

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express 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. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.



**SOLAR ENERGY
TECHNOLOGIES OFFICE**
U.S. Department Of Energy

Securing Solar for the Grid (S2G)

National Renewable Energy Laboratory

Award # 38445

Final Project Report

Period of Performance: October 2021 – September 2024

Principal Investigator: Danish Saleem

Team Members: Ryan Cryar, Zoe Dormuth, Jennifer Guerra, Jordan Peterson, Chelsea Neely, Emily Waligoske

DOE/GO-102025-6677

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

Strengthen and standardize cybersecurity approaches for electric grids with high penetrations of solar PV and other DERs

APPROACH

Collaboration among 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

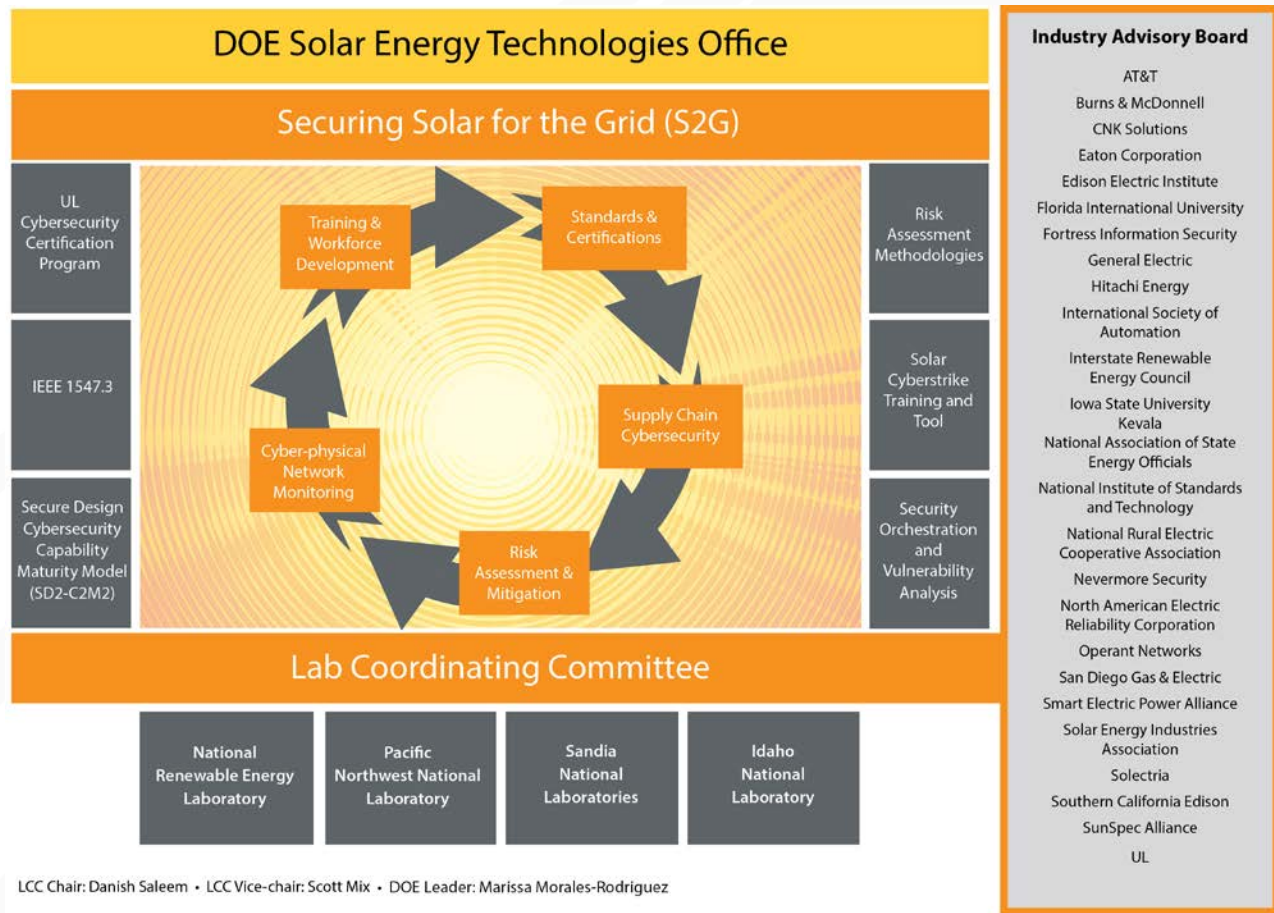
Development and dissemination of **standards' requirements, best practices, equipment testing procedures, assessment tools, as well as education and training materials** for cyber defense, posture and maturity tailored to solar technologies.



Overview of NREL's Contribution

Outcome

Through S2G, NREL supported the development of standards & certification, help improved DER supply chain cybersecurity, and developed cybersecurity risk profiles to understand benefits or implications for leveraging distributed energy resource management systems (DERMS) in centralized utility DERMS deployments or decentralized aggregator DERMS



Key Milestones for NREL

Cybersecurity Certification Standard

Lead the development of a cyber certification standard for solar PV industry

Develop test guidance to support UL 2941 certification standard

Support consensus development for UL 2941 among OEMs, utilities, installers, and aggregators

