Raising the Floor of Cybersecurity in Renewables

June 2023

INL Cyber Team

Cyber SHIELD for Renewables

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

Idaho National Laboratory

INL/MIS-23-71409

Cyber SHIELD Overview: Introduction

Raise the Cybersecurity Floor

***S**ecurity through **H**ardware **I**ntegration, **E**ducation, and **L**ayered **D**efense is an* INL initiative aimed at “raising the floor in cybersecurity for renewables”.

Grid of the Future

Within a decade, renewables will be the leading generation source in our grids. The transition must ensure the future grid is secure. Need to rapidly mature cybersecurity.

Funded Programs

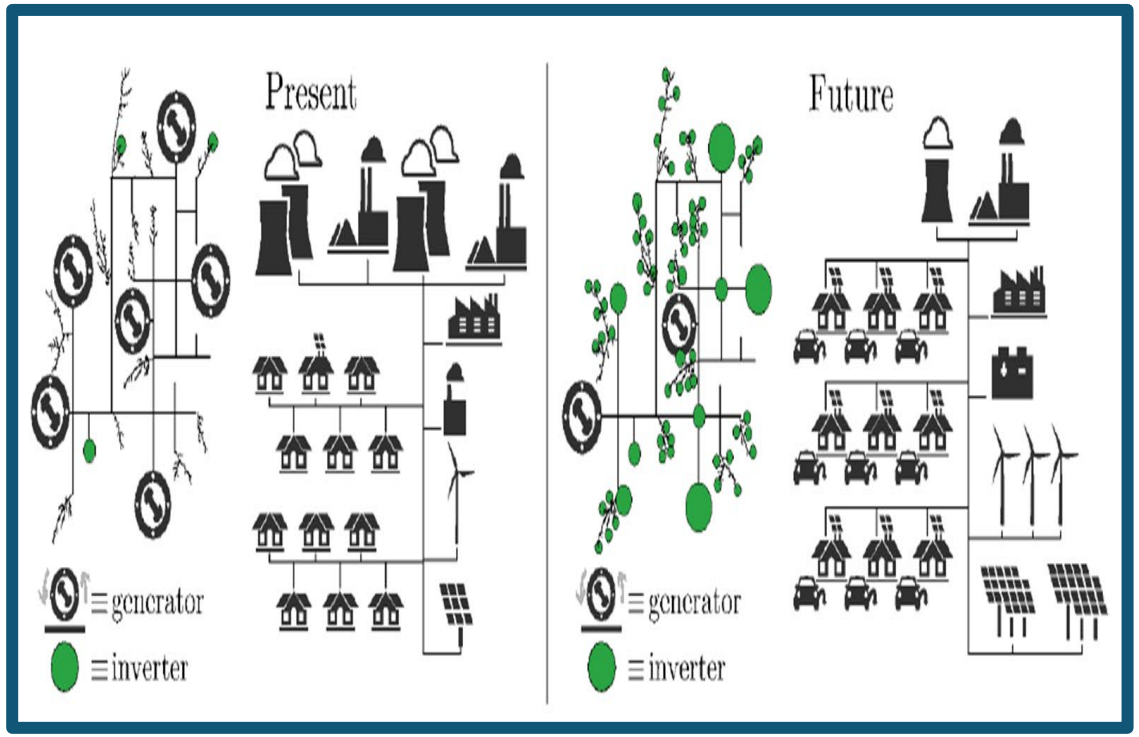
The Cyber SHIELD initiative leverages multiple robust tools that have been developed under DHS programs. These tools are tuned for use with renewable assets and accommodate any level of cyber maturity.

DOE-INL-Industry-Partnership

Targeted Support

The initial focus with the launch of the Cyber SHIELD program is the deployment of the INL Cybersecurity Evaluation Risk Tool (INL-CERT) and Asset Interaction Analysis (AIA).

Ensure grid security enhanced and renewable sector maturity as grid transition accelerates



Why?

- DOE funded engagement for a Public-Private Partnership
- Regulator bodies and Reliability organization shifting to recognize impact to the overall grid
- Insurance industry shift to burden of proof and expansion of contract litigation*
- Improved operational reliability and resiliency
- Lowering business risk

*University of California Sues Lloyd's Syndicates Over Cyber Insurance
https://www.wsj.com/articles/university-of-california-sues-lloyds-syndicates-over-cyber-insurance-da4675f5

Benefits of the tools

- Get to know what you have, better view of asset
- level risks - devices, protocols, misconfigurations.
- Helps identify potential attacks, vulnerabilities, and active exploits with more precision specific to your assets/devices.
- Increases network visibility to make informed decisions and improve reliability.
- Guided cybersecurity assessment tuned to the renewable industry to help identify or validate where your cyber program is.
- Ability to map network architecture within the assessment to control areas to help identify or validate your cyber posture
- Highlight possible next steps in evaluating strengths and weakness
- Ability to utilize DOE resources to explore and identify longer term commercial solutions.

