INL/MIS-24-77147-Revision-0

Securing Solar for the Grid: Spring 2024 IAB Meeting

March 2024

Megan Jordan Culler, Jake P Gentle, John Clay Bell II, Rita A Foster, Emma Mary Stewart, Daniel Alan Ricci

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-24-77147-Revision-0

Securing Solar for the Grid: Spring 2024 IAB Meeting

Megan Jordan Culler, Jake P Gentle, John Clay Bell II, Rita A Foster, Emma Mary Stewart, Daniel Alan Ricci

March 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Funded by:

SOLAR ENERGY
TECHNOLOGIES OFFICE
U.S. Department Of Energy

Securing Solar for the Grid (S2G)

Spring 2024 IAB Meeting

Presented on: March 14, 2024

Lab Coordinating Committee (LCC) Chair: Megan Culler (INL)
LCC Co-Chair: Danish Saleem (NREL)

Spring 2024 S2G IAB Meeting Agenda

- SETO Welcome (Marissa Morales-Rodriguez)
- LCC Updates (Megan Culler)
- Lab Updates
  - INL (Megan Culler)
  - NREL (Danish Saleem)
  - PNNL (Scott Mix)
  - Sandia (Birk Jones)
- Solar Cybersecurity Roadmap Workshop
- Upcoming Activities and Closeout

Funded by:

SOLAR ENERGY
TECHNOLOGIES OFFICE
U.S. Department Of Energy

Securing Solar for the Grid (S2G)

Lab Coordinating Committee Updates

Presented on: March 14, 2024

LCC Chair: Megan Culler
LCC Co-Chair: Danish Saleem

Funded by:

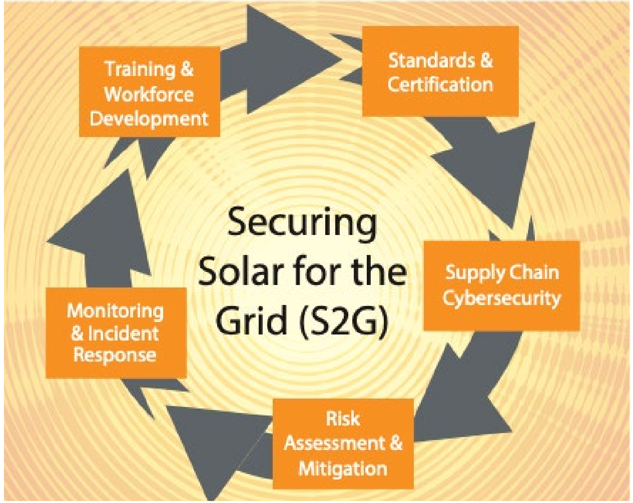
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Securing Solar for the Grid

Background and Objectives

- Growth of solar penetration along with historical lack of cybersecurity standards and industry awareness drives need for research and deployment-ready solutions
- Work with industry to address gaps in solar cybersecurity standards
- Develop tools and resources for cyber risk assessment
- Assess supply chain impacts and mitigations
- Promote training and education for solar stakeholders
- Advance monitoring & incident response capabilities

64 individuals representing 30+ organizations!



Training & Workforce Development
Standards & Certification
Securing Solar for the Grid (S2G)
Supply Chain Cybersecurity
Risk Assessment & Mitigation
Monitoring & Incident Response

Industry Advisory Board Members:

Trade associations (3)

Utilities (4)

Developers (2)

Manufacturers (3)

Consultants (5)

Security Solutions (7)

Standards Development Organizations (4)

Regulators (3)

Other (3)

Lab Coordinating Committee

NREL Transforming ENERGY

Pacific Northwest NATIONAL LABORATORY

Sandia National Laboratories

INL Idaho National Laboratory

Focus Areas of S2G

	FY22	FY23	FY24
National Renewable Energy Laboratory (NREL)	• Support UL cybersecurity certification program • Support for IEEE 1547.3 cybersecurity guide • Support supply chain security related activities • Convene, coordinate, facilitate LCC meetings	• Support UL cybersecurity certification program • Co-lead IEEE 1547.3 cybersecurity guide • Co-lead effort of including of cybersecurity in IEEE 1547-2025 standard revision • Support supply chain cybersecurity-related efforts • Support DERMS cybersecurity-related efforts • Convene, coordinate, facilitate & co-lead LCC meetings.	• Publish UL 2941 cybersecurity certification outline of investigation and support UL 2941 Technical Committee for consensus development. • Publish IEEE 1547.3 cybersecurity guide as vice-chair and support including cybersecurity recommendation to IEEE 1547-2025 standard requirements. • Develop test procedures for UL 2941 using single PV inverter and shared with UL • Incorporated industry and DOE feedback to DERMS cybersecurity paper
Pacific Northwest National Laboratory (PNNL)	• Support supply chain standards work for solar industry • Update distribution model to include Solar PV Resources • Perform Secure Design Cybersecurity Capability Maturity Model (SD2-C2M2) assessments.	• Support supply chain standards work for solar industry • Perform Secure Design Cybersecurity Capability Maturity Model (SD2-C2M2) assessments.	• Convert IEEE-9500 and LV Network to ePHASORSIM model with Solar DER and post with other converted models on GitHub • Perform Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2) assessments • Develop Solar Power Resilience Maturity Model (Sol-ReMM) tool
Idaho National Laboratory (INL)	• Support the development of Solar Cert tool • Develop Solar CyberStrike training and tool.	• Establish a risk assessment methodology by leveraging DHS's CSET tool tuned to solar industry • Develop Solar CyberStrike training and tool. • Supply chain security and automated cyber analysis	• Develop focused industry engagement strategy to use across tasks • Pilot full CyberStrike STOMCLOUD training • Promote adoption of risk analysis toolsets • Build HBOM library for solar • Explore ML for codified attack surface and defense
Sandia National Laboratories (Sandia)	• Support DHS Cyber Security Evaluation Tool • Develop Solar CyberStrike training and tool.	• SunSpec/Sandia cyber security working group • System level orchestration and automated response for security operation center. • Vulnerability analysis	• Define best practice for PV inverter secure boot, PV inverter vulnerability disclosure process • Development of an AI agent to explore best practices and standard requirements focused on AI implementations

