U.S. DEPARTMENT OF
ENERGY

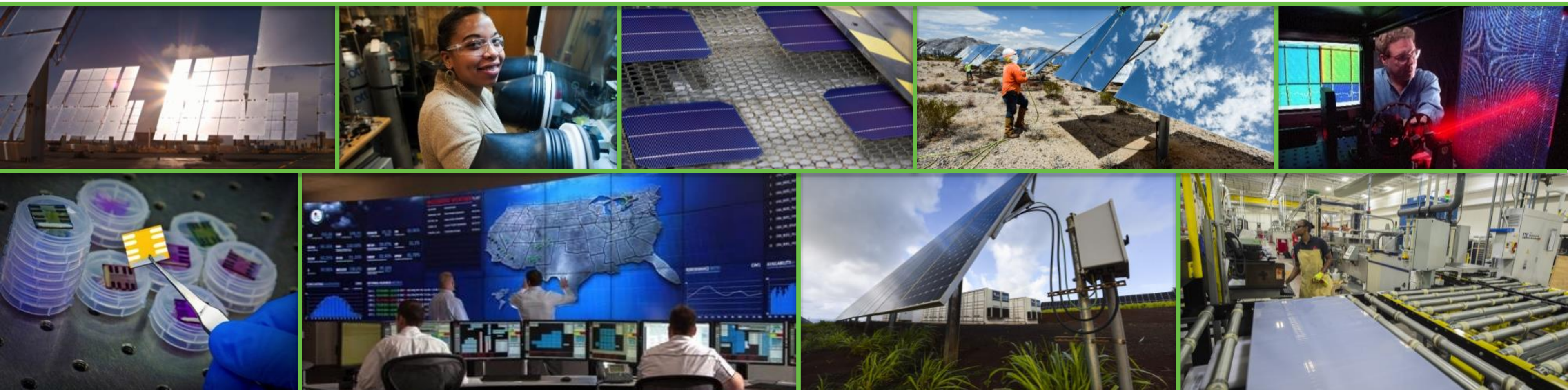
Office of
ENERGY EFFICIENCY &
RENEWABLE ENERGY

Securing Solar for the Grid (S2G): Cybersecurity for Solar Systems

DOE/EERE/SETO Systems Integration Webinar

Marissa Morales-Rodriguez, PhD
Technology Manager (Contractor)

May/2023

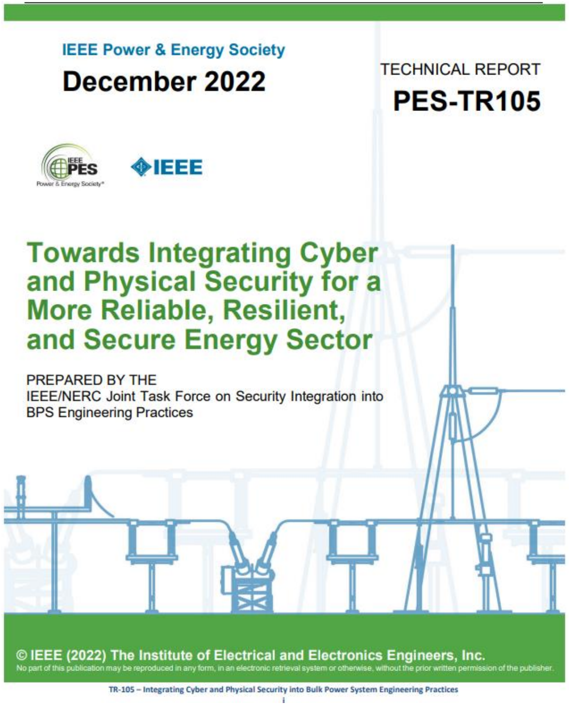


Agenda

- **Motivation**
- **Alignment with DOE Activities**
- **S2G: Securing Solar for the Grid**
  - Research Areas
  - Accomplishments
  - Get Engaged!
- **Conclusion/Summary**

To manage, optimize, and secure the future grid, new technologies, control techniques, and supporting reliability and security standards will be required.

Recent Reports



IEEE Power & Energy Society

December 2022

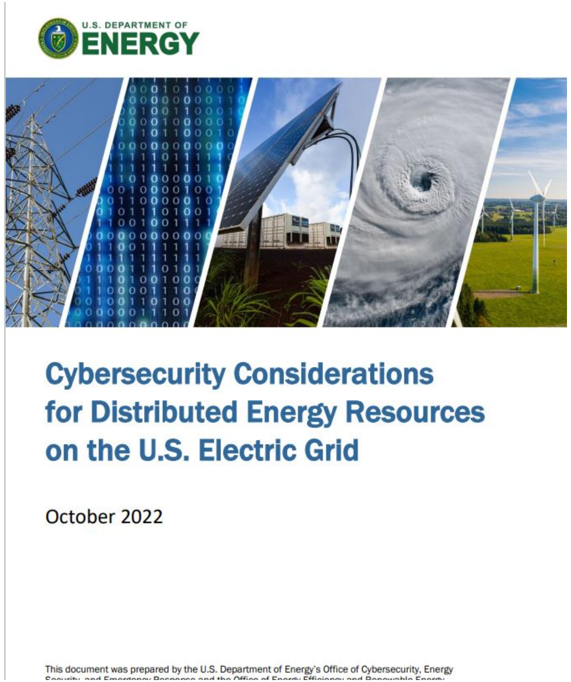
TECHNICAL REPORT

PES-TR105

Towards Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector

PREPARED BY THE
IEEE/NERC Joint Task Force on Security Integration into
BPS Engineering Practices

TR-105 – Integrating Cyber and Physical Security into Bulk Power System Engineering Practices
i



Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid

October 2022

This document was prepared by the U.S. Department of Energy's Office of Cybersecurity, Energy
Security, and Emergency Response and the Office of Energy Efficiency and Renewable Energy

Cybersecurity a Key Challenge and an EERE Priority

Goal 1: Accelerate Cyber Resilience R&D of EERE Operational Technologies

1.1 Improve cybersecurity defenses and resilience.

1.2 Mitigate vulnerabilities

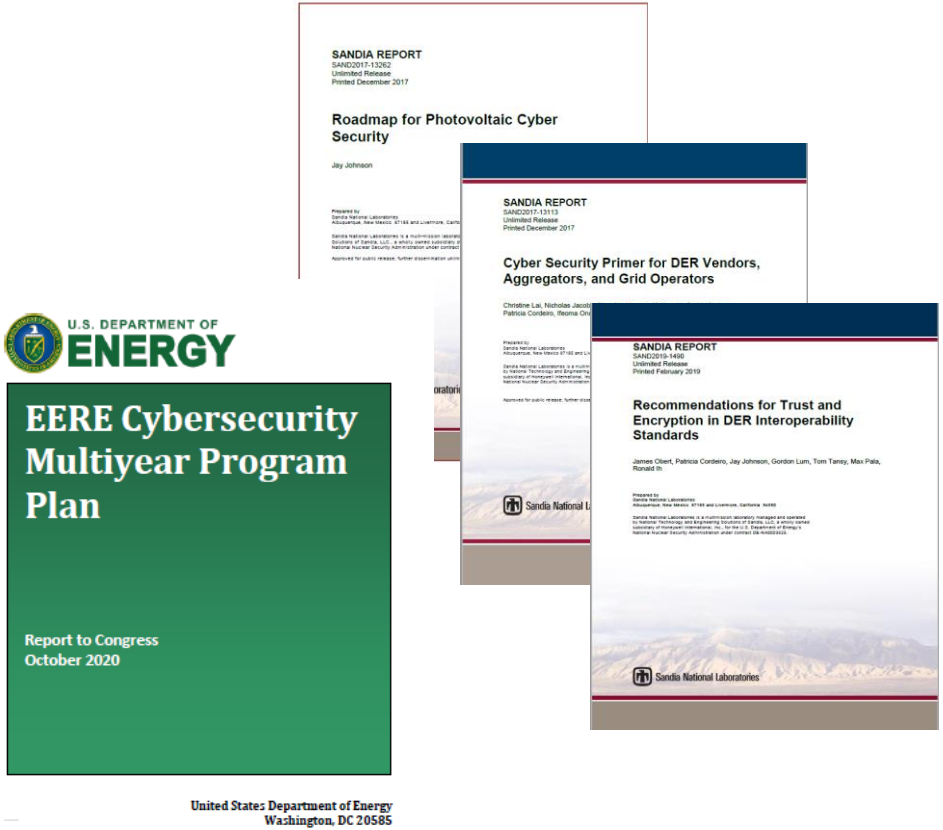
1.3 Next-generation cyber resilient technologies.