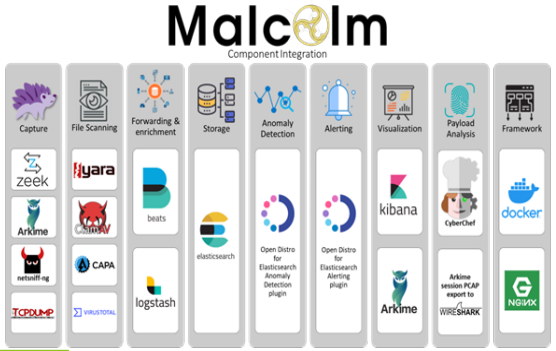
Cyber SHIELD Overview: Program Tools & Objectives

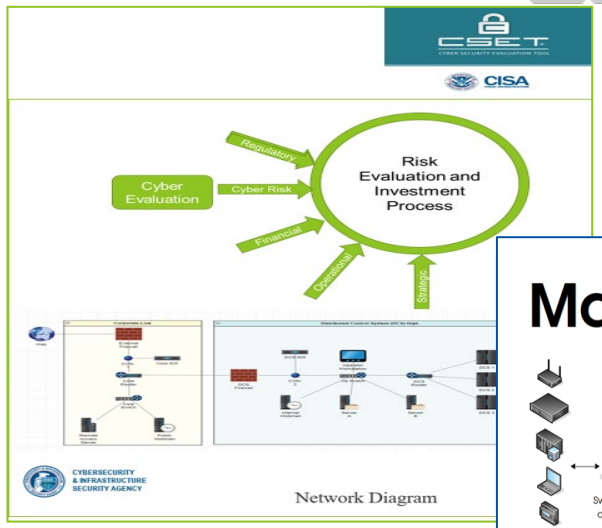
In order to support the “raise the floor” objectives, the initial focus has been deployment of three initiatives:

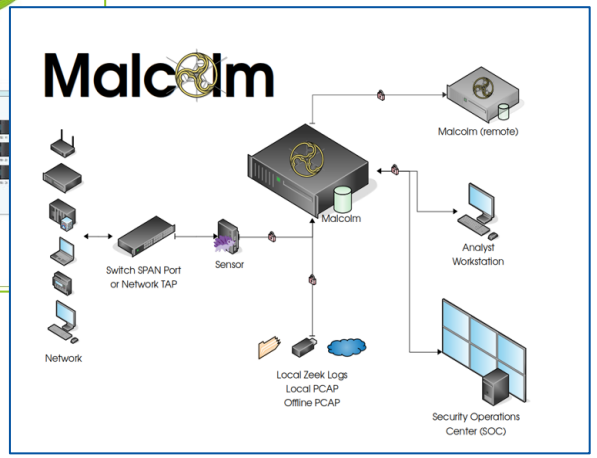
- INL Malcolm-AIA – ***Asset Interaction Analysis:*** Links assets to business processes and translates the business processes to OT devices. Supports deeper threat and vulnerability identification/analysis for user.

- INL Cyber CERT – ***Program Assessment:*** Provides entities access to a cybersecurity assessment of basic programs and capabilities along with risk-based recommendations for improving their maturity.

- INL Cyber CERT – ***Architecture Basics:*** Allows entities to plot network design and identify basic vulnerabilities in current state.





