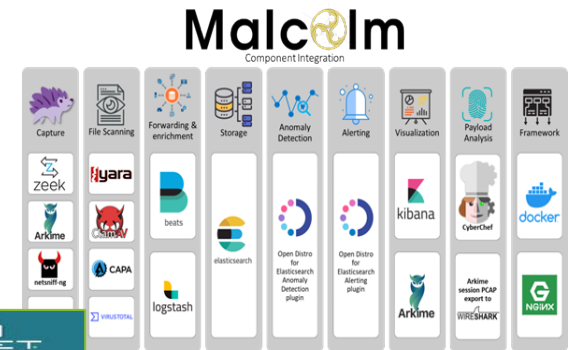
- Generation and distribution
- Regulatory requirements
- Insurance considerations
- Range of maturity
- Renewables as a portion of the managed assets

# Utility Scale: Cyber SHIELD Program Tools & Objectives

## SHIELD- Security through Hardware Integration, Education, and Layered Defense

Leverage existing cyber risk analysis tools but customize to renewables sectors

- INL AIA with Malcolm– **Asset Interaction Analysis**: Links assets to business processes and translates the business processes to OT devices. Supports deeper threat and vulnerability identification/analysis for user.
- INL Cyber CERT with CSET – **Architecture Basics**: Allows entities to plot network design and identify basic vulnerabilities in current state.
- INL Cyber CERT with CSET– **Program Assessment**: Provides entities access to a cybersecurity assessment of basic programs and capabilities along with risk-based recommendations for improving their maturity.



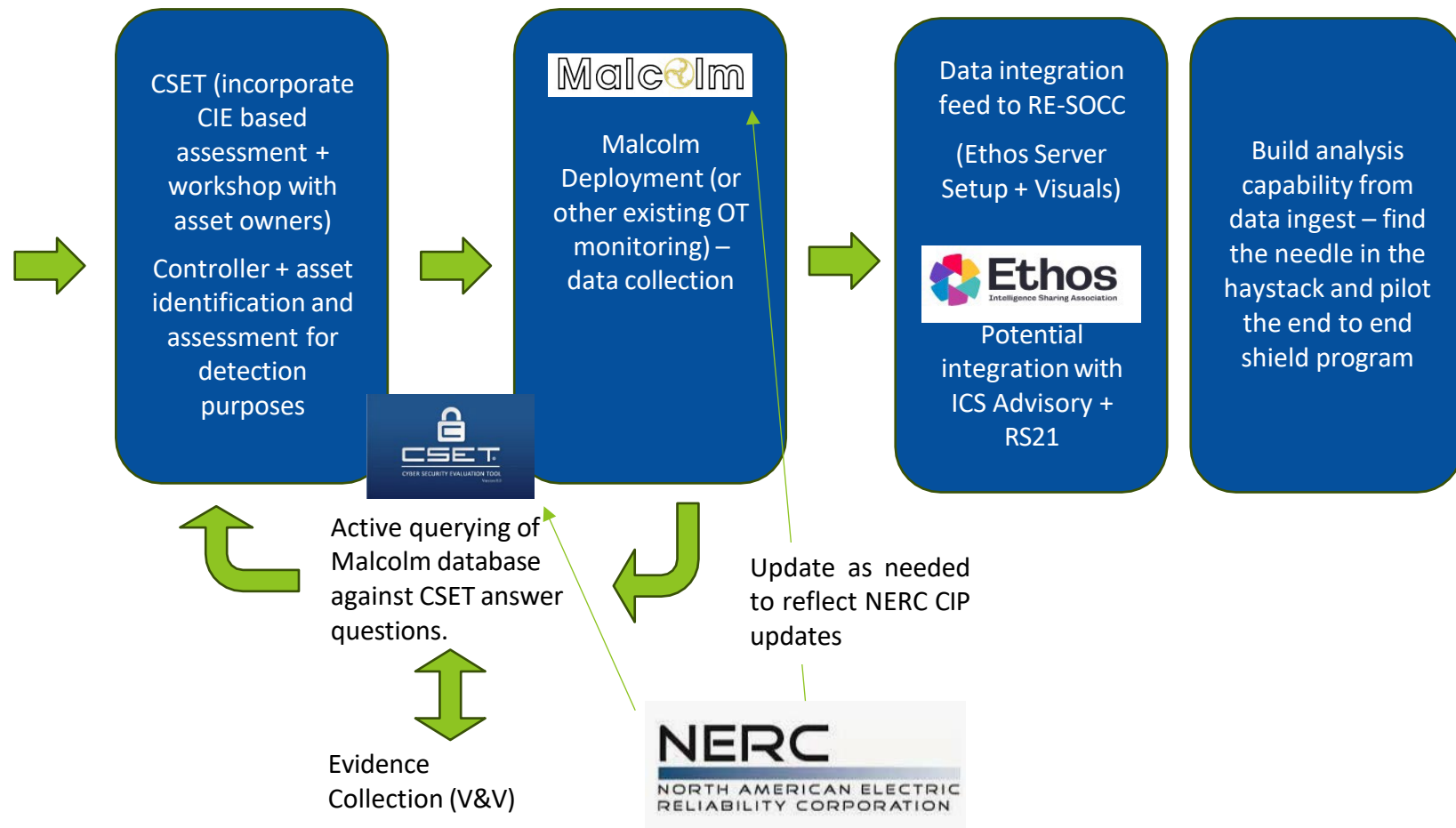
# Cyber SHIELD Ecosystem



Roll CIE Template for batteries, spreadsheet, scoring... into the CSET platform.