Goal 2: Increase EERE Stakeholder Cybersecurity Awareness

2.1 Improve situational awareness.

2.2 Enhance EERE technology cybersecurity maturity.

2.3 Identify opportunities for EERE stakeholder participation in cyber incident response exercises.



SANDIA REPORT
SAND2017-13262
Unlimited Release
Printed December 2017

Roadmap for Photovoltaic Cyber Security

Jay Johnson

SANDIA REPORT
SAND2017-13113
Unlimited Release
Printed December 2017

Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators

Christine Lai, Nicholas Jacob
Patricia Cordeiro, Ifeoma Onu

U.S. DEPARTMENT OF ENERGY

EERE Cybersecurity Multiyear Program Plan

Report to Congress
October 2020

United States Department of Energy
Washington, DC 20585

SANDIA REPORT
SAND2019-1490
Unlimited Release
Printed February 2019

Recommendations for Trust and Encryption in DER Interoperability Standards

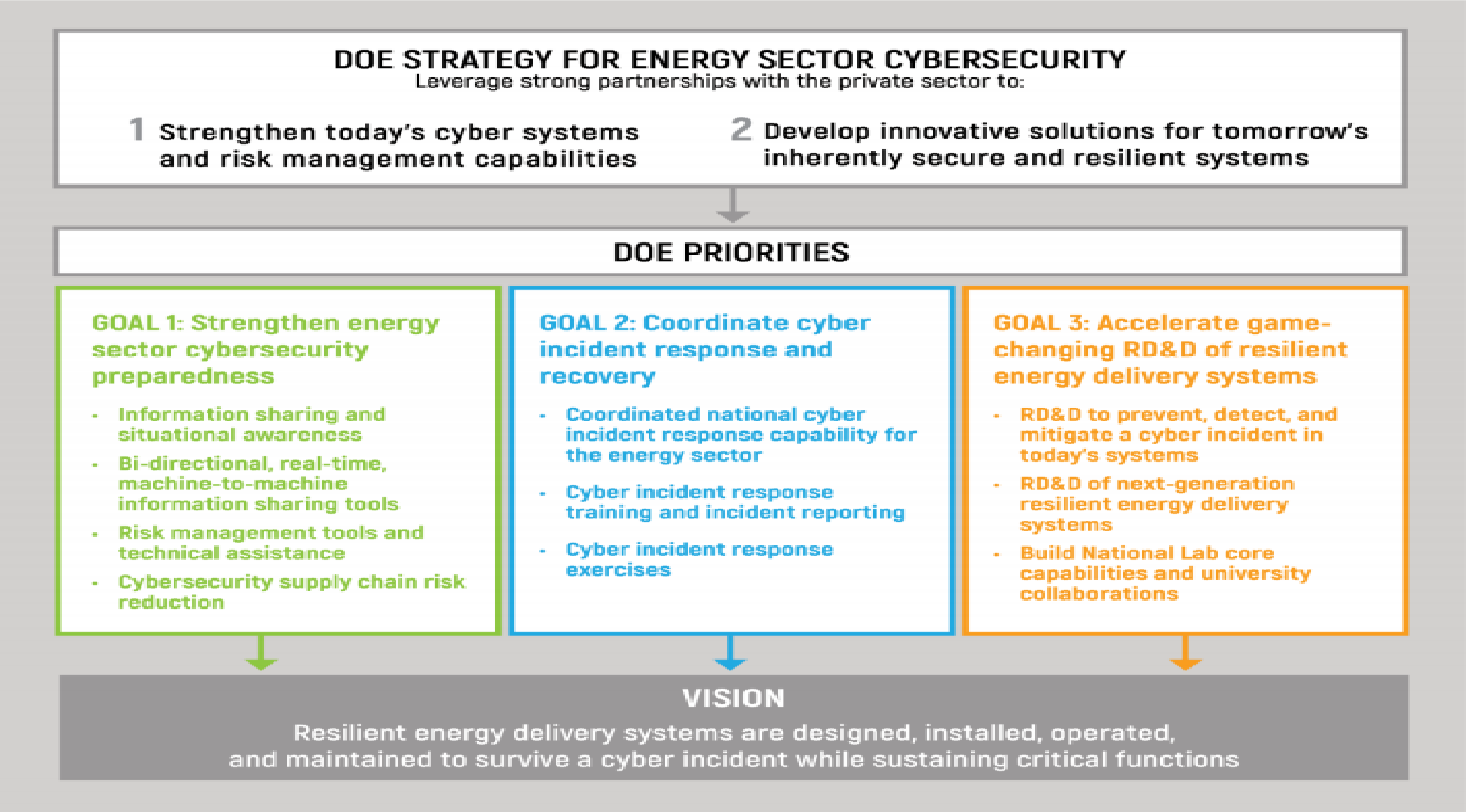
James Obert, Patricia Cordeiro, Jay Johnson, Gordon Lum, Tom Tansy, Max Pala, Ronald Ih

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

EERE and SETO Activities Align With DOE’s Broader Cybersecurity Strategies



DOE STRATEGY FOR ENERGY SECTOR CYBERSECURITY

Leverage strong partnerships with the private sector to:

1 Strengthen today’s cyber systems and risk management capabilities

2 Develop innovative solutions for tomorrow’s inherently secure and resilient systems

DOE PRIORITIES

GOAL 1: Strengthen energy sector cybersecurity preparedness

- Information sharing and situational awareness
- Bi-directional, real-time, machine-to-machine information sharing tools
- Risk management tools and technical assistance
- Cybersecurity supply chain risk reduction

GOAL 2: Coordinate cyber incident response and recovery

- Coordinated national cyber incident response capability for the energy sector
- Cyber incident response training and incident reporting
- Cyber incident response exercises

GOAL 3: Accelerate game-changing RD&D of resilient energy delivery systems

- RD&D to prevent, detect, and mitigate a cyber incident in today’s systems
- RD&D of next-generation resilient energy delivery systems
- Build National Lab core capabilities and university collaborations

VISION

Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions

S2G: Securing Solar for the Grid

VISION

Achieving high cybersecurity maturity levels for solar technologies, equipment, supply chains, facilities, as well as the bulk and distribution electric power grids.