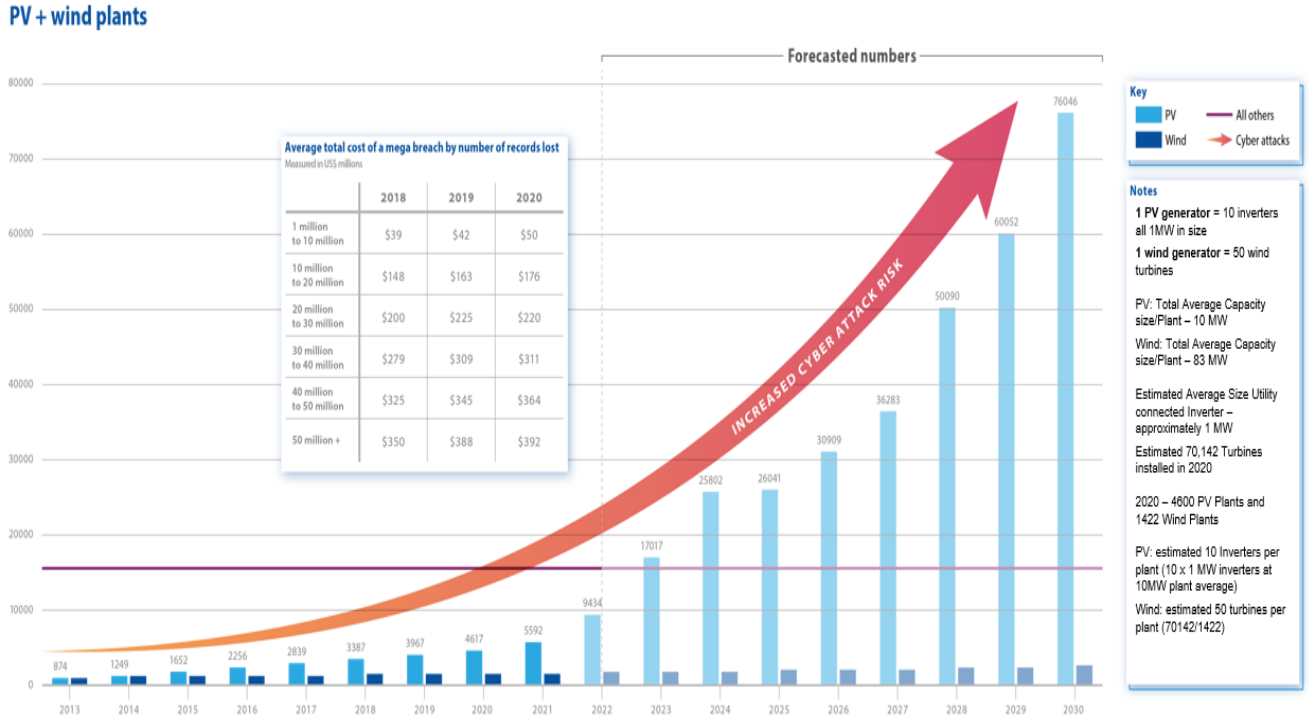


Cyber SHIELD Overview: The Security Imperative

Operational and Reliability Risk Priorities

- Operational and Cybersecurity Resilience
- Cybersecurity Threat and Risk Mitigation

The rapid and frequent evolution of technology and the cyber threat landscape brings <u>urgency</u> to the importance of maturing security within the renewable sector to support effective transition.

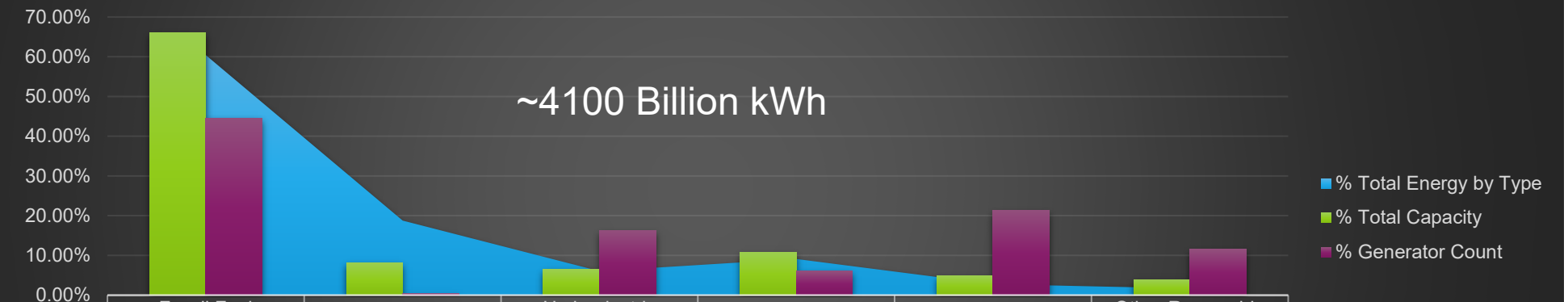


Average total cost of a mega breach by number of records lost
Measured in US$ millions

	2018	2019	2020
1 million to 10 million	$39	$42	$50
10 million to 20 million	$148	$163	$176
20 million to 30 million	$200	$225	$220
30 million to 40 million	$279	$309	$311
40 million to 50 million	$325	$345	$364
50 million +	$350	$388	$392

The number of generator plants will increase +400%, significantly increasing the potential cyber attack space.