CIE (CESER) Clean Energy Guide feeds into WETO/SETO/Hydro:

- Wind (start from batteries)
- Solar (start from batteries)
- Hydro (start from micro Nuclear)



# GDO Technical Assistance for Digital Assurance (TADA) Overview

- Improve resilience in the grid modernization space with enhanced security programs to awardees
- Secure digital energy infrastructure by guiding organizations through a tailored analysis and mitigation program to determine their current security posture.
- Provide technical assistance for evaluating supply chain & protection choices against consequences
- Help organizations develop a future sustainable assessment and procurement planning program
- Rapidly respond to changing regulatory landscape and cutting-edge equipment



# Regulation & Standards

## Federal Regulation

- NERC CIP
- Low impact criteria
- NERC IBR registration

## State-level regulation

- NASEO
- NARUC

## Standards

- IEEE
- IEC
- UL
- Sunspec
- SEIA

## Insurance

- Requirements to develop and maintain cyber policies
- Exclusions for state-sponsored activity

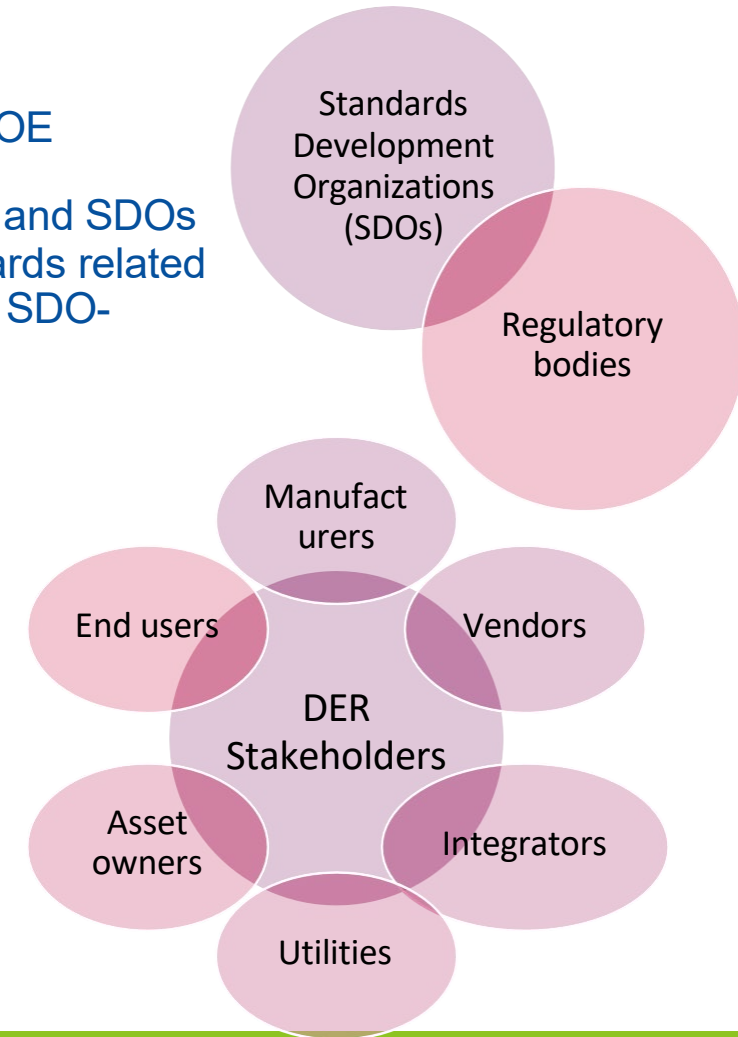
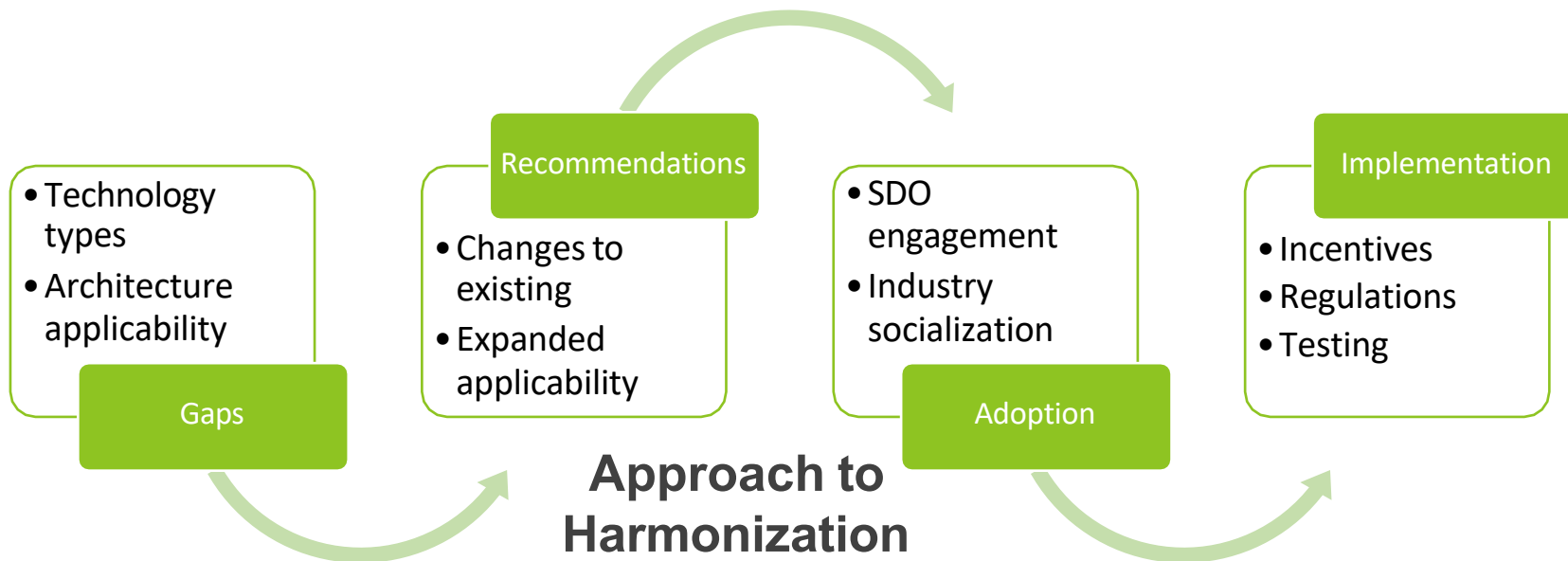
## Best Practices

