

01 0 1

00 011

0101



Technical Assistance for Securing Digital Energy Infrastructure

April 10 2024

Emma M Stewart
Chief Power Grid Scientist
National and Homeland Security

csdet.ta@inl.gov
Emma.stewart@inl.gov

INL/MIS-24-77594

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

 Idaho National Laboratory

Outline

1. Identifying the Challenge
2. Proposed Approach
3. Contrasting with Cyber Plans
4. Request for Information
5. Current Actions and Path to Technical Assistance (TA)

Bottom Line Up Front

- Core Challenge: Many of the Inverters, BESS, EVSE and Software packages have a limited domestic supply chain
- We must enable the resilient deployment, while providing appropriate mitigations, training, support and security management solutions for digital controls
- GDO enlisted INL to develop and deliver a component security evaluation and mitigation technical assistance program for key digital energy components
- Technical Assistance is being offered to all GRIP and Grid Resilience State/Tribal Formula Grant Program Awardees at different stages of procurement and design
- This is the launch of that program, later parts of the presentation include links and contact info to sign up
- CSDET.TA@INL.GOV
- <https://www.energy.gov/gdo/grid-resilience-and-innovation-partnerships-grip-program-technical-assistance-resource-center>

Navigating Supply Chain Challenges

Building Resilient Systems for Electric Grid Modernization

- The main concern revolves around the availability of US-manufactured products for electric grid modernization and navigating the challenges presented by the geopolitical supply chain landscape.
- How do we drive modernization – while appropriately mitigating risk and consequence
- Project design optimization – secure supply chain and criticality of the application to your operation is a primary consideration
- Equipment to be discussed:
 - Electric Vehicles (EVs) + EV Supply Infrastructure
 - Battery Energy Storage Systems (BESS) + management systems
 - Inverters
 - Orchestration software (Distributed Energy Resources Management Systems [DERMS]/Advanced Distribution Management Systems [ADMS])
 - [Critical-and-Emerging-Technologies-List-2024-Update.pdf](#) ([whitehouse.gov](https://www.whitehouse.gov))

See the following sections of the FOA for information on disclosure requirements, domestic content, and related information: IV.D.xxi; IV.I; VI.B; Appendix B; Appendix C.

Acronyms and Definitions 1

Acronym	Description	Details
BESS	Battery Energy Storage System	Entire system, from pack to grid connection (inc BMS, PCS, Inverter, Transformer, controllers)
BES (in terms of NERC CIP)	Bulk Electric System	The big grid/transmission
BMS	Battery Management System	Charge Controller and Environmental Management
BMS	Building Management System	
EMS	Energy Management System	Emma Mary Stewart, Emergency Management System
Site supervisory control/SCADA	Supervisory Control and Data Acquisition	
ADMS	Advanced Distribution Management System	Collection of advanced control, operations and planning applications

Acronyms and Definitions 2

Acronym	Description	Details
SIS	Safety Instrumentation System	
NERC CIP	North American Electric Reliability Council – Critical Infrastructure Protection	
DERMS	Distributed Energy Resource Management System	Mass orchestration of DER
DO	Distribution Operator	
AOO	Asset Owner Operator	
DSO	Distribution System Operations	
IBR	Inverter Based Resource	Resources which have an inverter to connect to the grid
EVSE	Electric Vehicle Supply Equipment	

Acronyms and Definitions 3

Acronym	Description	Details
AMI	Advanced Metering Infrastructure	
FAN	Field Area Network	
VPP	Virtual Power Plant	Set of devices in a geographical area, approximately/loosely mass orchestrated
Microgrid		Set of devices in a local area, orchestrated and islandable/can operate independently
CIE	Cyber Informed Engineering	

Acronyms and Definitions 4

ICS	Industrial Control Systems	
Malware		software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system
Vulnerability		weakness in an IT or OT system that can be exploited by an attacker to deliver a successful attack. They can occur through flaws, features or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal
Exploit		An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic

Recent Renewable Energy Cyber Attacks



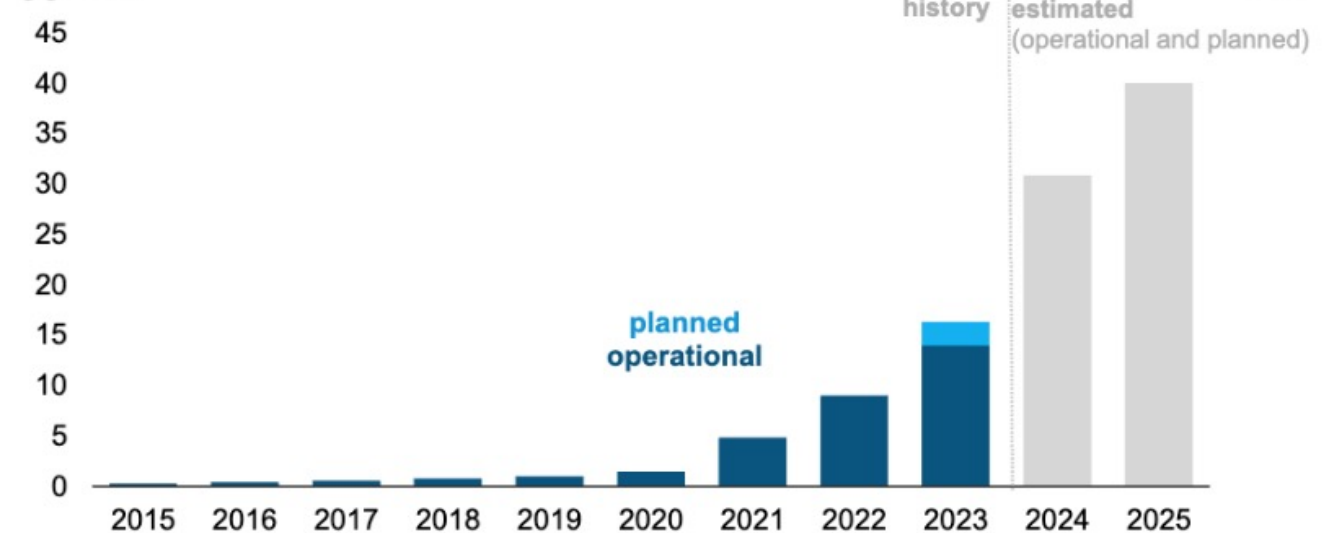
- Increased renewable sector influence
- Primary U.S. adversaries
 - China
 - Russia
 - Iran
 - North Korea
- Development of more sophisticated attacks

Why Does This Matter?

Emerging energy markets are transforming...

- Batteries, BMS, IBR's are a core underpinning technology of clean energy transition
- It can be difficult to find products manufactured in the US
- Purchasing equipment from a foreign entity can come with some security risk
- Appropriate design and secure operation is key

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



Current Trends

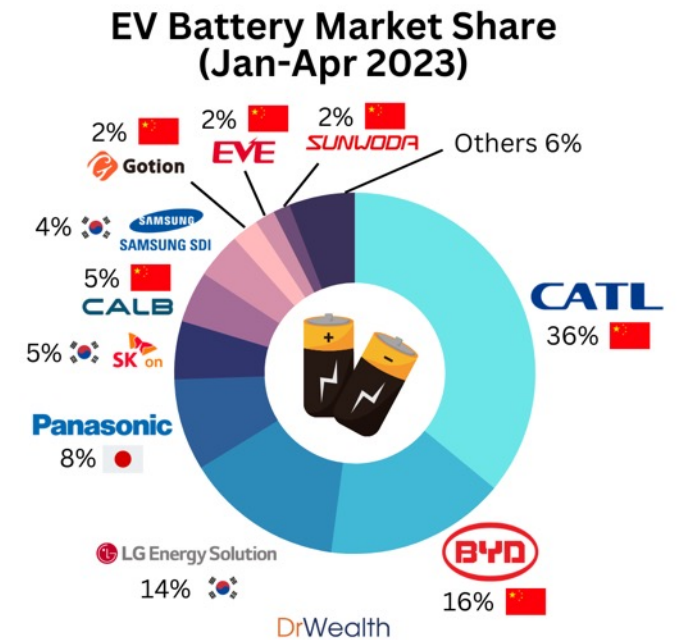
A) Transition to Brand Ownership and Origin (Including business relations)

Example: Batteries once embedded as cells by various vendors are now marketed as whole systems, incorporating integrated sensors and branded independently.

- Shift towards integrators and hybrid models.
- Many U.S. OEMs have a counterpart OEM based in China with a similar name.