GOAL

Ensure the cybersecurity of electric grids with high penetration levels of solar PV and other DERs

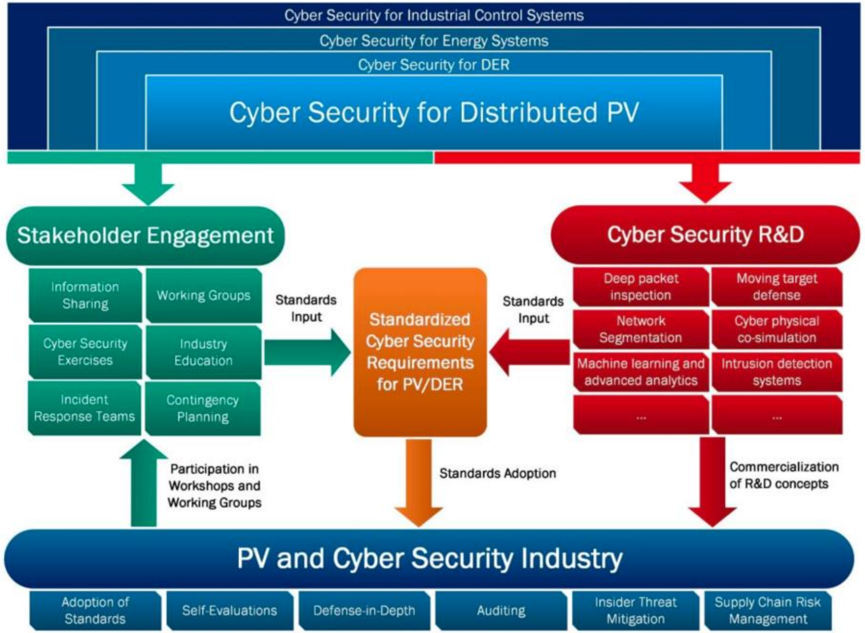
APPROACH

A collaborative effort by multiple national labs, DOE offices, and industry to address gaps in requirement standards, best practices, testing and analysis for solar PV and DERs cybersecurity

EXPECTED OUTCOMES

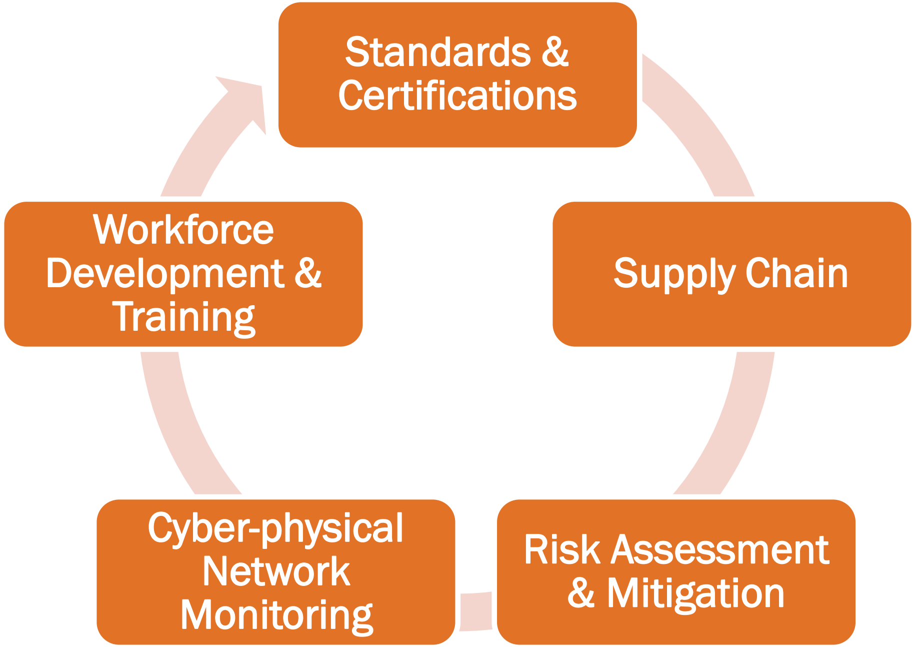
Development and dissemination of **requirement standards, best practices**, **equipment testing procedures, assessment tools, as well as education and training materials** for cyber defense, posture and maturity tailored to solar technologies.

Securing Solar for the Grid (S2G): Cyber-physical Integrated Approach



Cyber Security for Industrial Control Systems
Cyber Security for Energy Systems
Cyber Security for DER
Cyber Security for Distributed PV
Stakeholder Engagement
Information Sharing
Working Groups
Cyber Security Exercises
Industry Education
Incident Response Teams
Contingency Planning
Standards Input
Standardized Cyber Security Requirements for PV/DER
Standards Input
Cyber Security R&D
Deep packet inspection
Moving target defense
Network Segmentation
Cyber physical co-simulation
Machine learning and advanced analytics
Intrusion detection systems
...
...
Participation in Workshops and Working Groups
Standards Adoption
Commercialization of R&D concepts
PV and Cyber Security Industry
Adoption of Standards
Self-Evaluations
Defense-in-Depth
Auditing
Insider Threat Mitigation
Supply Chain Risk Management

Source: RoadmapforPhotovoltaicCyberSecuritySAND2017-132624-10-2018



Standards & Certifications
Supply Chain
Risk Assessment & Mitigation
Cyber-physical Network Monitoring
Workforce Development & Training

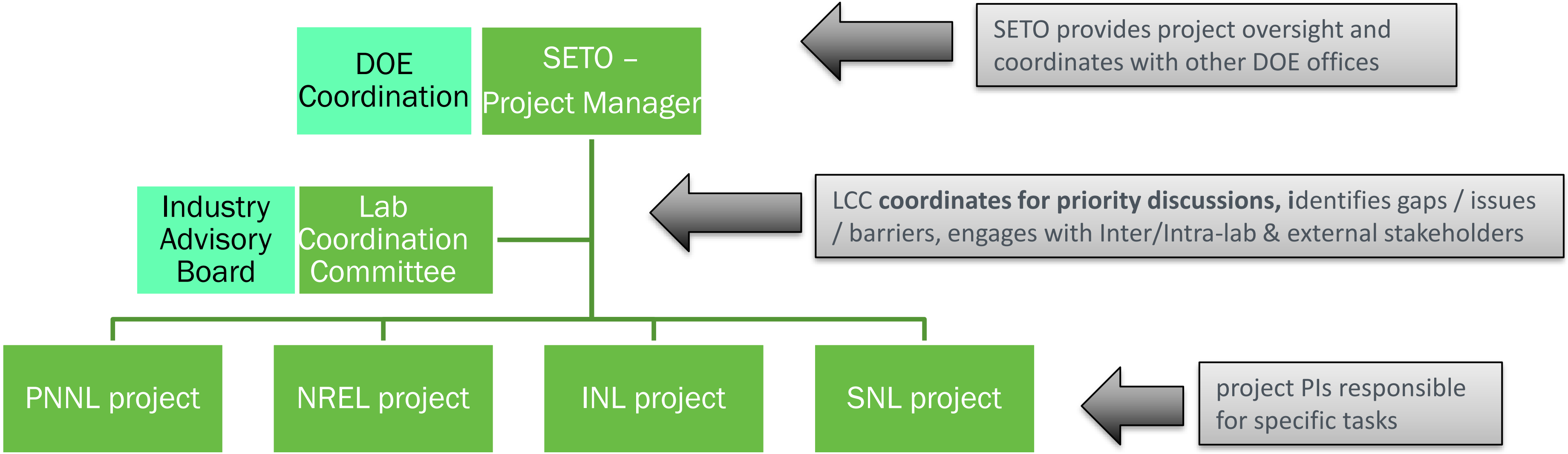
Sandia National Laboratories

INL Idaho National Laboratory

NREL Transforming ENERGY

Pacific Northwest NATIONAL LABORATORY

Project Management Structure



DOE Coordination

SETO – Project Manager

Industry Advisory Board

Lab Coordination Committee

PNNL project

NREL project

INL project

SNL project

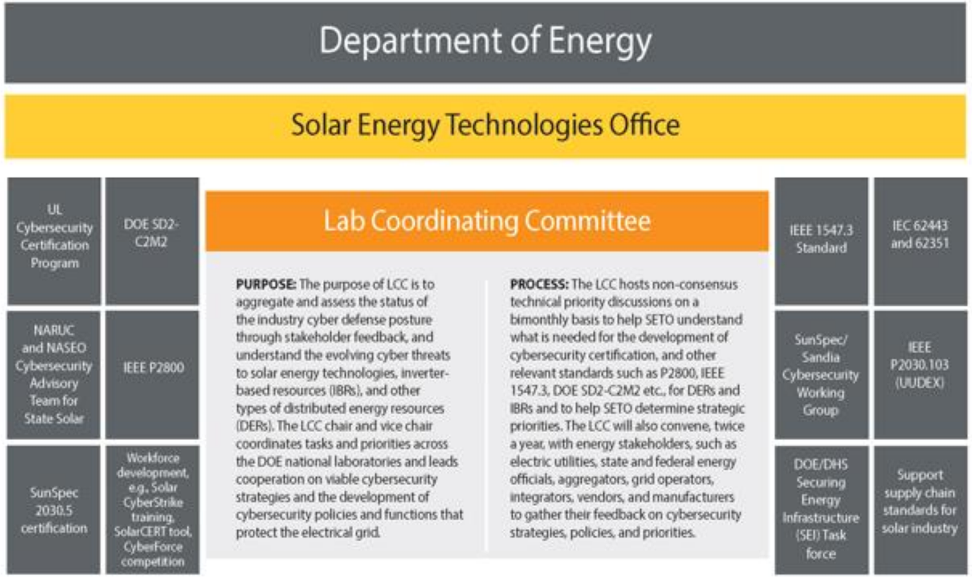
SETO provides project oversight and coordinates with other DOE offices