Focus Areas of S2G

	FY22	FY23	FY24
National Renewable Energy Laboratory (NREL)	• Support UL cybersecurity certification program • Support for IEEE 1547.3 cybersecurity guide • Support supply chain security related activities • Convene, coordinate, facilitate LCC meetings	• Support UL cybersecurity certification program • Co-lead IEEE 1547.3 cybersecurity guide	• Publish UL 2941 cybersecurity certification outline of investigation and support UL 2941 Technical Committee for consensus development. • Publish IEEE 1547.3 cybersecurity guide as vice-chair and support including cybersecurity recommendation to IEEE 1547-2025 standard requirements. • Develop test procedures for UL 2941 using single PV inverter and shared with UL • Incorporated industry and DOE feedback to DERMS cybersecurity paper
Pacific Northwest National Laboratory (PNNL)	• Support supply chain standards work for solar industry • Update distribution model to include Solar PV Resources • Perform Secure Design Cybersecurity Capability Maturity Model (SD2-C2M2) assessments.		• Convert IEEE-9500 and LV Network to ePHASORSIM model with Solar DER and post with other converted models on GitHub • Perform Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2) assessments • Develop Solar Power Resilience Maturity Model (Sol-ReMM) tool
Idaho National Laboratory (INL)	• Support the development of Solar Cert tool • Develop Solar CyberStrike training and tool.	DHS's CSET tool tuned to solar industry • Develop Solar CyberStrike training and tool. • Supply chain security and automated cyber analysis	• Develop focused industry engagement strategy to use across tasks • Pilot full CyberStrike STOMCLOUD training • Promote adoption of risk analysis toolsets • Build HBOM library for solar • Explore ML for codified attack surface and defense
Sandia National Laboratories (Sandia)	• Support DHS Cyber Security Evaluation Tool • Develop Solar CyberStrike training and tool.	• SunSpec/Sandia cyber security working group • System level orchestration and automated response for security operation center. • Vulnerability analysis	• Define best practice for PV inverter secure boot, PV inverter vulnerability disclosure process • Development of an AI agent to explore best practices and standard requirements focused on AI implementations

Standards Development and Best Practices

Education and Workforce Training

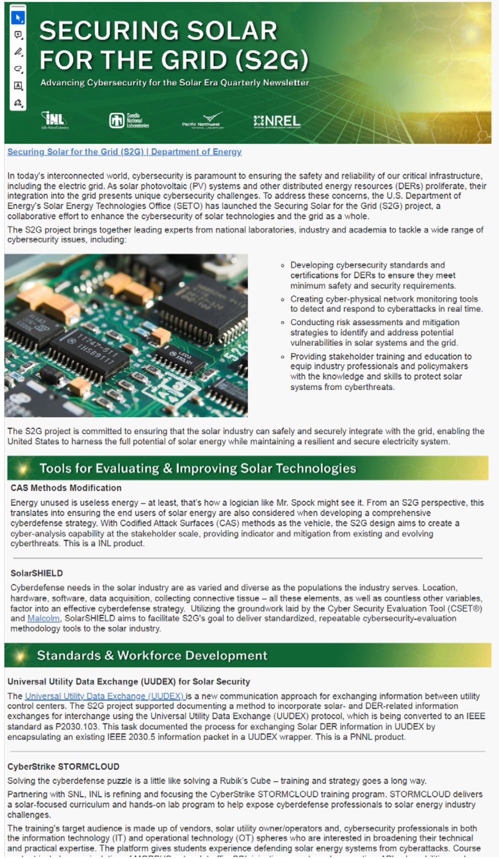
Cybersecurity Tool Kit and Supply Chain

Recent S2G Events

- IEEE 1547 meeting participation
- Engagement with NERC SITE’s and SPIDER working groups
- Energy Transitions Summit (2/5/24-2/8/24)
  - 2/5/24: CyberStrike STORMCLOUD workshop
  - 2/6/24: S2G Panel
  - 2/8/24: CyberStrike STORMCLOUD workshop
- 2024 IEEE Innovative Smart Grid Technologies North America (IGST NA) conference