- Non-binding
- Enforced by organization

# Grid Modernization Initiative: Assessment of DER Cyber Security Standards

## Objectives

- **Assess and report** existing DER cybersecurity standards, certification programs, and DOE supported efforts
- **Harmonize** DER cybersecurity certification requirements originating from UL, IEC, IEEE and SDOs
- **Document, and publish** a dataset and library of existing and under development standards related to DER security operations **Publish and obtain buy in** across the country for use of the SDO-agnostic library, curation for new entries, and management of search functions
- **Solicit feedback** from other standards-focused projects
- **Address gaps** in cybersecurity certification standards, including standardized testbed environments, data collection, and reporting.



# Putting research into practice: How does it get adopted?

- Case study partners
- Technical assistance
- Training & workforce development
- Tabletop exercises
- Full-scale exercises
- Participation in industry and government standards groups and advisory boards



# CyberStrike STORMCLOUD



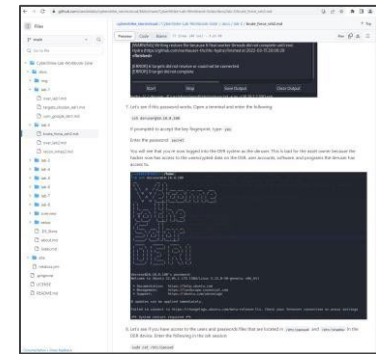
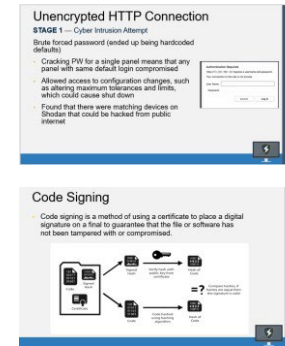
The *CyberStrike STORM CLOUD* training workshop was designed to enhance the ability of renewable energy and operators to prepare for a cyber incident impacting industrial control systems with specific considerations of the architectures and limitations of renewable energy.

- Renewables focused
  - Solar, wind, & EVs (coming soon)
- Emphasis on emerging and unique threats for renewables
  - Remote access
  - Diverse stakeholder ecosystem
- Framework uses Lockheed Cyber Kill Chain

## Curriculum

## Hardware

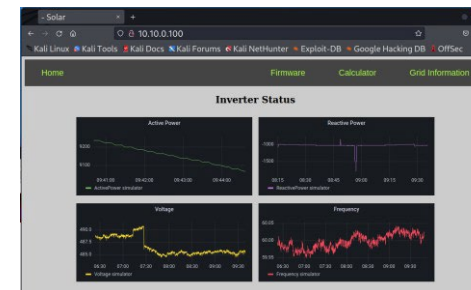
## Exercises



## Cybersecurity Tools

## DER Interfaces

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>• Shodan</li> <li>• Xhydra</li> <li>• NMAP</li> <li>• Wireshark</li> <li>• Ettercap</li> </ul> | <ul style="list-style-type: none"> <li>• Custom web interface</li> <li>• VNC Viewer</li> <li>• SSH</li> <li>• SunSpec MODBUS</li> <li>• IEEE 2030.5</li> </ul> |
|---|--|