LCC **coordinates for priority discussions,** identifies gaps / issues / barriers, engages with Inter/Intra-lab & external stakeholders

project PIs responsible for specific tasks

LCC Activities

- Regularly meet to assess current industry trends and facilitate non-consensus discussion and debate on project priorities.
- Coordinate activities and promotes collaboration with CESER and EERE offices.
- Facilitate Industry Advisory Board meetings. The purpose is to:
  - Gather industry priorities and effectiveness feedback
  - Perform stakeholder engagement to assess industry gaps, issues, and barriers
  - Disseminate project outcomes
  - Perform continuous reprioritization evaluation.
- Facilitate periodic informational webinars, led or supported by the national labs.



Department of Energy
Solar Energy Technologies Office
Lab Coordinating Committee
UL Cybersecurity Certification Program
DOE SD2-C2M2
NARUC and NASEO Cybersecurity Advisory Team for State Solar
IEEE P2800
SunSpec 2030.5 certification
Workforce development, e.g., Solar CyberStrike training, SolarCERT tool, CyberForce competition
IEEE 1547.3 Standard
IEC 62443 and 62351
SunSpec/ Sandia Cybersecurity Working Group
IEEE P2030.103 (UUDEX)
DOE/DHS Securing Energy Infrastructure (SEI) Task force
Support supply chain standards for solar industry

PURPOSE: The purpose of LCC is to aggregate and assess the status of the industry cyber defense posture through stakeholder feedback, and understand the evolving cyber threats to solar energy technologies, inverter-based resources (IBRs), and other types of distributed energy resources (DERs). The LCC chair and vice chair coordinates tasks and priorities across the DOE national laboratories and leads cooperation on viable cybersecurity strategies and the development of cybersecurity policies and functions that protect the electrical grid.

PROCESS: The LCC hosts non-consensus technical priority discussions on a bimonthly basis to help SETO understand what is needed for the development of cybersecurity certification, and other relevant standards such as P2800, IEEE 1547.3, DOE SD2-C2M2 etc., for DERs and IBRs and to help SETO determine strategic priorities. The LCC will also convene, twice a year, with energy stakeholders, such as electric utilities, state and federal energy officials, aggregators, grid operators, integrators, vendors, and manufacturers to gather their feedback on cybersecurity strategies, policies, and priorities.

Research Areas

STANDARDS DEVELOPMENT & BEST PRACTICES

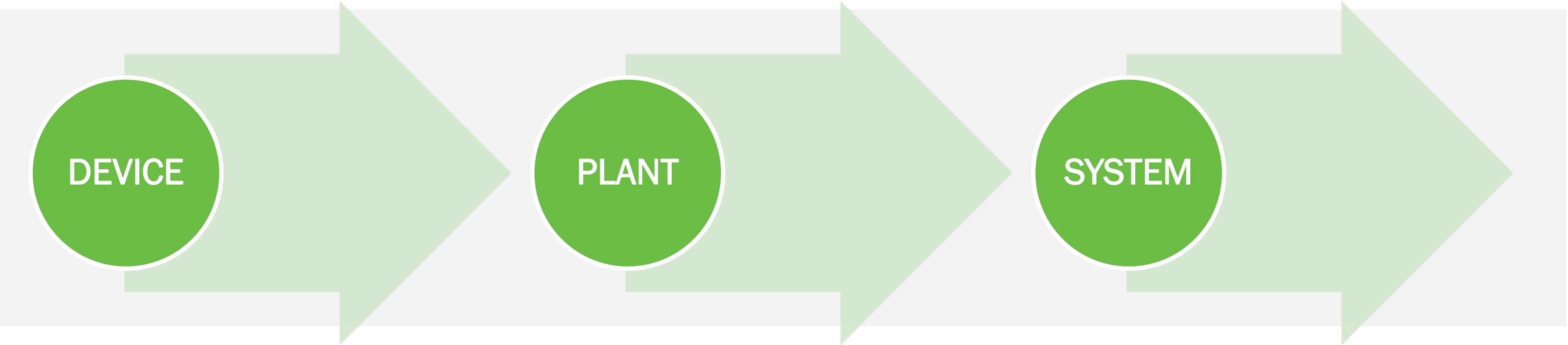
Stakeholder engagement to investigate gaps and develop best practices that can become standards to enable the secure integration of inverter-based resources and DERs.

EDUCATION & WORKFORCE DEVELOPMENT

Development of educational modules and training to increase cybersecurity awareness and knowledge within solar stakeholders.

CYBERSECURITY TOOL KIT & SUPPLY CHAIN

R&D of tools to understand cybersecurity posture, risk assessment to inform investments, and device design security & maturity model for cyber supply chain.



INCREASING CYBERSECURITY LEVELS OF SOLAR TECHNOLOGIES

Project Activities

STANDARDS DEVELOPMENT & BEST PRACTICES

- NREL & UL established requirements for IBR/DER cybersecurity certification
- NREL published IEEE 1547.3 cybersecurity guide for DERs.
- NREL conducted initial gap analysis for supply chain cybersecurity.
- Cybersecurity risk analysis for DERS
- Cybersecurity requirements for DERMS.
- Support SDOs working groups

EDUCATION, WORKFORCE & STAKEHOLDER ENGAGMENT

- Leveraging CESER's Cyber Strike, SNL & INL developed training modules and demonstrations to train solar cyber defenders. Created first 5 lessons for the Solar CyberStrike program, DER Simulator with SunSpec Modbus and IEEE 2030.5 server, and single-axis tracking system.
- Support the development of cybersecurity requirements for state energy officials (NASEO and NARUC).
- Engagement with solar vendors for project participation.
- Industry Advisory Board

CYBERSECURITY TOOLKIT & SUPPLY CHAIN

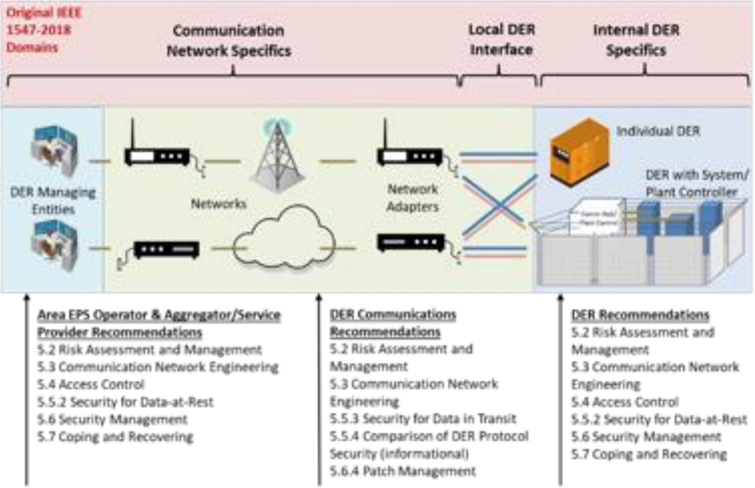
- SNL & INL created the Solar Cybersecurity Evaluation and Risk Informed Toolkit (SolarCERT) leveraging DHS' CSET.
- SNL Security Orchestration and Automation and Response.
- PNNL Cyber-Physical Detection and Range (CPYDAR) tool to enable the development, replication and benchmarking of cyber security test procedures for solar PV test system models.
- PNNL Secure-design & development maturity model and assessment tool for DERs (S2D-C2M2) solar vendors.