LCC Updates

- New S2G quarterly newsletter
- Targeting training and partnership with industry organizations
- Update to the 2017 Roadmap for PV Cybersecurity
- Second IAB meeting will be held in-person at RE+
  - Anaheim, CA
  - Sept. 9-12, 2024)



SECURING SOLAR FOR THE GRID (S2G)

Advancing Cybersecurity for the Solar Era Quarterly Newsletter

Securing Solar for the Grid (S2G) | Department of Energy

In today's interconnected world, cybersecurity is paramount to ensuring the safety and reliability of our critical infrastructure, including the electric grid. As solar photovoltaic (PV) systems and other distributed energy resources (DERs) proliferate, their integration into the grid presents unique cybersecurity challenges. To address these concerns, the U.S. Department of Energy's Solar Energy Technologies Office (SETO) has launched the Securing Solar for the Grid (S2G) project, a collaborative effort to enhance the cybersecurity of solar technologies and the grid as a whole.

The S2G project brings together leading experts from national laboratories, industry and academia to tackle a wide range of cybersecurity issues, including:

- Developing cybersecurity standards and certifications for DERs to ensure they meet minimum safety and security requirements.
- Creating cyber-physical network monitoring tools to detect and respond to cyberattacks in real time.
- Conducting risk assessments and mitigation strategies to identify and address potential vulnerabilities in solar systems and the grid.
- Providing stakeholder training and education to equip industry professionals and policymakers with the knowledge and skills to protect solar systems from cyberthreats.

The S2G project is committed to ensuring that the solar industry can safely and securely integrate with the grid, enabling the United States to harness the full potential of solar energy while maintaining a resilient and secure electricity system.

Tools for Evaluating & Improving Solar Technologies

CAS Methods Modification

Energy unused is useless energy – at least, that's how a logician like Mr. Spock might see it. From an S2G perspective, this translates into ensuring the end users of solar energy are also considered when developing a comprehensive cyberdefense strategy. With Codified Attack Surfaces (CAS) methods as the vehicle, the S2G design aims to create a cyber-analysis capability at the stakeholder scale, providing indicator and mitigation from existing and evolving cyberthreats. This is a INL product.

SolarSHIELD

Cyberdefense needs in the solar industry are as varied and diverse as the populations the industry serves. Location, hardware, software, data acquisition, collecting connective tissue – all these elements, as well as countless other variables, factor into an effective cyberdefense strategy. Utilizing the groundwork laid by the Cyber Security Evaluation Tool (CSET®) and Malcolm, SolarSHIELD aims to facilitate S2G's goal to deliver standardized, repeatable cybersecurity-evaluation methodology tools to the solar industry.

Standards & Workforce Development

Universal Utility Data Exchange (UUDEX) for Solar Security

The Universal Utility Data Exchange (UUDEX) is a new communication approach for exchanging information between utility control centers. The S2G project supported documenting a method to incorporate solar- and DER-related information exchanges for interchange using the Universal Utility Data Exchange (UUDEX) protocol, which is being converted to an IEEE standard as P2030.103. This task documented the process for exchanging Solar DER information in UUDEX by encapsulating an existing IEEE 2030.5 information packet in a UUDEX wrapper. This is a PNNL product.

CyberStrike STORMCLOUD

Solving the cyberdefense puzzle is a little like solving a Rubik's Cube – training and strategy goes a long way.

Partnering with SNL, INL is refining and focusing the CyberStrike STORMCLOUD training program. STORMCLOUD delivers a solar-focused curriculum and hands-on lab program to help expose cyberdefense professionals to solar energy industry challenges.

The training's target audience is made up of vendors, solar utility owner/operators and, cybersecurity professionals in both the information technology (IT) and operational technology (OT) spheres who are interested in broadening their technical and practical expertise. The platform gives students experience defending solar energy systems from cyberattacks. Course

Funded by:

SOLAR ENERGY
TECHNOLOGIES OFFICE
U.S. Department Of Energy

Securing Solar for the Grid (S2G)

Idaho National Laboratory Updates

Presented on: March 14, 2024

Principal Investigator: Megan Culler

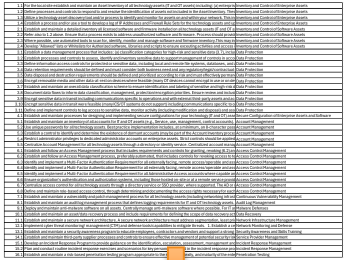
Other Contributors: Jake Gentle, Emma Stewart, Daniel Ricci, Rita Foster, Crash Bell

INL/MIS-24-77147

CyberSHIELD

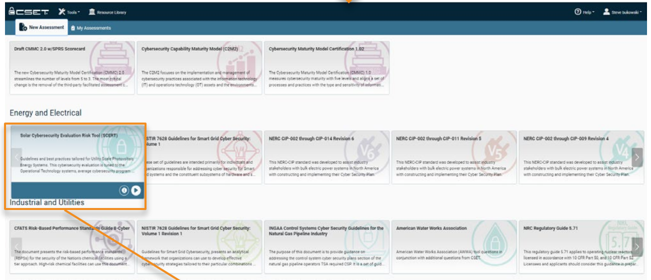
Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