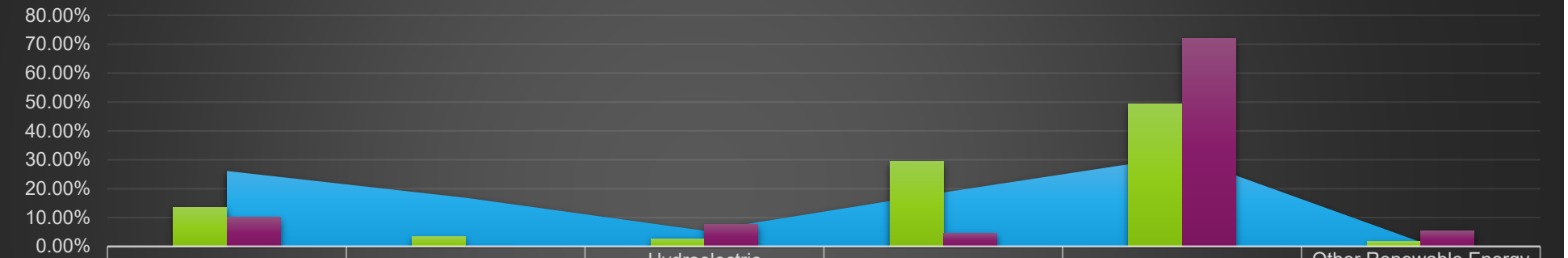
% Total Units, Energy, and Capacity



	Fossil Fuel Generation	Nuclear	Hydroelectric Conventional	Wind	Solar PV Utility	Other Renewable Energy Sources
% Total Energy by Type	60.42%	18.75%	6.06%	9.11%	2.78%	1.69%
% Total Capacity	66.03%	8.05%	6.44%	10.75%	4.86%	3.87%
% Generator Count	44.44%	0.38%	16.30%	6.03%	21.33%	11.53%

2021

% Total Units, Energy, and Capacity



	Fossil Fuel Generation	Nuclear	Hydroelectric Conventional	Wind	Solar PV Utility	Other Renewable Energy Sources
% Total Energy by Type	26.13%	16.89%	5.46%	18.73%	31.27%	1.52%
% Total Capacity	13.45%	3.42%	2.73%	29.50%	49.25%	1.64%
% Generator Count	10.10%	0.18%	7.72%	4.67%	71.88%	5.46%

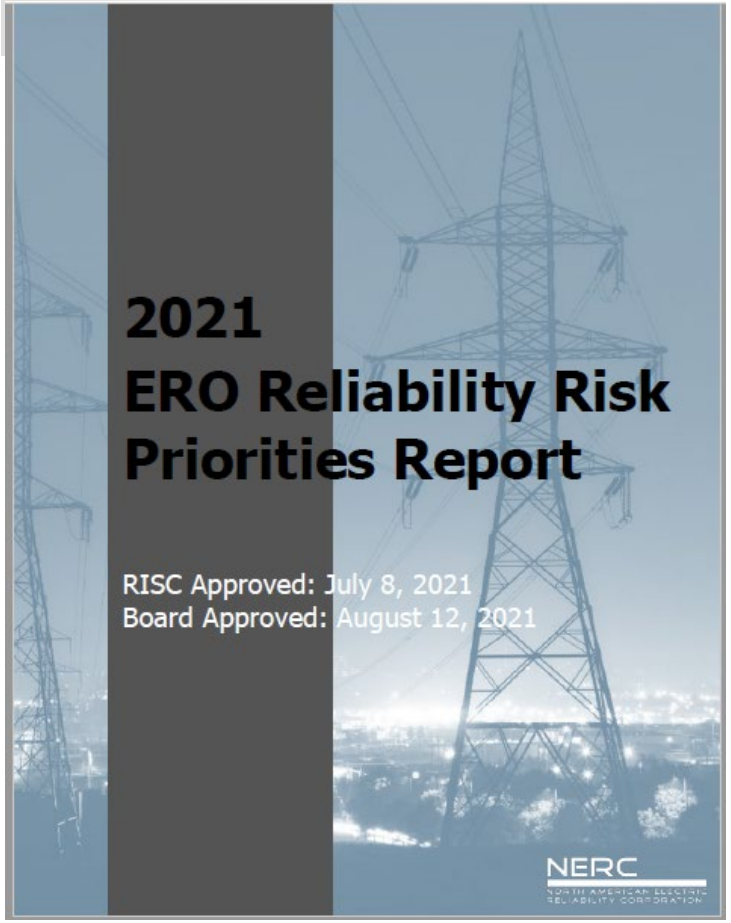
% Total Energy by Type % Total Capacity % Generator Count