# Deploying clean energy cyber-physical capabilities extending successful programs

**Cyber-Informed Engineering (CIE)** – “engineer out” cyber risk throughout the design and operation lifecycle, rather than add cybersecurity controls later

**Cirrus** – Cloud Preparation framework for small and medium utilities

**Technical Assistance** – Non-Domestic Storage / Power Electronics risk mitigation

**Supply chain SME led analysis:** cyber vulnerability testing, forensics, and digital subcomponent enumeration

**VPP/Aggregator** – Table-Top Exercise and Playbook

**Malcolm** – open-source intrusion detection and hunt system, deployment and analysis



Improves cybersecurity supply chain for ICS



Uses expert testing



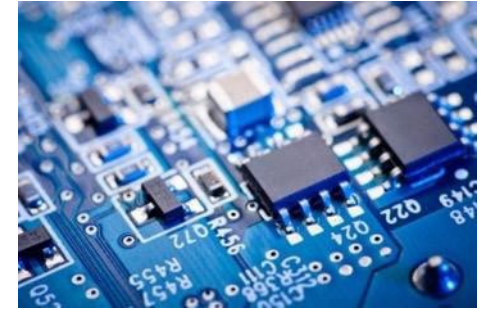
Identifies common-mode vulnerabilities



Partners with vendors and asset owners



Relationships & Continuing Engagement



# Cirrus Tool Rapid Development and Deployment

*Responsible use of cloud in Operational Technology*

<https://inl.gov/cirrus/>

- A **consequence-driven decision support framework** for entities to assess their grid modernization deployment strategy in the cloud
- Test against use cases and partner users **enabling adequate assessment** of deployment plans.
- IAB (30+ attendees) – bimonthly (short)
- COP – bimonthly (15 – 20 attendees)
- Users – 6 demonstration, move to licensing model



IDAHO NATIONAL LABORATORY

# Tooling: CIE-BAT

## Cyber-Informed Engineering Battery Analysis Tool

- In use by 1 IOU and 3 coops,

### CIEBAT & CIEMAT

Cyber-Informed Engineering (CIE)  
Tools for Utility Security

The Cyber Informed Engineering Battery Analysis Tool (CIEBAT) and Cyber-Informed Engineering Microgrid Analysis Tool (CIEMAT) were developed in collaboration with the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER). These tools are designed to enhance the security and resilience of energy infrastructure by integrating Cyber-Informed Engineering (CIE) principles and resilient design into the deployment, operation and management of battery energy storage systems (BESS), including hybrid integrations with solar and microgrids.

#### Deployment and Support

Both tools are being actively deployed through the Grid Deployment Office (GDO) technical assistance (TA) programs, providing vital support to utility design and integration engineers, along with cybersecurity teams as they integrate these digital technologies into their energy systems. This deployment ensures that new installations are not only efficient but also secure-by-design. The tailored technical assistance for digital assurance in grid resilience aids utilities in implementing these tools effectively, optimizing their systems' performance. By integrating CIEMAT and CIEBAT, utilities can enhance their energy systems' security posture and provide continued reliable energy services.

#### Outputs Tailored to Utility-Specific Needs

The output of CIEBAT and CIEMAT is highly customized, providing results and recommendations that are specific to the utility's infrastructure and operational context. This tailored approach ensures that the utilities can implement practical and effective measures that align with their unique system configurations and service requirements.

**References:**  
 CESER <https://www.energy.gov/cybersecurity>  
 TA Program <https://www.energy.gov/ta>  
 Cyber-Informed Engineering (CIE) <https://www.energy.gov/cie>

Contact: Emma Stewart [Emma.Stewart@idaho.gov](mailto:Emma.Stewart@idaho.gov)

Idaho National Laboratory

**Table 1: ID# Action (Labeling Function)**

ID#	Action (Labeling Function)	CIE Mitigation
C1	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C2	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C3	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C4	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C5	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C6	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C7	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C8	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C9	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C10	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C11	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C12	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C13	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C14	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C15	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C16	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C17	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	

**Table 2: Energy Source Name, Energy Source Type, Power Rating**

Energy Source Name	Energy Source Type (DC/AC)	Power Rating
Ex. Site Controller (ETU) <td>DC/AC <td>1 MW</td> </td>	DC/AC <td>1 MW</td>	1 MW
Ex. Site Utility Controller <td>DC/AC <td>4 MW</td> </td>	DC/AC <td>4 MW</td>	4 MW