- FY24 Plans:
  - Release updates to CSET and Malcolm
  - Provide documentation for industry engagement requirements
  - Identify deployment challenges and mitigations from industry engagements
  - Improve integration of Malcolm with CSET
- Accomplishments to date:
  - Tailored solar questions added to CSET
  - Solar architectures added to CSET
  - Common solar OT protocol parsing added to Malcolm
  - Malcolm Asset Interaction Analysis Guide released
    - https://cisagov.github.io/Malcolm/docs/asset-interaction-analysis.html
    - https://cset-renewables-download.inl.gov/
- Requests for industry engagement:
  - Interested in a SHIELD engagement? Reach out:
    - https://resilience.inl.gov/INLCYBERSHIELD
    - cybershield@inl.gov
    - Dan Ricci: Daniel.Ricci@inl.gov



1.1	For the local site establish and maintain an Asset Inventory of all technology assets (IT and OT assets) including: (a) enterpris	Inventory and Control of Enterprise Assets
1.2	Define processes and controls to respond to and resolve the identification of assets not included in the Asset Inventory. Thes	Inventory and Control of Enterprise Assets
1.3	Utilize a technology asset discovery tool and/or process to identify and monitor for assets on and within your network. This in	Inventory and Control of Enterprise Assets
1.4	Establish a process and/or use a tool to develop a log of IP Addresses and Firewall Rule Sets for the technology assets and up	Inventory and Control of Enterprise Assets
2.1	Establish and maintain a detailed inventory all licensed software and firmware installed on all technology assets (IT and OT a	Inventory and Control of Software Assets
2.2	Refer also to 1.2 above. Ensure that a process exists to address unauthorized software and firmware. Process should provid	Inventory and Control of Software Assets
2.3	Where possible, use automated tools to scan for, identify, monitor and manage software and firmware inventory.This may in	Inventory and Control of Software Assets
2.4	Develop "Allowed" lists or Whitelists for Authorized software, libraries and scripts to ensure exceuting activities and access i	Inventory and Control of Software Assets
3.1	Establish a data management process that includes: (a) classification categories for high-risk and sensitive data (3.7), inclu	Data Protection
3.2	Establish processes and controls to assess, identify and inventory sensitive data to support management of controls in acco	Data Protection
3.3	Define information access controls for protected or sensitive data, including local and remote file systems, databases, and a	Data Protection
3.4	Data retention requirements should be defined and must consider both business need and any regulatory/legal/contractual	Data Protection
3.5	Data disposal and destruction requirements should be defined and prioritized according to risk and must effectively perman	Data Protection
3.6	Encrypt removable media and other data-at-rest on devices where feasible (many OT devices cannot encrypt in use or on de	Data Protection
3.7	Establish and maintain an overall data classification scheme to ensure identification and labeling of sensitive and high-risk d	Data Protection
3.8	Document data flows to inform data classification, management, protection/encryption priorities. Ensure review and inclusi	Data Protection
3.9	Encrypt sensitive data in transit including communications specific to operations and with external third-party assets and ac	Data Protection
3.10	Encrypt sensitive data in transit were feasible (many ICS/OT systems do not support) including communications specific to o	Data Protection
3.11	Define and implement controls to log access to sensitive data, monitor activity (including modification and disposal) and ass	Data Protection
4.1	Establish and maintain processes for designing and implementing secure configurations for your technology (IT and OT) asse	Secure Configuration of Enterprise Assets and Software
5.1	Establish and maintain an inventory of all accounts for IT and OT assets (e.g., Service, use, management, control accounts).	Account Management
5.2	Use unique passwords for all technology assets. Best practice implementation includes, at a minimum, an 8-character pass	Account Management
5.3	Establish a control to identify and determine the existence of dormant accounts (may be part of the Account Inventory proces	Account Management
5.4	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Strict controls should be applied	Account Management
5.5	Centralize Account Management for all technology assets through a directory or identity service. Centralized account mana	Account Management
6.1	Establish and follow an Access Management process that includes requirements and controls for granting, revoking (6.2) an	Access Control Management
6.2	Establish and follow an Access Management process, preferably automated, that includes controls for revoking access to te	Access Control Management
6.3	Identify and implement a Multi-Factor Authentication Requirement for all externally facing, remote access/operable and ass	Access Control Management
6.4	Identify and implement a Multi-Factor Authentication Requirement for all externally facing, remote access/operable and ass	Access Control Management
6.5	Identify and implement a Multi-Factor Authentication Requirement for all Administrative Access accounts where capable an	Access Control Management
6.6	Ensure organization's authentication and authorization systems, including those hosted on-site or at a remote service provid	Access Control Management
6.7	Centralize access control for all technology assets through a directory service or SSO provider, where supported. The AD or	Access Control Management
6.8	Define and maintain role-based access control, through determining and documenting the access rights necessary for each	Access Control Management
7.1	Establish and maintain a vulnerability and patch management process for all technology assets (including networking infrast	Continuous Vulnerability Management
8.1	Establish and maintain an audit log management process that defines logging requirements for IT and OT technology assets.	Audit Log Management
9.1	Deploy and maintain anti-malware software on all assets. Centrally manage anti-malware software where possible. For IT ar	Malware Defenses
10.1	Establish and maintain an asset/data recovery process and include requirements for defining the scope of data recovery act	Data Recovery
11.1	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least priv	Network Infrastructure Management
12.1	Implement cyber threat monitoring/ management (CTM) and defense tools/capabilities to mitigate threats. 1. Establish a ce	Network Monitoring and Defense
13.1	Establish and maintain a security awareness program to educate employees, contractors and vendors and support a strong	Security Awareness and Skills Training
14.1	Establish and maintain third-party supplier processes and controls to ensure effective management of potential security risk	Service Provider Management
15.1	Develop an Incident Response Program to provide guidance on the identification, escalation, assessment, management and	Incident Response Management
15.2	Plan and conduct routine incident response exercises and scenarios for key person[illegible]d in the incident response pro	Incident Response Management
16.1	Establish and maintain a risk-based penetration testing program appropriate to the s[illegible]lexity, and maturity of the ente	Penetration Testing