2030

Cyber SHIELD: Risk for the Grid

Changing Resource Mix and Cybersecurity are the highest Ranked Risks

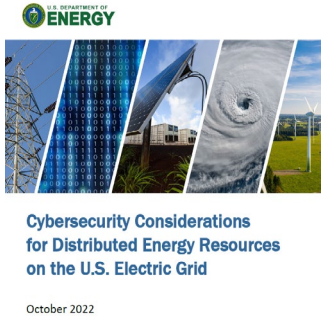
NERC Reliability - Risk



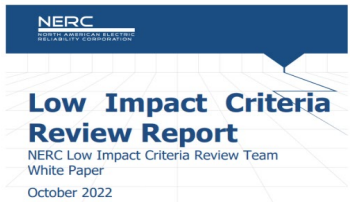
Cyber SHIELD Overview: The Security Imperative

Regulatory Compliance & Legal Readiness

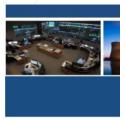
FERC, NERC, Federal Legislative and State Pressure



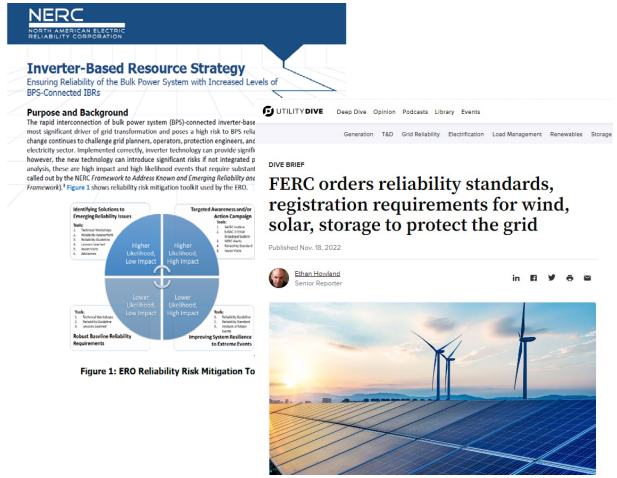
"DOE Cybersecurity Report Provides Recommendations to Secure Distributed Clean Energy on the Nation's Electricity Grid" ~DOE CESER October 6, 2022



CIP Standards Revisions



- Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for protection of user authentication information (e.g. combinations of usernames and passwords) for remote access to low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.
- Requirement(s) for detection of malicious communications to/between low impact BES Cyber Systems at assets containing those systems that have external routable connectivity.



"we find that unregistered IBRs connected to the Bulk-Power System, regardless of size and transmission or sub-transmission voltage, that in the aggregate have a material impact on Bulk-Power System performance should be registered." -

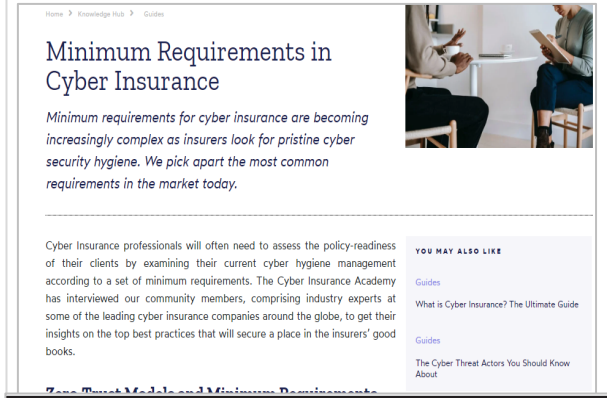
NERC IBR Registration Work-Plan

Generator Owner – Inverter-Based Resource (GO-IBR):

Owners of IBRs which have aggregate nameplate capacity of less than or equal to 75 MVA and greater than or equal to 20 MVA interconnected at a voltage greater than or equal to 100 kV; or

Owners of IBRs which have aggregate nameplate capacity of greater than or equal to 20 MVA interconnected at a voltage less than 100 kV.