S2G: SECURING SOLAR FOR THE GRID

STANDARDS & CERTIFICATIONS

Upcoming Guides & DER Certification Programs

- **Cybersecurity Guidance**
- IEEE 1547.3 "Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems"
- **DER Certification Programs**
- UL 2941 "Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources"
- SunSpec DER Cybersecurity Certification Program, announced April 28, 2022 (https://sunspec.org/sunspec-cybersecurity-certification-work-group/)



Original IEEE 1547-2018 Domains

Communication Network Specifics

Local DER Interface

Internal DER Specifics

DER Managing Entities

Networks

Network Adapters

Individual DER

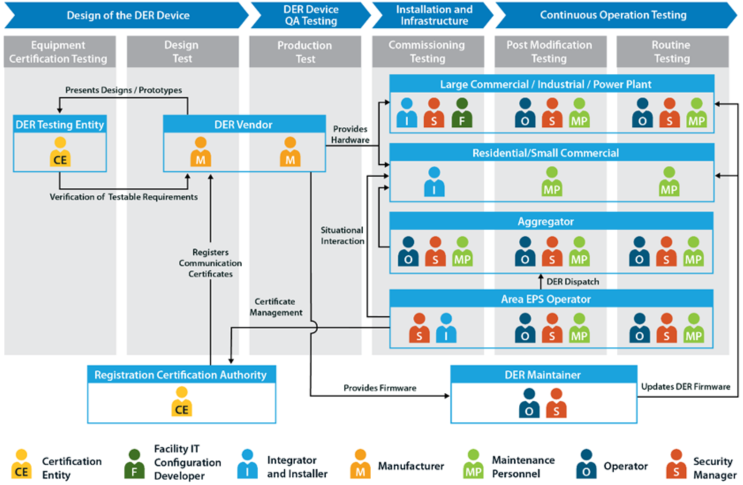
DER with System/ Plant Controller

Area EPS Operator & Aggregator/Service Provider Recommendations
5.2 Risk Assessment and Management
5.3 Communication Network Engineering
5.4 Access Control
5.5.2 Security for Data-at-Rest
5.6 Security Management
5.7 Coping and Recovering

DER Communications Recommendations
5.2 Risk Assessment and Management
5.3 Communication Network Engineering
5.5.3 Security for Data in Transit
5.5.4 Comparison of DER Protocol Security (informational)
5.6.4 Patch Management

DER Recommendations
5.2 Risk Assessment and Management
5.3 Communication Network Engineering
5.4 Access Control
5.5.2 Security for Data-at-Rest
5.6 Security Management
5.7 Coping and Recovering

IEEE 1547.3 Scope



Design of the DER Device

DER Device QA Testing

Installation and Infrastructure

Continuous Operation Testing

Equipment Certification Testing

Design Test

Production Test

Commissioning Testing

Post Modification Testing

Routine Testing

Presents Designs / Prototypes

DER Testing Entity

CE

DER Vendor

M M

Verification of Testable Requirements

Provides Hardware

Situational Interaction

Registers Communication Certificates

Certificate Management

Large Commercial / Industrial / Power Plant

I S F O S MP O S MP

Residential/Small Commercial

I MP MP

Aggregator

O S MP O S MP O S MP

DER Dispatch

Area EPS Operator

S I O S MP O S MP

Registration Certification Authority

CE

Provides Firmware

DER Maintainer

O S

Updates DER Firmware

CE Certification Entity

F Facility IT Configuration Developer

I Integrator and Installer

M Manufacturer

MP Maintenance Personnel

O Operator

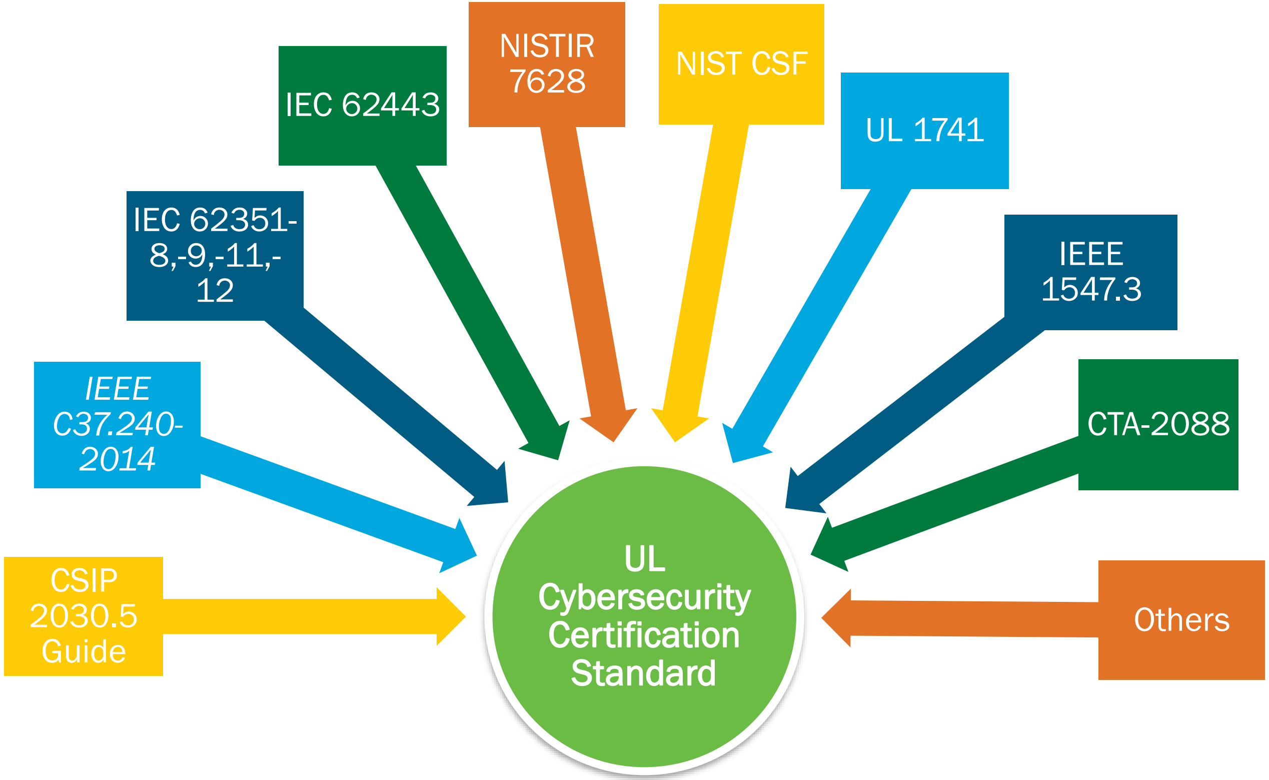
S Security Manager

Cybersecurity Tests in IEEE 1547.3

Many Standards and Guides Exist – Why a New One?