Solar Questions



Draft CMMC 2.0 w/SPRS Scorecard
The new Cybersecurity Maturity Model Certification (CMMC) 2.0 streamlines the number of levels from 5 to 3. The most critical change is the removal of the third-party facilitated assessment c...

Cybersecurity Capability Maturity Model (C2M2)
The C2M2 focuses on the implementation and management of cybersecurity practices associated with the information technology (IT) and operations technology (OT) assets and the environments...

Cybersecurity Maturity Model Certification 1.02
The Cybersecurity Maturity Model Certification (CMMC) 1.0 measures cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of informati...

Energy and Electrical

Solar Cybersecurity Evaluation Risk Tool (SCERT)
Guidelines and best practices tailored for Utility Scale Photovoltaic Energy Systems. This cybersecurity evaluation is tuned to the Operational Technology systems, average cybersecurity program ...

STIR 7628 Guidelines for Smart Grid Cyber Security: lume 1
ese set of guidelines are intended primarily for individuals and anizations responsible for addressing cyber security for Smart d systems and the constituent subsystems of hardware and s...

NERC CIP-002 through CIP-014 Revision 6
This NERC-CIP standard was developed to assist industry stakeholders with bulk electric power systems in North America with constructing and implementing their Cyber Security Plan.

NERC CIP-002 through CIP-011 Revision 5
This NERC-CIP standard was developed to assist industry stakeholders with bulk electric power systems in North America with constructing and implementing their Cyber Security Plan.

NERC CIP-002 through CIP-009 Revision 4
This NERC-CIP standard was developed to assist industry stakeholders with bulk electric power systems in North America with constructing and implementing their Cyber Security Plan.

Industrial and Utilities

CFATS Risk-Based Performance Standards Guide 8-Cyber
The document presents the risk-based performance standards (RBPSs) for the security of the Nation's chemical facilities using a tier approach. High-risk chemical facilities can use this document ...

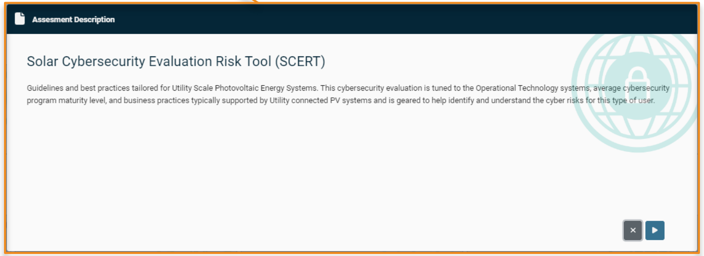
NISTIR 7628 Guidelines for Smart Grid Cyber Security: Volume 1 Revision 1
Guidelines for Smart Grid Cybersecurity, presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations ...

INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry
The purpose of this document is to provide guidance on addressing the control system cyber security plans section of the natural gas pipeline operators TSA required CSP. It is a set of guid...

American Water Works Association
American Water Works Association (AWWA) tool questions in conjunction with additional questions from CSET.

NRC Regulatory Guide 5.71
This regulatory guide 5.71 applies to operating nuclear reactors licensed in accordance with 10 CFR Part 50, and 10 CFR Part 52. Licensees and applicants should consider this guidance in prepar...

CSET Dashboard Featuring SCERT



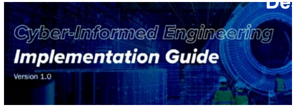
Assessment Description

Solar Cybersecurity Evaluation Risk Tool (SCERT)

Guidelines and best practices tailored for Utility Scale Photovoltaic Energy Systems. This cybersecurity evaluation is tuned to the Operational Technology systems, average cybersecurity program maturity level, and business practices typically supported by Utility connected PV systems and is geared to help identify and understand the cyber risks for this type of user.