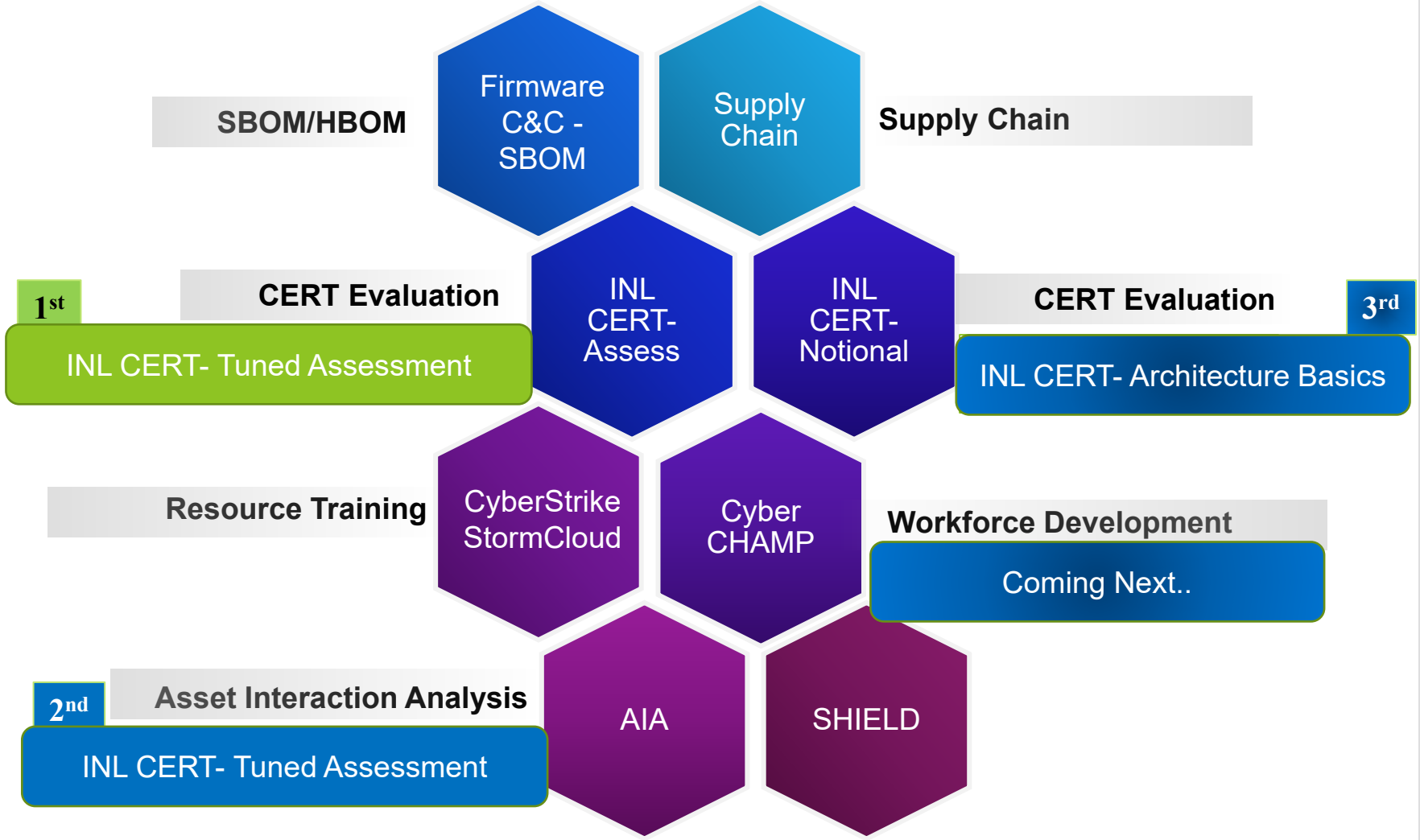
Insurance Policy and Commercial Litigation Trends – No more wiggle room

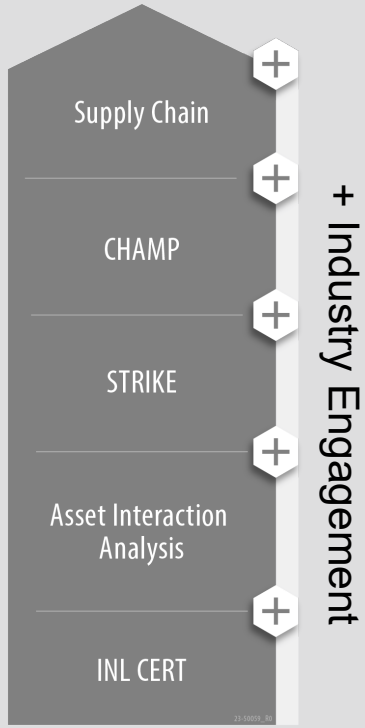


CIP-003-9FERC Approves Extending Risk Management Practices to Low-Impact Cyber Systems