**Table 3: ID#, Action, CIE Mitigation**

ID#	Action	CIE Mitigation
C1	Level of Power Supply leading to the disruption of power supply to the loads.	2
C2	BEES has its charging and discharging operations manipulated leading to overloading and decreased life of BE.	0
C3	BEES within the local electrical grid. This inevitably disrupts the operation of other grid-connected devices and leads to these cascading effects from the compromised BEES to the overall grid stability.	1
C4	The BEES operator loses regulatory compliance and legal action because the BEES severely disrupts its ability to maintain access to grid control systems, thus a violation of cybersecurity.	3
C5	The BEES operator suffers an economic and financial impact due to a violation of cybersecurity, leading to a loss of trust and a decline in market share due to widespread media coverage and public scrutiny from the failure of the BEES to supply power to its customers.	4
C6	The BEES operator takes within and external responsibility for an unavailability of time and the company loses substantial financial losses due to both the BEES downtime, as well as the costs associated with investigating the breach, restoring system functionality, and implementing enhanced digital measures.	5

**Table 4: ID#, Action, CIE Mitigation**

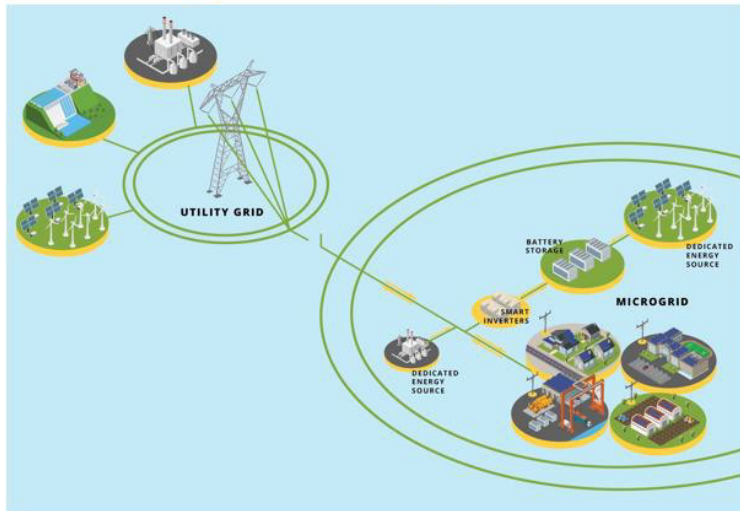
ID#	Action	CIE Mitigation
C1	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C2	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C3	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C4	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C5	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C6	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C7	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C8	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C9	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C10	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C11	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C12	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C13	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C14	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C15	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	
C16	The BESS power management system regulates the power output and the state of charge of the battery cells, ensuring optimal performance and safety.	
C17	The BESS inverter converts the direct current (DC) output of the battery cells to alternating current (AC) that matches the local load's voltage and frequency.	

- 1 Analyze System Services
- 2 Analyze Consequence
- 3 Analyze CIE Mitigations

# CIE-MAT

## Cyber-Informed Engineering Microgrid Analysis Tool

### CIE Microgrid Template



**Multi-step tool** focused on supporting Cooperative Utilities and aids in their ability to determine a **cybersecurity protection scheme** (i.e., CIE protections, Digital protections) for a **Microgrid installation**.

Image provided by [The Microgrid Solution | Energized by Edison](#)

### Steps in the Template

- 1** Determine System Criticality (i.e., Impacts, Funding, Load Profile)
- 2** Detail and Describe the System Characteristics (i.e., BESS, PV, Generators, IBR Resources, etc.)
- 3** Select Grid Services Provided (i.e., Backup Power, Voltage Regulation, etc.)
- 4** Describe how the System provides Grid Service(s). (i.e., Enabling Functions)
- 5** Describe the Misuse of those Enabling Functions.
- 6** Select Mitigations (i.e., CIE, C2M2, IEEE 1547, etc.) for the People, Process, and Technologies identified in Misuse.



### CIEBAT & CIEMAT

Cyber-Informed Engineering (CIE) Tools for Utility Security

The Cyber-Informed Engineering Battery Analysis Tool (CIEBAT) and Cyber-Informed Engineering Microgrid Analysis Tool (CIEMAT) were developed in collaboration with the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER). These tools are designed to enhance the security and resilience of energy infrastructure by integrating Cyber-Informed Engineering (CIE) principles and resilient design into the deployment, operation and management of battery energy storage systems (BESS), including Hybrid integrations with solar and microgrids.

#### Deployment and Support

Both tools are being actively deployed through the Grid Deployment Office (GDO) technical assistance (TA) programs, providing vital support to utility design and integration engineers, along with cybersecurity teams as they integrate these digital technologies into their energy systems. This deployment ensures that new installations are not only efficient but also secure-by-design. The tailored technical assistance for digital assurance in grid resilience aids utilities in implementing these tools effectively, optimizing their systems' performance. By integrating CIEMAT and CIEBAT, utilities can enhance their energy systems' security posture and provide continued reliable energy services.

#### Outputs Tailored to Utility-Specific Needs

The output of CIEBAT and CIEMAT is highly customized, providing results and recommendations that are specific to the utility's infrastructure and operational context. This tailored approach ensures that the utilities can implement practical and effective measures that align with their unique system configurations and service requirements.