The UL cybersecurity certification standard will:

- Build on past work
- Map and leverage security requirements from industry best practices for hardware and software
- Provide an information hub for DER Industry stakeholders
- Establish “security by design”

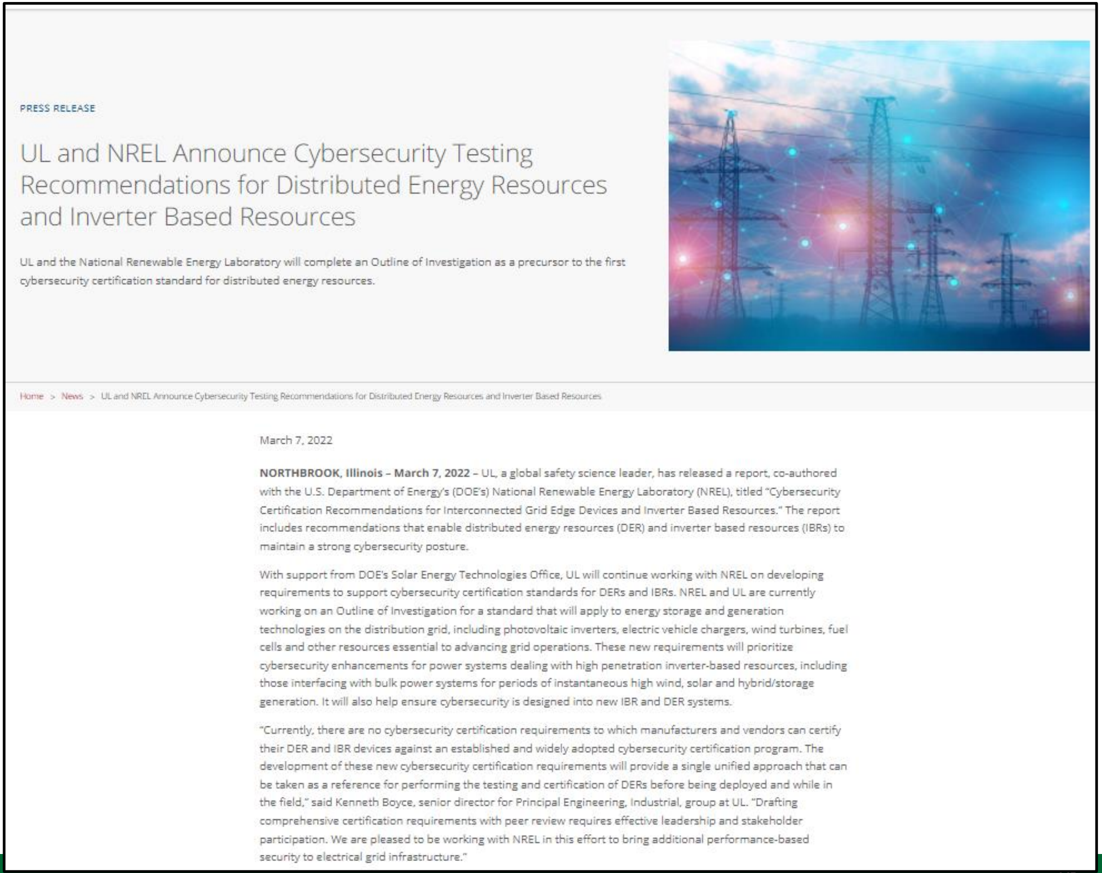


Note: All these standards serve a different purpose. The UL cybersecurity certification standard will not replace them by any means.

Outline of Investigation (OOI) for UL 2941

- The requirements will provide a single unified approach for testing and certification of DERs *in advance* of deployment.
- The certification will be applicable to generation and energy storage technologies.

- UL and NREL are actively developing the OOI.
- **We will welcome participation from industry.**
- To receive news and information, please visit UL news.



PRESS RELEASE

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

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

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

March 7, 2022

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

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

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

S2G: SECURING SOLAR FOR THE GRID

RISK ASSESSMENT & MITIGATION

INL Cyber SHIELD-INL CERT

INL *Cybersecurity Risk Evaluation Tool*

Main Goal

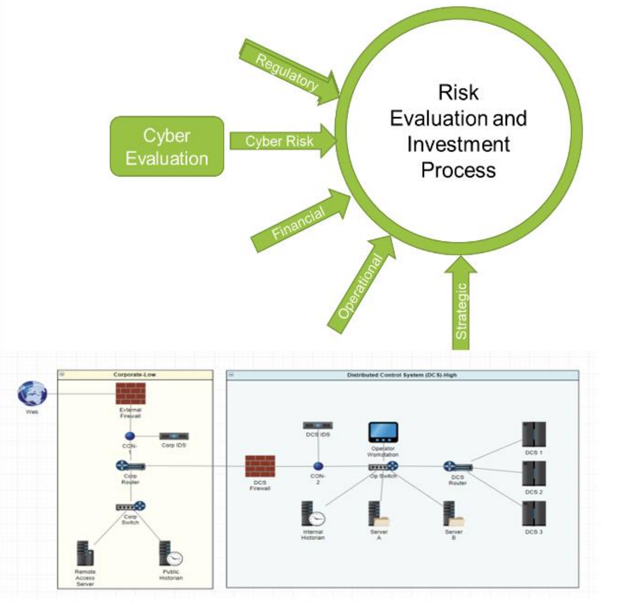
Deliver a standardized, repeatable cybersecurity valuation methodology that is tuned to the needs and characteristics of the renewable industry subsectors and can provide insight and guidance quantitatively to better informed, broader, risk-based investment decisions surrounding renewable IT and OT cybersecurity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

Key features:

- ✓ Renewable Sector Focused Capability
- ✓ Leverages DHS CSET tool, with multiple years of $$$ investment
- ✓ Open-Source and tuned for Solar 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. Design tool to map network architecture and obtain clear view to common design related risks and mitigation options
3. Immediate access to input supporting program and resource planning capabilities to more quickly meet maturity objectives



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Network Diagram

IDAHO NATIONAL LABORATORY

SHIELD–Malcolm

Asset Interaction Analysis

Main Goal

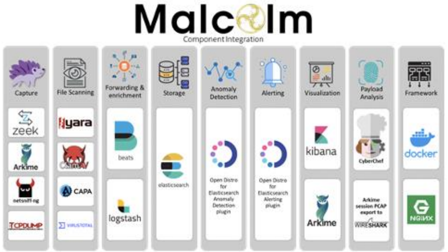
Links assets to business processes and translates business processes to OT devices. Supports deeper threat and vulnerability identification/analysis for user

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 you identify potential attacks, vulnerabilities, active exploits with more precision specific to your assets/devices
3. Increases visibility into your network to inform decisions and improve reliability



Asset Interaction Analysis

Malcolm

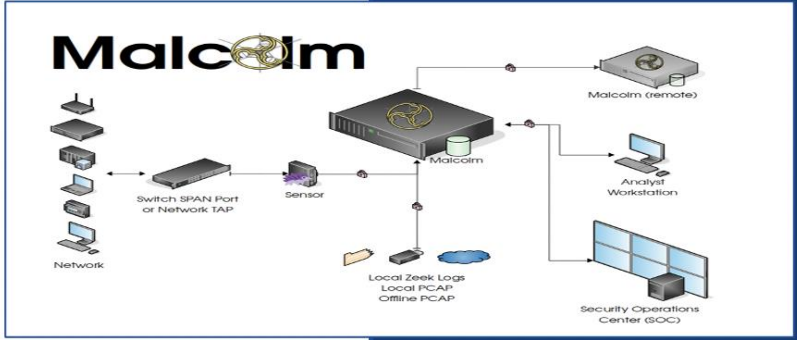
Malcolm Key Benefits & Deployment Overview

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



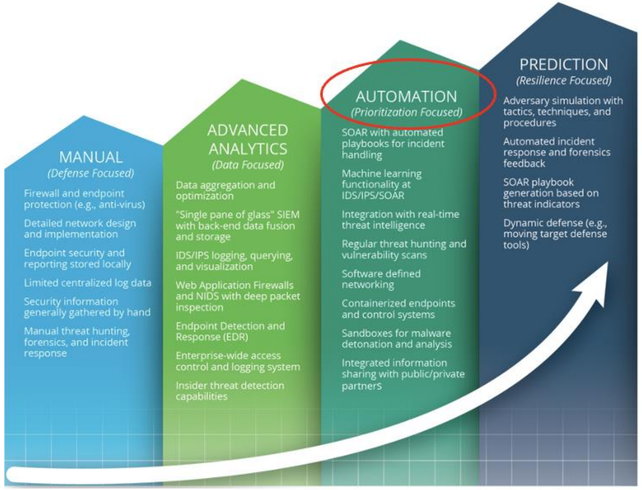
IDAHO NATIONAL LABORATORY

S2G: SECURING SOLAR FOR THE GRID

CYBER-PHYSICAL NETWORK MONITORING

Security Orchestration for DER Equipment

- Sandia developing next-generation **security automation** incorporating multiple data streams and threat intelligence.
  - Threat, intrusion detection, and other data is pooled into a Security Information and Event Management (SIEM) application in the **Security Operations Center** (SOC).
  - Detects a variety of DER attacks and **responds quickly** (<30 second response time).
  - Automated or human-in-the-loop responses: network topology changes, block IPs, revoke access/certs, modifying VPN/SSH access, etc.