INL - Cyber SHIELD

Raising the Floor on Cybersecurity for grid scale renewables





Cyber SHIELD Industry Resources

SHIELD–Malcolm

Asset Interaction Analysis

Key Challenges Targeted

Links assets to business processes and translates business processes to OT devices. Supports deeper threat and vulnerability identification/analysis for user

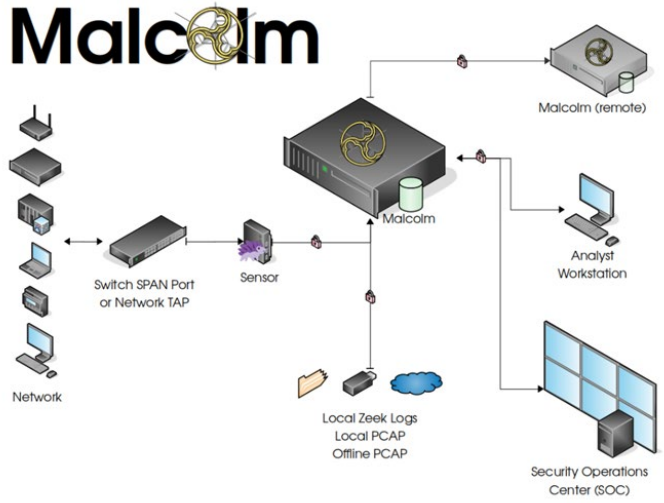
Key features:

- ✓ Malcolm: A first step in asset to business processes mapping
- ✓ Works with a spectrum of cyber maturity adding capability at their level
- ✓ Significant investment by others (DHS)

Top 3 Benefits:

1. Get to know what you have, better view of asset level risks - devices, protocols, misconfigurations.
2. Helps identify potential attacks, vulnerabilities, and active exploits with more precision specific to your assets/devices.
3. Increases network visibility to make informed decisions and improve reliability.

Threat Monitoring and Analytics



Asset Interaction Analysis

Malcolm

Malcolm Key Benefits & Deployment Overview

Deploying AIA

INL will deploy hardware (spec'd to multiple environments) and work with your team on installation and configuration for your network

INL will work with your team to identify capture points and configure data collection

INL encourages plant owners and operators to incorporate the capability after engagement

INL Cyber SHIELD-INL CERT

INL Cybersecurity Risk Evaluation Tool

CERT- Program Assessment

CERT- Architecture Basics

CSET CYBER SECURITY EVALUATION TOOL

CISA CYBER+INFRASTRUCTURE

Key Challenges Targeted

Deliver a standardized, repeatable cybersecurity valuation methodology tuned to the needs and characteristics of the renewable industry subsectors, which can provide insight and guidance for better informed, broader, risk-based investment decisions surrounding renewable IT and OT cybersecurity programs.

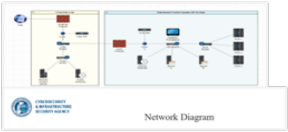
Key features:

- ✓ Renewable Sector Focused Capability
- ✓ Leverages DHS CSET tool, with multiple years of $$$ investment
- ✓ Open-Source and tuned for renewable industry

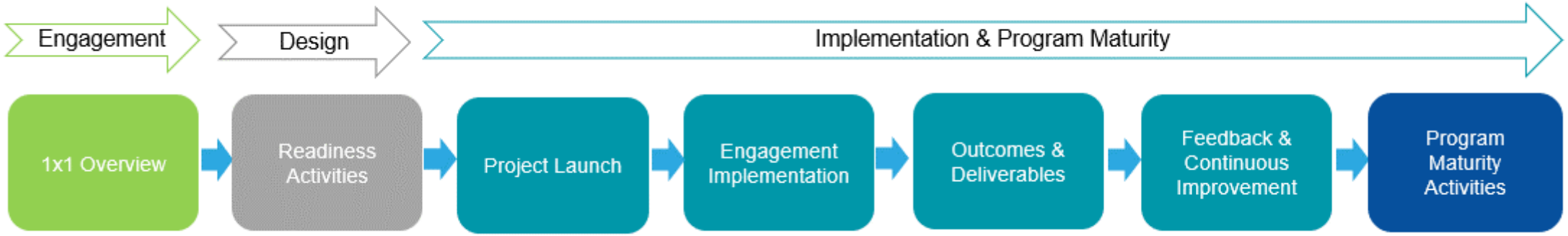
Top 3 Benefits:

1. Guided cybersecurity assessment and risk-based report to enhance cybersecurity programs leveraging established framework tuned for renewable asset sector
2. Ability to map network architecture within the assessment to control areas to help identify or validate your cyber posture
3. Immediate access to input supporting cyber program and resource planning capabilities to more quickly meet maturity objectives

Leveraging INL Resources to Mature Cybersecurity Posture and Risk Mitigation Capabilities

Phase I Unstructured	Phase II Reactive	Phase III Evolving	Phase IV Proactive	Phase V Optimized
"The impact of control failures is just a cost of doing business."	**"We have minimum controls and address security risks reactively, as they arise"**	**"We are better but still learning how to consistently and effectively execute"**	**"Understanding and managing emerging security risks is everyone's job."**	**"Strong security programs make us a better company, paving the way to improved performance."**
• No or limited defined processes or controls • Siloed and inconsistent practices • Business areas follow different paths to reconcile control issues • No systems in place to track key controls • Approaches are tactical • No processes in place to measure performance	• Processes and controls are defined but not formally documented • Performance management is centralized (where applicable) but lacks central leadership • Limited or no proactive efforts or coordination • Manual or limited performance testing • Limited engagement from key stakeholders • External relationship management is siloed, inconsistent and reactive	• Executing controls are defined and many are formally documented • Basic governance is in place to support a programmatic management of execution • Buy-in from leadership and all business areas • Adequate resources and staffing to execute controls • Technology solutions are available, but ad-hoc and limited • Ownership of controls generally established	• Centralized leadership to set vision and objectives, central program management, design and implementation • Controls are structured, planned and formally documented • Governance and accountabilities are clearly defined • Controls performance is actively measured with ability to anticipate risks and exposures • Program and controls are integrated as part of annual risk management processes • A combination of standard and custom-developed tools • Performance reporting	• Processes and controls are formally defined and documented, coordinated across organizations and strategically designed • Programmatic approach to training and communications to offer complete visibility across the enterprise • Formal quality assurance controls. Performance is regularly audited for consistent execution • Failures are evaluated and lessons learned are implemented and shared as part of extent-of-condition • Governance and oversight programs are robust, formally structured, centrally led and managed • Technology solutions integral part of all processes
Practices in the domain are not being performed as measured by responses to the relevant cyber framework questions in the domain	All practices that support the goals in a cyber framework domain are being performed as measured.	All specific practices are not only performed but are also supported by planning, defined stakeholders, and relevant standards and guidelines. All practices are performed, planned and have basic governance infrastructure in place to support.	All practices are performed, planned, managed, monitored and controlled	All practices in a cyber framework domain are performed, planned, managed, measured and consistent across all constituencies within an organization who have a vested interest in the performance of the practice
Recommended Cyber Shield Resources ✓ Cyber CERT – Basic Assessment ✓ Cyber CERT – Diagram Essentials ✓ Cyber Champ 	***Recommended Cyber Shield Resources*** ✓ Cyber CERT – Basic Assessment ✓ Cyber CERT – Diagram Essentials ✓ Cyber Champ ✓ Malcolm – Initial Deployment 	***Recommended Cyber Shield Resources*** ✓ Cyber CERT – General Cyber Hygiene ✓ Cyber CERT – Managed Diagram ✓ Cyber Champ ✓ Malcolm – Managed Deployment 	***Recommended Cyber Shield Resources*** ✓ Cyber CERT – Full Framework Assessment ✓ Cyber CERT – Advanced Diagram ✓ Cyber Champ ✓ Malcolm – Advanced Deployment 	***Recommended Cyber Shield Resources*** ✓ Cyber CERT – Full Framework Assessment ✓ Cyber CERT – Advanced Diagram ✓ Cyber Champ ✓ Malcolm – Advanced Deployment 

Conclusion



Looking for industry participants to get involved and leverage these resources to improve their cybersecurity maturity.

Designed to minimize level of effort from your teams (understand resources are often thin).

Partner information protection and confidentiality considerations have been integrated.

Outcomes and deliverables focused on identifying risk, mitigation activities, and prioritization.

Next Steps: Readiness

1) Partner Maturity Model
2) Partner Site Survey Questionnaire
3) Partner NDA
4) Partner SOP document for Network interaction

To discuss more or to sign up contact:
Stephen A. Bukowski at Idaho National Laboratory | stephen.bukowski@inl.gov

https://resilience.inl.gov/INLCYBERSHIELD

Questions: CYBERSHIELD@INL.gov

Idaho National Laboratory