CyberSHIELD Ecosystem

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

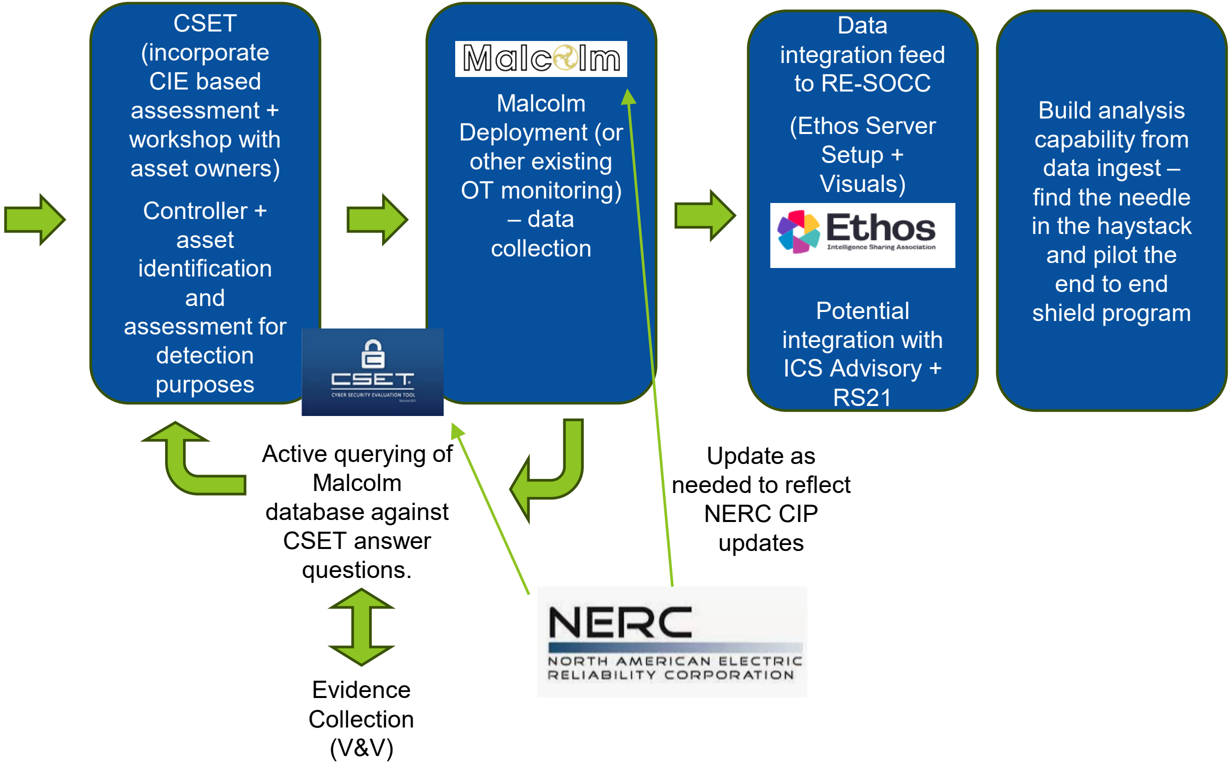


Cyber-Informed Engineering
Implementation Guide
Version 1.0

CIE Template for solar, spreadsheet, scoring… into the CSET platform.

CIE (CESER) Clean Energy Guide feeds into solar version:

- Leverage existing battery guide



CSET (incorporate CIE based assessment + workshop with asset owners)

Controller + asset identification and assessment for detection purposes

Malcolm

Malcolm Deployment (or other existing OT monitoring) – data collection

Data integration feed to RE-SOCC

(Ethos Server Setup + Visuals)

Ethos

Potential integration with ICS Advisory + RS21

Build analysis capability from data ingest – find the needle in the haystack and pilot the end to end shield program

Active querying of Malcolm database against CSET answer questions.

Evidence Collection (V&V)

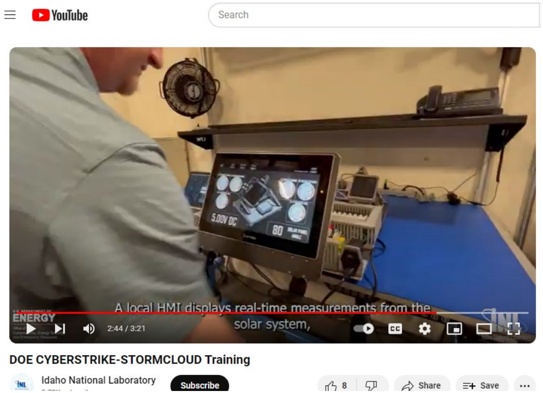
Update as needed to reflect NERC CIP updates

CSET
CYBER SECURITY EVALUATION TOOL
Ethos Intelligence Sharing Association
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CyberStrike STORMCLOUD

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

- FY24 Plans:
  - Manufacture 10 kits with updated hardware
  - Update curriculum with 2023 events
  - Prep for virtualization to make it more accessible
- Accomplishments to date:
  - 6 kits manufactured
  - CyberStrike STORMCLOUD promotional video released https://www.youtube.com/watch?v=4G2aTzz0zKg
  - All 8 lab exercises now tested by participants
- Upcoming training:
  - Full day tutorial at IEEE PES GM
  - Modules to be offered at RE+