#### References

CSDET <https://csl.gov/national-security/csl/>  
TA Program <https://csl.gov/cadet/technical-assistance-and-training/>  
Cyber-Informed Engineering (CIE) <https://csl.gov/national-security/csl/>

#### Contact

Emma Stewart [Emma.Stewart@inl.gov](mailto:Emma.Stewart@inl.gov)

#### Comprehensive Analytical Approach

The CIEBAT and CIEMAT tools operate through a structured three-step process designed to provide a thorough and utility-specific analysis:

- 1 Analysis of System Services:** This initial step involves a detailed examination of the energy system's operational services. For battery systems, this might include energy storage, load balancing, and frequency regulation. For microgrids, the focus could be on power distribution, load management, and integration with the broader grid.
- 2 Consequence-Focused Analysis:** In this step, the tools conduct a consequence analysis to assess the potential impacts of system failures or cyber incidents. This analysis focuses on identifying high-consequence functions within the system that could lead to significant disruptions if compromised. The tools evaluate the criticality of these functions to prioritize protection efforts.
- 3 Cyber-Informed Engineering Mitigation Analysis:** The final step involves applying CIE principles to develop and recommend mitigation strategies. This analysis incorporates cybersecurity considerations directly into the engineering process, ensuring that the designed mitigation measures are effective against cyber threats while maintaining system performance. The output is a set of tailored recommendations that address the specific vulnerabilities and operational needs of the utility.

INL Idaho National Laboratory

# Liberty Eclipse

- Annual cybersecurity preparedness exercise that brings together federal partners, and operational technology (OT) and cybersecurity experts from the energy sector to validate the security of their cyber defense systems, plans, policies, and procedures in a scaled environment.
- Full-scale exercise with utility participants
- Energized, but disconnected, test bed
- Red team, led by INL, executes scenarios on components found in real systems requiring coordinated response from cybersecurity teams (SOC) and power operations teams (Ops Center)



Testbed leverages commercial protection and control devices using systems commonly found in utility substations across the country.

Contact: Megan Culler  
[megan.culler@inl.gov](mailto:megan.culler@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.*

# Enhancing Grid Security)

"Rip and replace not feasible in the short term."

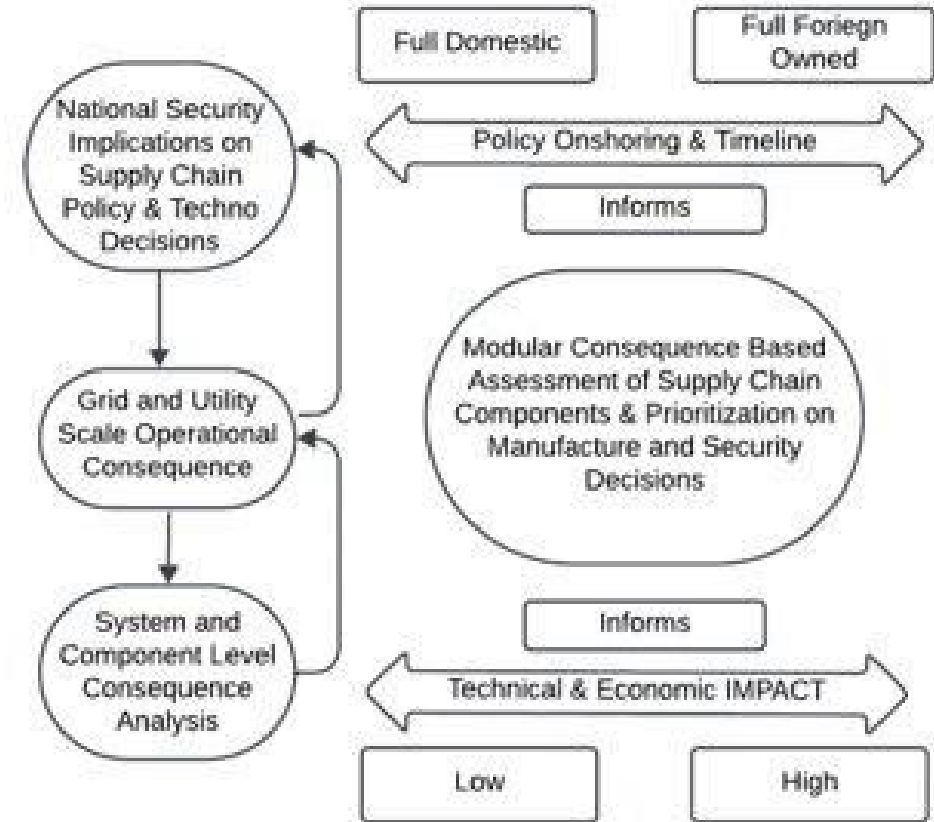
## Short Term Solutions:

- Building Better Controls
- Implementing Robust Security Measures

Using Cyber-Informed Frameworks to evaluate systems and system of systems – for driving future supply chain policy decisions

## Quantitative Supply Chain Decisions:

- What matters?
- How and when to move ?
- Cost impact?
- Drive change over time?