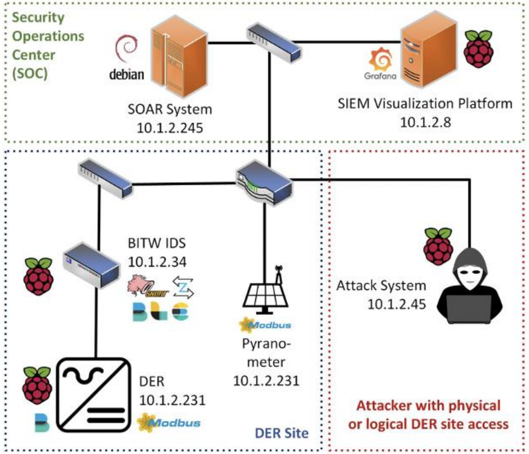

MANUAL
(Defense Focused)
Firewall and endpoint protection (e.g., anti-virus)
Detailed network design and implementation
Endpoint security and reporting stored locally
Limited centralized log data
Security information generally gathered by hand
Manual threat hunting, forensics, and incident response

ADVANCED ANALYTICS
(Data Focused)
Data aggregation and optimization
"Single pane of glass" SIEM with back-end data fusion and storage
IDS/IPS logging, querying, and visualization
Web Application Firewalls and NIDS with deep packet inspection
Endpoint Detection and Response (EDR)
Enterprise-wide access control and logging system
Insider threat detection capabilities

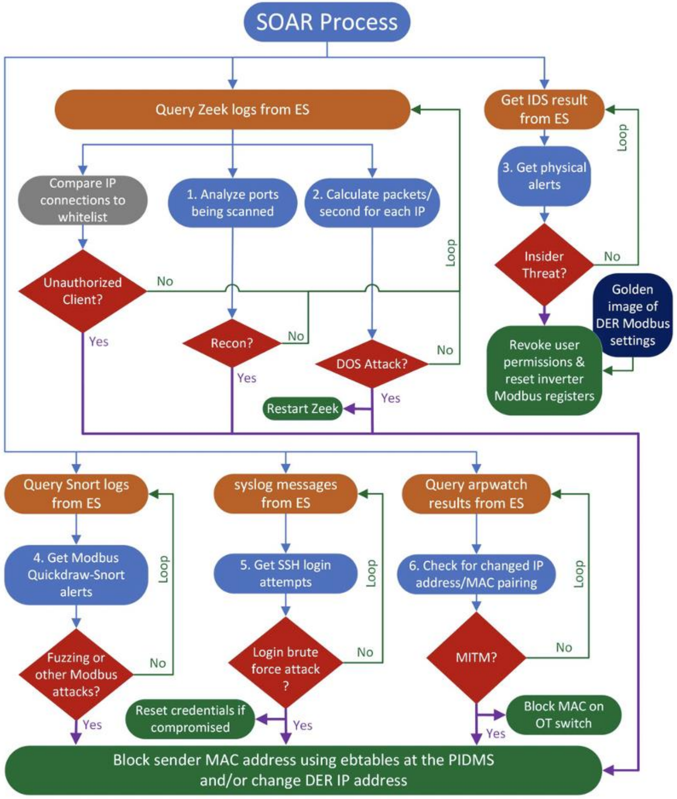
AUTOMATION
(Prioritization Focused)
SOAR with automated playbooks for incident handling
Machine learning functionality at IDS/IPS/SOAR
Integration with real-time threat intelligence
Regular threat hunting and vulnerability scans
Software defined networking
Containerized endpoints and control systems
Sandboxes for malware detonation and analysis
Integrated information sharing with public/private partners

PREDICTION
(Resilience Focused)
Adversary simulation with tactics, techniques, and procedures
Automated incident response and forensics feedback
SOAR playbook generation based on threat indicators
Dynamic defense (e.g., moving target defense tools)

SOC Maturity Levels



Sandia Testbed


SOAR Process
Query Zeek logs from ES
Compare IP connections to whitelist
1. Analyze ports being scanned
2. Calculate packets/ second for each IP
Unauthorized Client?
No
Yes
Recon?
No
Yes
DOS Attack?
No
Yes
Restart Zeek
Loop
Get IDS result from ES
3. Get physical alerts
Insider Threat?
No
Loop
Golden image of DER Modbus settings
Revoke user permissions & reset inverter Modbus registers
Query Snort logs from ES
4. Get Modbus Quickdraw-Snort alerts
Fuzzing or other Modbus attacks?
No
Yes
Loop
syslog messages from ES
5. Get SSH login attempts
Login brute force attack ?
No
Yes
Loop
Reset credentials if compromised
Query arpwatch results from ES
6. Check for changed IP address/MAC pairing
MITM?
No
Yes
Loop
Block MAC on OT switch
Block sender MAC address using ebtables at the PIDMS and/or change DER IP address
1

Automated Response Playbook

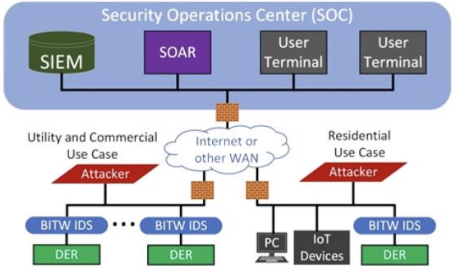
Intrusion Detection and Mitigation for Photovoltaics

2022 R&D 100 WINNER

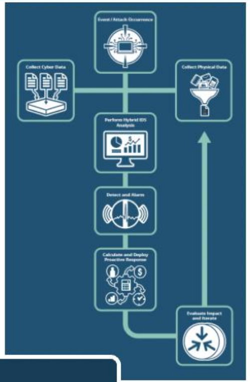
Sandia is developing solar-specific Security Operations Centers (SOCs) with intrusion detection and automated mitigation

- Cyber-physical approach uses network and power system data to detect attacks
- Adaptive Resonance Theory establishes detection thresholds for physical attacks with online learning

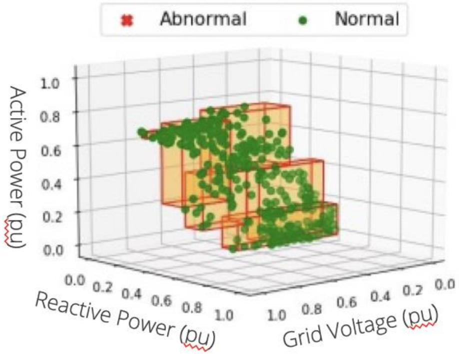
Security Operations Center



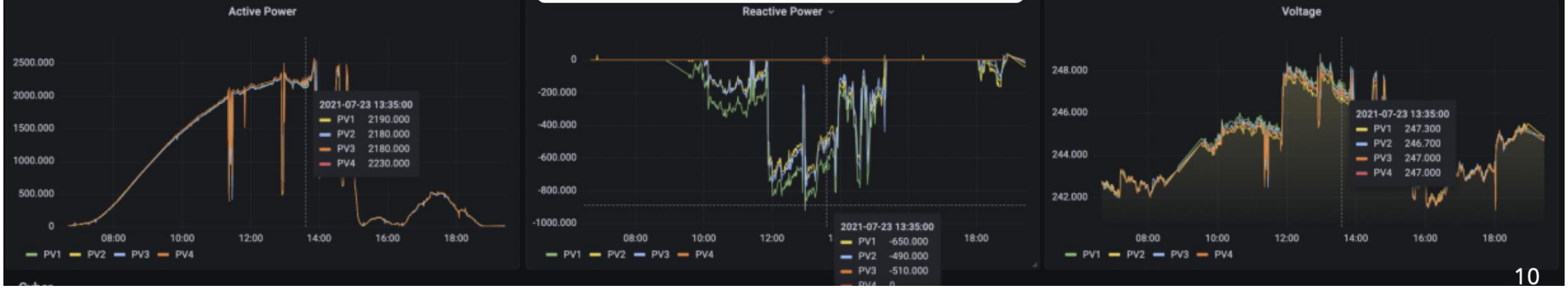
Hybrid analysis and mitigation process


Event / Attack Occurrence
Collect Cyber Data
Collect Physical Data
Perform Hybrid IDS Analysis
Detect and Alarm
Calculate and Deploy Proactive Response
Evaluate Impact and Iterate