A local HMI displays real-time measurements from the solar system,

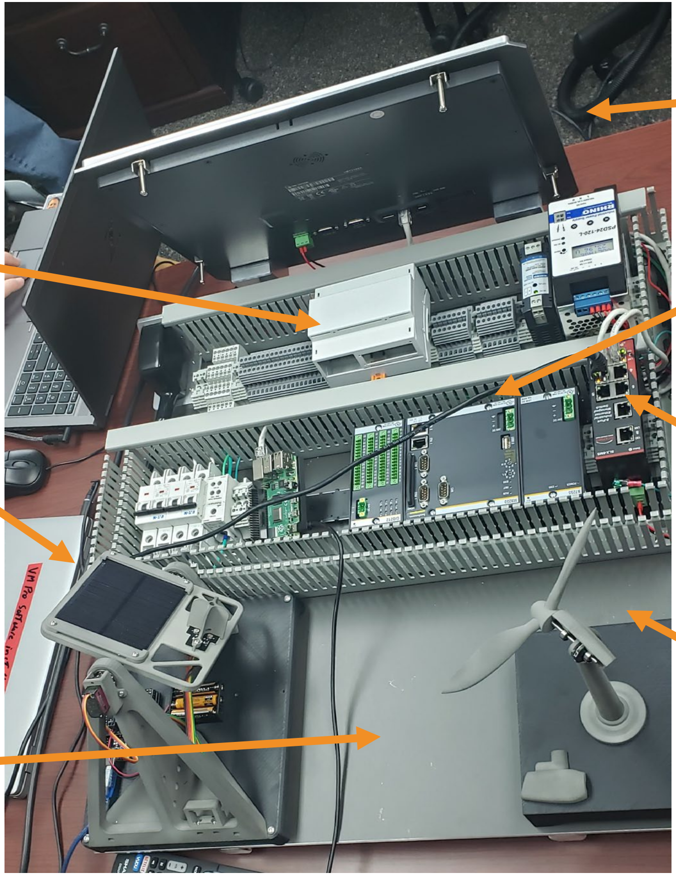
DOE CYBERSTRIKE-STORMCLOUD Training

Idaho National Laboratory

Subscribe

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

CyberStrike Storm Cloud Demo Kit



HMI

Solar "inverter" – Raspberry Pi emulator

Bachmann controller to be used for wind

Network switch for the DER system

Single-axis solar

Open platform design to allow wind turbine to blow

Space for EV model

Supply Chain Security

- FY24 Plans:
  - Prioritize inverters to investigate
  - Perform HBOM analysis of new inverters
  - Develop hardware catalog that can be cross-referenced with known vulnerabilities
- Accomplishments to date:
  - Hardware enumeration completed for 3 unique inverters
  - Vulnerabilities associated with hardware documented
  - Prioritization methodology developed

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Prioritization Methodology

- Question: What are the most important solar inverters to include in supply chain analysis?
- Challenges
  - No “gold source” list of key solar inverters
  - Cannot collect same data points for all inverters
  - Frequent additions and changes to company names/structures
- Identified criteria based on open-source information for vendors and several lists (allow lists and market research firms)
- Criteria used to weight each option
- Gaps
  - Allow lists target new standards, may exclude older models
  - Focus on 3-phase inverters
  - Market vs. market trends

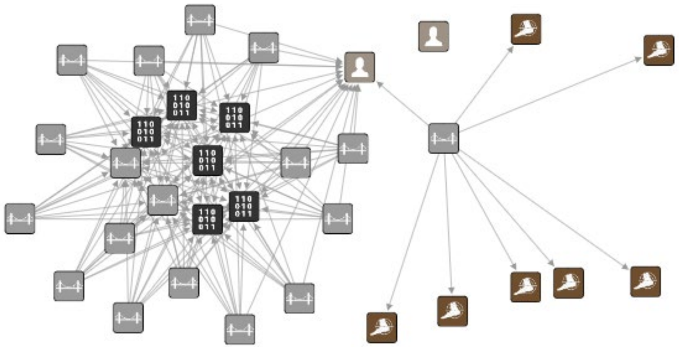
Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Codified Attack Surfaces (CAS)

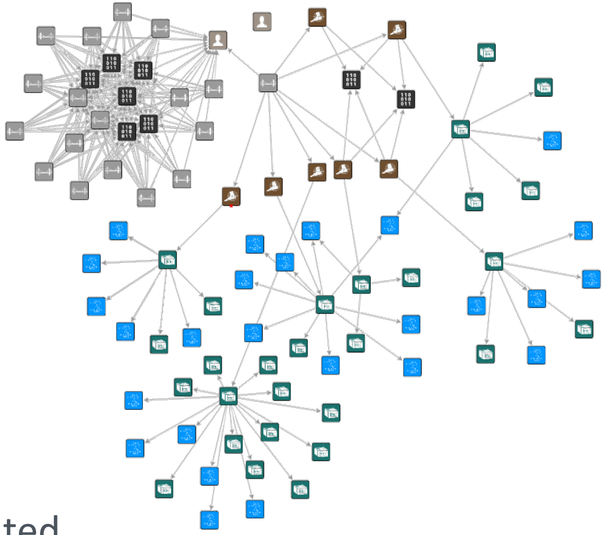
- FY24 Plans:
  - Create limited automated cyber analysis capability to provide indicator and mitigation from current and emerging cyber issues.
  - Apply CAS to solar installations **codified representative architectures** for residential, commercial/industrial and utility scale infrastructures.
    - Notional CAS used for larger cyber analysis centers, such as CESER ETAC
  - Use natural language processing to scrape web information to enrich intelligence and help build representative architectures
- Accomplishments to date:
  - CAS Method Modification
    - Codified attack surfaces for several solar test environments
    - Modeled threats, common weaknesses, and attack paths in STIX
  - Risk score for 16 inverters based on cyber threat observables
    - History of vulnerability processing (flaw remediation evidence)
    - Versions tied to vulnerabilities
    - Days to creation of updates