Solution Short Term Mitigation & Operate through the challenge: implement and test a dynamic framework, which provides a customizable & effective "wrapping" around the products, mitigating the highest consequence events



# Driving Supply Chain Movement for Sustainable Energy Security (Long Term Solutions)

## Grid Deployment Office + CESER Program:

Combined approaches for rapidly developing and deploying data driven solutions for securing digital infrastructure

**Goal:** Enable transition to a secure digital energy landscape by providing infrastructure owners and operators, suppliers, with necessary data, tools and guidance

- **Responsible Use of Cloud Framework (GDO):** Introduce an all-hazards and cybersecurity-aware engineering framework to guide cloud deployments specifically tailored for distribution utilities.
- **Technical Assistance Program for Non-Domestic Equipment (GDO):** Bolster the security and efficiency of non-domestic energy infrastructure, providing the DOE GRIP Program awardees with risk reduction strategies for Distribution, BESS, EV, Clean Energy infrastructure
- **AI for Substations and Data Sharing Risk Analyses (GDO)**



- **BESS Initiative (CESER):** Data Driven solutions for nondomestic Battery Energy
- **Storage Systems (BESS),** Consequence analysis to navigate supply chain risks and develop sustainable control processes



Solutions Long Term Direction: Create a program which can strategically analyze the energy transition product market, and provide data driven technical direction for long term mitigations and onshoring

# Trends in ICS Malware

[2010] Stuxnet

- Very aggressive
- Targeted specific version/configuration of PLCs

- Targeting protocols, not devices
- Flexible and extensible
- Accompanied by wipers

[2015] Industroyer / CrashOverride

- Framework targeting 4 OT protocols
- First known malware targeting electric grid
- Persistent backdoors
- Pre-defined timer for execution
- Included DoS against relays and wiper tool

[2017] Triton

- Designed to manipulate safety instrumented systems
- Only affected specific Schneider Triconix safety system
- Modifies in-memory firmware to execute arbitrary code
- Only works if controller is in “program” mode instead of “run” mode
- Bugs in malware allowed it to be discovered before execution

[2022] Incontroller/ Pipedream

- 3 modules targeting Schneider PLC, Omcron PLC, OPCUA protocol
- Capabilities include disrupting, modifying, and disabling safety controllers

[2022] Industroyer2

- Targeted IEC-60870-4-104
- Customized configurations to modify malware behavior to specific devices (i.e. relays) in target environment
- Enhanced reproducibility against different environments

# Risk Management Architecture: Consequences

POTENTIAL IMPACT BY STAKEHOLDER			
Event	Utility (Non-Operator)	Operator (Facility/Aggregator/Utility)	Manufacturer, Integrator, or Installer
Loss of View		<ul style="list-style-type: none"> <li>Loss of revenue</li> </ul>	<ul style="list-style-type: none"> <li>Reduce reputation</li> <li>Financial liability</li> </ul>
Loss of Control	<ul style="list-style-type: none"> <li>Energy imbalance</li> </ul>	<ul style="list-style-type: none"> <li>Propagated failures</li> <li>Injury</li> <li>Equipment damage</li> </ul>	<ul style="list-style-type: none"> <li>Reduce reputation</li> <li>Financial liability</li> </ul>
Denial of View		<ul style="list-style-type: none"> <li>Improper operation</li> </ul>	<ul style="list-style-type: none"> <li>Reduce reputation</li> <li>Financial liability</li> </ul>
Denial of Control		<ul style="list-style-type: none"> <li>Improper operation</li> </ul>	<ul style="list-style-type: none"> <li>Reduce reputation</li> <li>Financial liability</li> </ul>
Denial of Safety	<ul style="list-style-type: none"> <li>Injury</li> </ul>	<ul style="list-style-type: none"> <li>Injury</li> </ul>	<ul style="list-style-type: none"> <li>Reduce reputation</li> <li>Financial liability</li> </ul>
Manipulation of View	<ul style="list-style-type: none"> <li>Improper control decision</li> </ul>	<ul style="list-style-type: none"> <li>Improper control decision</li> </ul>	<ul style="list-style-type: none"> <li>Reduce reputation</li> <li>Financial liability</li> </ul>
Manipulation of Control	<ul style="list-style-type: none"> <li>Additional energy resources</li> <li>Injury</li> </ul>	<ul style="list-style-type: none"> <li>Loss of reliable operation</li> <li>Activation of critical load algorithm</li> <li>Loss of required generation</li> <li>Failure to meet contractual obligations</li> </ul>	<ul style="list-style-type: none"> <li>Reduce reputation</li> <li>Technical investigation</li> <li>Financial liability</li> </ul>
Manipulation of Sensors and Instruments	<ul style="list-style-type: none"> <li>Energy imbalance</li> <li>Failure of regulatory compliance</li> </ul>	<ul style="list-style-type: none"> <li>Improper operation</li> <li>Severe mechanical damages</li> <li>Loss of revenue resource</li> <li>Increased operation and maintenance costs</li> </ul>	<ul style="list-style-type: none"> <li>Reduce reputation</li> <li>Increase after-sale expenses</li> <li>Potential product call-back</li> <li>Financial liability</li> </ul>
Manipulation of Safety	<ul style="list-style-type: none"> <li>Extended restoration time</li> <li>Failure of regulatory compliance</li> </ul>	<ul style="list-style-type: none"> <li>Injury or death</li> <li>Loss of intellectual property</li> <li>Technical investigation</li> </ul>	<ul style="list-style-type: none"> <li>Devalue brand name</li> <li>Reduce market share</li> <li>Decommission the product from the market</li> <li>Financial liability</li> </ul>