Machine learning data classification



Physical DER data



S2G: SECURING SOLAR FOR THE GRID

Workforce Development & Training

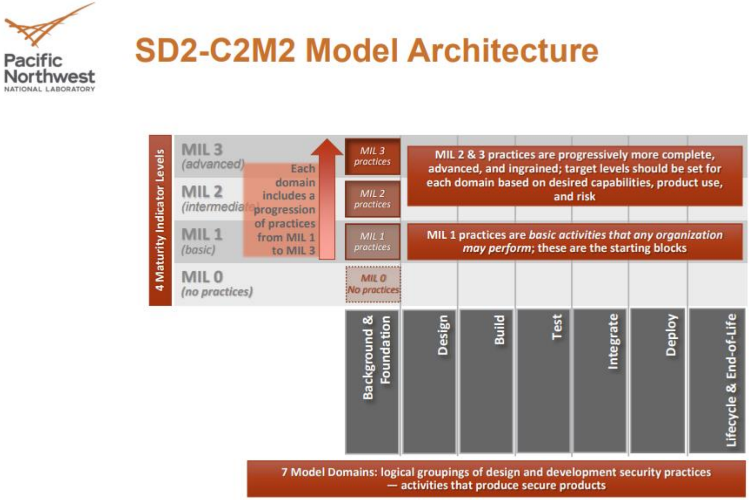
Training solar cyber defenders

- Sandia is creating a new renewable energy cybersecurity **CyberStrike training program** for solar inverters, EV chargers, and wind systems.
- 8-hour classes with lectures (slides) and exercises
  - Virtual machine environment for hands-on training without hardware
  - Implementing a hands-on training with hardware including a single axis solar tracker.
- Hardware prototypes have been designed and are being prepared for production.

S2G: SECURING SOLAR FOR THE GRID

Supply Chain

Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2)

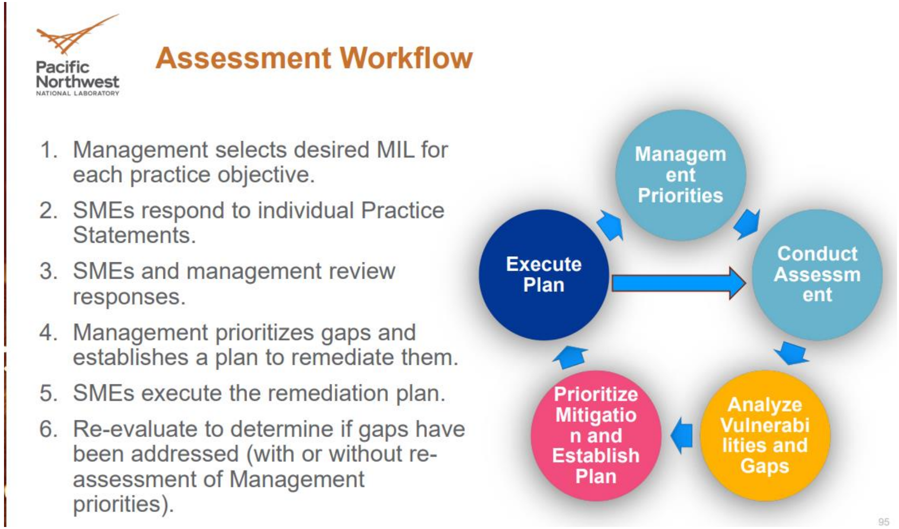


SD2-C2M2 Model Architecture

MIL 2 & 3 practices are progressively more complete, advanced, and ingrained; target levels should be set for each domain based on desired capabilities, product use, and risk

MIL 1 practices are *basic activities that any organization may perform*; these are the starting blocks

7 Model Domains: logical groupings of design and development security practices — activities that produce secure products



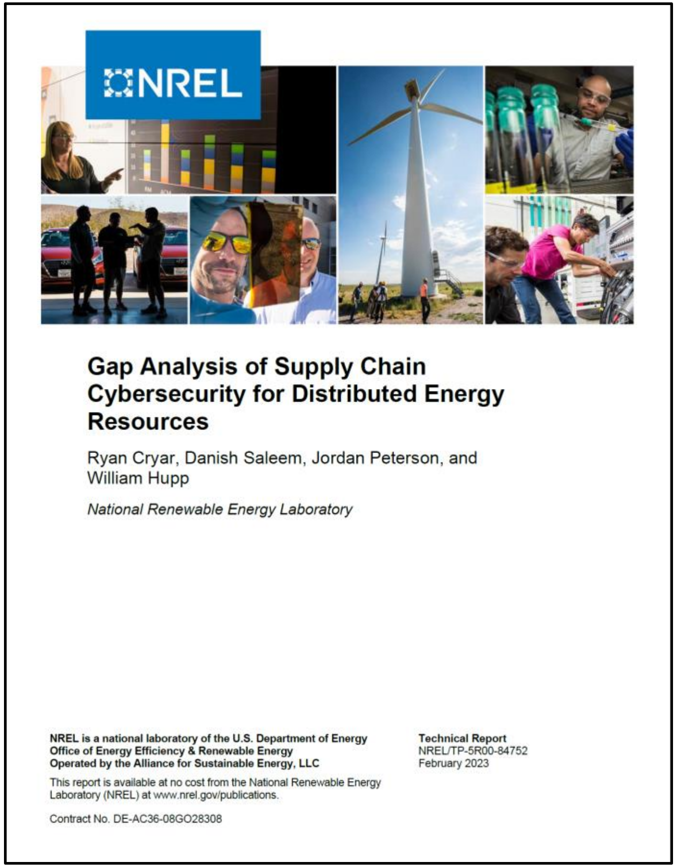
Assessment Workflow

1. Management selects desired MIL for each practice objective.
2. SMEs respond to individual Practice Statements.
3. SMEs and management review responses.
4. Management prioritizes gaps and establishes a plan to remediate them.
5. SMEs execute the remediation plan.
6. Re-evaluate to determine if gaps have been addressed (with or without re-assessment of Management priorities).

Managem ent Priorities
Conduct Assessm ent
Analyze Vulnerabi lities and Gaps
Prioritize Mitigatio n and Establish Plan
Execute Plan
95

Report: Supply Chain Cybersecurity for Clean Energy Sector

- Establish a framework for DER supply chain cybersecurity
- Engage industry for assessments
- Create open-source software guidance
- Establish a testing and certification ecosystem for DER software supply chain cybersecurity
- Address the issue of lacking standards for DER supply chain cybersecurity
- Form working groups for best practices



NREL

Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources

Ryan Cryar, Danish Saleem, Jordan Peterson, and William Hupp

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-84752
February 2023

In Conclusion

- ❑ The rapid deployment of renewables and distributed energy resources onto the power grid presents new challenges to energy sector cybersecurity.
- ❑ A **holistic approach** in information technology (IT) and operation technology (OT) risk management is needed that encompass utility systems with customer owned DER devices and third-party operated systems.
- ❑ Need to build **community awareness and information sharing** mechanisms to incorporates equipment standards and vigorous testing, validation, and certification – including global supply chains for products like solar inverters.
- ❑ The **DOE and national labs** can provide technical expertise, research and testing capabilities, and funding to support industry
- ❑ **Collaboration** is crucial – within DOE program offices, other federal agencies, state and local governments, and industry.

S2G: SECURING SOLAR FOR THE GRID

End of Presentation