WAVgraph Enrichment for 1 Solar Inverter

Funded by:
SOLAR ENERGY
TECHNOLOGIES OFFICE
U.S. Department Of Energy



Most common weaknesses
Most used attack patterns



- WAVgraph enrichment adds new vulnerabilities and known exploited vulnerabilities from DHS CISA repository
- Updated STIX style Enforcer includes kill chain capabilities for 2 different kill chain techniques (Lockheed-Martin kill chain, SANS ICS kill chain)

Questions

- How important is supply chain security at your organization? What steps are being taken to address supply chain challenges?
- Would you be interested in a virtual version of the CyberStrike STORMCLOUD training?
- What barriers exist for the deployment of open-source tools at your organization?
- Are there challenges for cyber risk analysis at your organization?

INL PI Megan Culler: megan.culler@inl.gov

SOLAR ENERGY
TECHNOLOGIES OFFICE
U.S. Department Of Energy

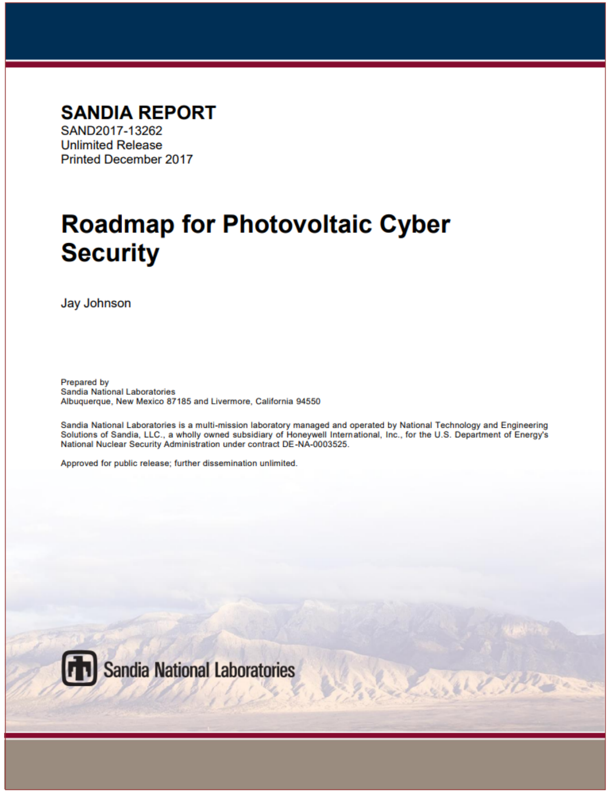
Roadmap for Solar Cybersecurity

IAB Workshop

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

Roadmap for Solar PV Cybersecurity

- What?
  - New version of the Roadmap for PV Cybersecurity
  - Near-term, mid-term, and long-term milestones for key cybersecurity focus areas
- Why?
  - 2017 version only looked 5 years out
  - Strategy for SETO, targets for labs and industry
- How?
  - Lab contributions and industry feedback



SANDIA REPORT
SAND2017-13262
Unlimited Release
Printed December 2017

Roadmap for Photovoltaic Cyber Security

Jay Johnson

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

Sandia National Laboratories is a multi-mission 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-NA-0003525.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Funded by:
SOLAR ENERGY
TECHNOLOGIES OFFICE
U.S. Department Of Energy

Roadmap for Solar PV Cybersecurity

Contents

- Executive Summary
- National Energy Cybersecurity Efforts
- Solar Energy Technology Landscape
- Solar Cyber Threat Landscape
- Solar Cybersecurity R&D
- Standards Development
- Best Practices
- Stakeholder Roles & Industry Targets

Vision and Milestones

Broader Context

Technology Background

Motivation & Trends

What can labs do?

How to adopt?

How to implement?

Who’s responsible?

Funded by:
SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

A Look Ahead – Where will S2G be?

- March 26-28 SETO Peer Review
- April 16-28 ESTIG Spring O&M User Group Balance of Plant Roundtable
- May 15-16 SEIA Clean Energy Security and Reliability Forum (in partnership with RE+ Texas)
- July 21 IEEE PES GM: Full day CyberStrike STORMCLOUD tutorial
- Sept. 9-12 RE+: S2G IAB Fall In-Person meeting
- Supply chain webinar coming soon

Closeout

- Additional comments or questions?