# Risk Reduction Through Automation

Tech Talk with RF

Brent Castagnetto, CISSP

10.28.2024



# About Me

## Brent Castagnetto

- Co-Founder NovaSync (2020-Present)
- Partner, Archer Security Group (2016-Present)
- EnergySec Instructor (2016-Present)
- WECC – CIP Auditor Manager (2010-2016)
- Over 20 Years of Cyber Security Experience
- Certifications: CISSP, CBRM, CBRA, MABR



- “The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency.”
  - Bill Gates



# Why Automate?

**Task Execution**

**Efficiency and Productivity**

**Innovation**

# Latent Vulnerabilities

- The entity was checking an incorrect patch source
- Security Patch evaluations were missed
- Risk exposure to systems for nearly three years



<https://www.rfirst.org/wp-content/uploads/2024/08/2024-CIP-Themes-and-Lessons-Learned.pdf>



# Latent Vulnerabilities

- Legacy admin access remained
- No regular “account validation”
- The issue was ONLY identified as the tracking system was being replaced



<https://www.rfirst.org/wp-content/uploads/2024/08/2024-CIP-Themes-and-Lessons-Learned.pdf>

# Latent Vulnerabilities

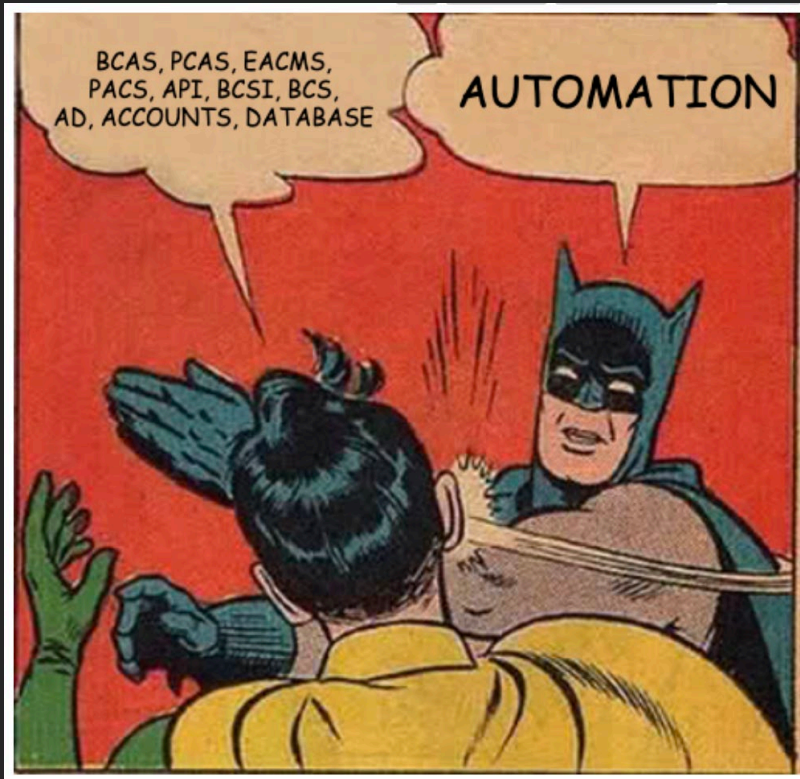
- Often difficult to detect
- Manual process challenges
- Things we may consider lower risk

# Latent Vulnerabilities

- Compliance, Security, BIA, DR, Safety Teams all have a seat at Impact, Risk and Controls table.
  - Business Impact Analysis
  - Risk Management
  - Internal Controls
  - Documented Processes
  - Training
  - Automation
  - Training



# Systems to Consider



- automation applied to an inefficient operation will magnify the inefficiency”
- Baseline Monitoring Tools
- Patch Management Systems
- Asset Management Databases
- Access Management Solutions
- Internal Controls
- Risk Management

# How does automation reduce risk?

- System Monitoring
- Visibility
- Workflow
- Security



# How does automation reduce risk?

## Compliance Optimization

- Reduce human error
- Monitoring and Reporting
- End to End Processes
- Audit Ready
- Trend analysis
- (True) Access Management
- Training
  - Including Cyber and Physical Security Training



# Why Automate?

**Task Execution**

**Efficiency and Productivity**

**Innovation**

# Thank you very much!

---

- Brent Castagnetto, CISSP  
[b.castagnetto@archerint.com](mailto:b.castagnetto@archerint.com)  
[brent@novasync.co](mailto:brent@novasync.co)  
801.597.7957





# THANK YOU

***Join us for our next Tech Talk -  
November 18th***

**[Webinar Link](#)**