B) Establishment of LLCs for each Battery Energy Storage System (BESS) site


C) Transition of ownership from utility to Third-Party Owners (Primarily financiers)



Trends 2

- D) Implementation of Operator-as-a-Service Models
- E) Focus on rapid interconnection and cost targets
- F) Generator registration under NERC CIP IBR Phase 1
 - 20MW, >70kV must register GO-IBR
- G) Retention of Service and Communications Control by OEMs
 - “you didn’t pay for Volt/Var – can be turned off remotely

Common Challenges in Procurement & Integration

1. Failing Chips 
2. Persistent Communications 
3. Hardcoded Passwords 
4. Operation & Maintenance Models
5. White Labeled Products 
6. Insecure Support Software
7. No SBOMS or HBOMs 
8. Unknown Supply Chain 'Spiderweb' for Integrated Systems
9. Limited Threat and Consequence Modeling Capabilities



Best Practices and Considerations for Your Projects

- Purpose of discussion: consideration and evaluation of supply chain choices in application and design
- Consider your risk through consequence-based frameworks (<https://inl.gov/national-security/cie/>)
- Resilience and security can be considered in all topics even if not specific to cybersecurity
- Determine what you are allowed to do:
 - Defense-serving entities may have different requirements
 - State and Local guidelines
 - Tax credits for sites with domestic content, and Foreign Entities of Concern (FEOC)
- Review National Defense Authorization Act (NDAA) language*
 - FY24 NDAA, Section 154: Prohibition on Availability of Funds for Procurement of Certain Batteries
- Contracting language is important – ensure roles and responsibilities are clear

See the following sections of the FOA for information on FEOCs, disclosure requirements, domestic content, and related information: IV.D.xxi; IV.I; VI.B; Appendix B; Appendix C.

** <https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf>*

Launch Plan: How to Evaluate and Protect

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



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

Applied Template & Guided Assessment Framework

Technical Assistance to improve resilience and reliability of new infrastructure

Purpose & Program Overview:

- Enhancing resilience in grid modernization with robust security programs.
- Guiding participants through a customized analysis and mitigation program.
- Evaluating current security posture, supply chain, and protection options.

Additional Program Offerings:

- Physical/forensics equipment assessment on-site or in-situ at INL/Partner Entity.
- Workshop on generalized process and security framework (utilizing CIE type methods)
- Procurement/contract language in development

Short Engagement:

- Mature programs with specific assessments available.
- Selected analysis conducted.

Expert Match:

- Guided workshops and templates provided.
- Specific site visits for in-depth analysis.

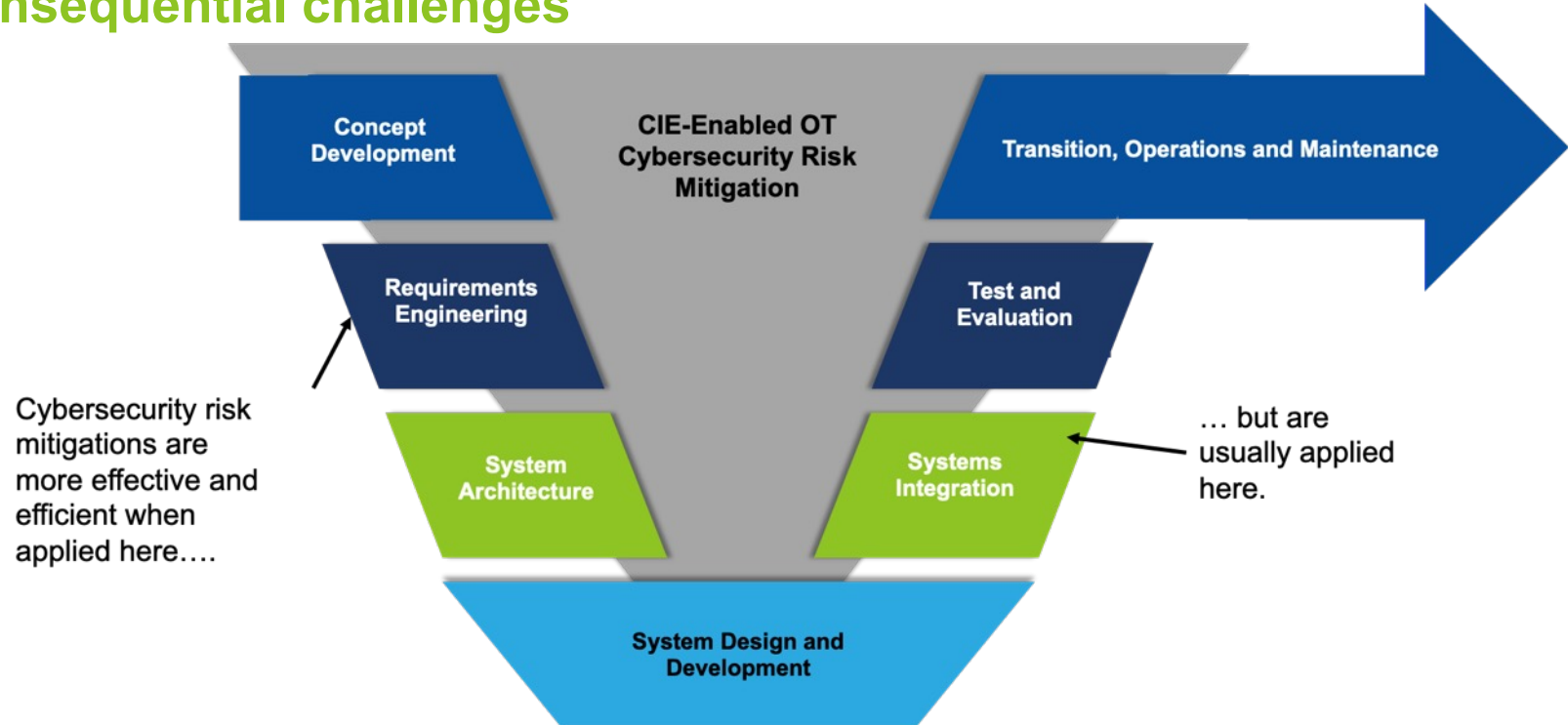
Deep Dive:

- Focus on entities new to OT or this style of OT.
- Introduction to OT Security.
- Ongoing advice for supply chain risk mitigation.
- Provide physical/forensics assessment of equipment either in-situ, or on site at NL

Framework is Designed using Cyber-Informed Engineering (CIE)

Engineering out the most consequential challenges

- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.

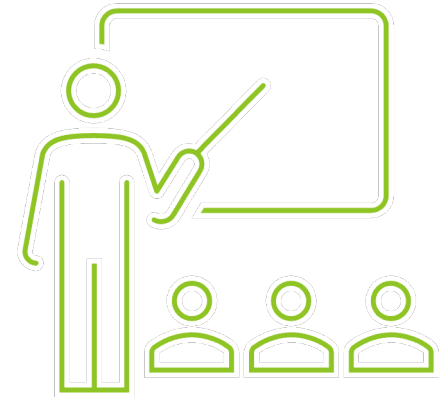


- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to engender a **culture of security** aligned with the existing industry safety culture.

Contrasting with Cyber Plans

Technical Assistance (TA) Overview:

- TA is tailored to swiftly adapt to evolving regulatory and policy changes, aligning the timing and depth of inquiries with National Laboratory subject matter experts (SMEs) in key topical areas.
- This program enhances and supplements existing technical assistance initiatives conducted by different DOE program offices.
- It complements cyber plans by providing training, workshops, and tailored guidance, contributing to their continuous evolution over time.



Technical Assistance Outline

Introduction:

- Enter information into the application portal, including a brief description of the equipment and stage of procurement/design process.
- Within two (2) business days, a program representative will acknowledge receipt via email and schedule a short conversation to clarify the request.

Short Advisory:

- Questions that can be answered with short and narrow responses and includes the assessment template and related training.

Expert Match:

- Addresses inquiries that require increased resources and is for applicants in the design or contracting stage requiring review or development of specific Cyber Informed Engineering (CIE) guidance.

Deep Dive:

- Addresses inquiries that require substantial resources and a lengthy development process. The applicant might require assistance with scenarios including sourcing, the physical assessment of equipment being installed, or an on-site inspection for site expansion.

Applicant Engagement:

- Applicants may evolve through all three assistance levels over time, contingent on project staging.

Summary

TA Applicants Receive:

- Guided analysis framework & subject matter expert (SME) engagement.
- Customized template development tailored to their needs.
- Assessment for supply chain risk reduction.
- Possible connections to asset inventory and monitoring tools.
- In situ or NL-based analysis of physical equipment being procured.

Outcomes Developed:

- Long-term mitigations and supply chain guidance.
- Comprehensive gap analysis for resilience in the digital transition.
- Data-driven insights for informed decision-making.

How to Access the TA – Contact us

- GRIP and Grid Resilience State/Tribal Formula Grant Program Awardees seeking technical assistance can contact **csdet.ta@inl.gov**.
- (Or emma.stewart@inl.gov)
- Within two (2) business days, a representative from the program will contact the entity to schedule a preliminary conversation. This conversation will help identify the needs of the entity and subject matter topic, as well as the type of assistance required.
- **csdet.ta@inl.gov**
- <https://www.energy.gov/gdo/grid-resilience-and-innovation-partnerships-grip-program-technical-assistance-resource-center>



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.