Cybersecurity Guide for DERs

Develop a guide with recommendations for cybersecurity of DERs i.e., IEEE 1547.3

Integrate cybersecurity recommendations into IEEE 1547 standard

Solar PV Supply Chain Cybersecurity

Analyze and document the gaps in the supply chain cybersecurity for DERs

Publish cybersecurity recommendations for solar PV industry

Lead a solar supply chain cybersecurity workshop

Cybersecurity Guide for DERs

Identify applicable cybersecurity standards and/or guidelines for DERMS

Identify cybersecurity considerations for DERMS

Develop cybersecurity risk profiles for DERMS

Impact of NREL's Work Through S2G



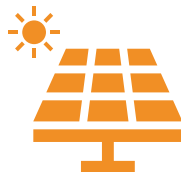
Led S2G proposal in
FY 2018

Led the laboratory
coordination
committee (LCC) as
chair in FY22 and
FY23, and as vice
chair in FY24



Co-led the
development of UL
2941 OOI for solar
cybersecurity
certification standard

Co-led the
development IEEE
1547.3 cybersecurity
guide for DERs



Conducted gap
analysis for DER
supply chain
cybersecurity

Compiled supply
chain cybersecurity
recommendations

Defined DERMS
cybersecurity risk
profiles



Coordination of
cybersecurity
requirements from
key industry
stakeholders

Developed testing
guidance for cyber
certification of PV
inverters



Led development of
LCC structure such as
charter, graphic,
information page,
invitation emails, etc.

Co-hosted LCC
meetings, recruited
members, and much
more

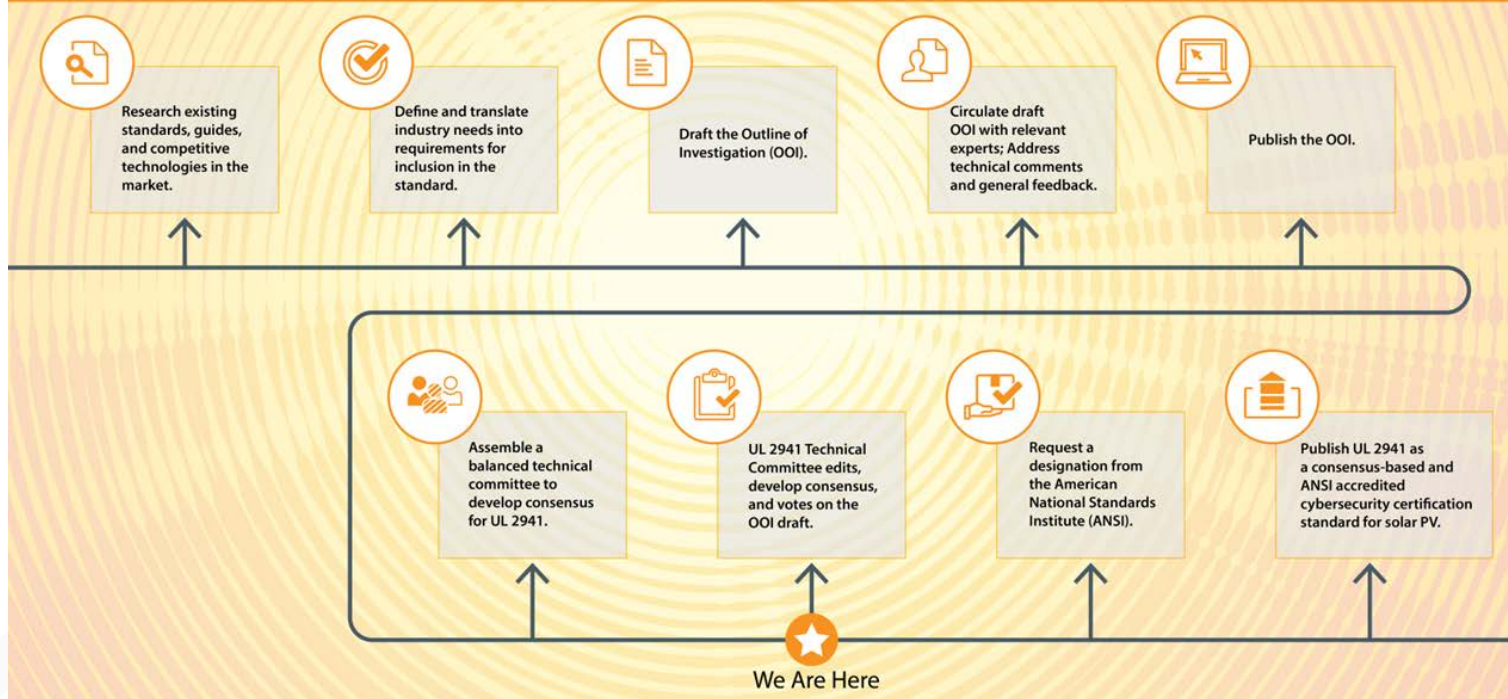


Developed impactful
reports and research
papers to pave the
way for new
cybersecurity
standards,
certifications, tools,
and recommended
practices for DERs

The project supported a **first of its kind cybersecurity certification standard** that can be used to validate cybersecurity posture of solar PV inverters before deployment and while in the field.

UL 2941: Cybersecurity Certification Standard

Underwriter Laboratories 2941: Where are we in the process?



IEEE 1547.3: Cybersecurity Guide for DERs

P1547 Revision Working Group: Expectations of SG Leads & Facilitator

Proposed Focus of this Revision

Integrate 2020 amendment

Fixes from 1547 adoption

Fixes from UL 1741 SB
revisions

Promote selected P1547.9
guidance to requirements

Fixes for V2G
commissioning procedures
(as it pertains to the base
1547 standard and not
1547.1)

Promote selected IEEE
1547.3 cybersecurity
recommendations to
IEEE 1547 standard
requirements

Add recommended DER
settings file format based
on EPRI working group
recommendations

Remove barriers for GFM
identified by UNIFI et al.

- IEEE 1547.3 cybersecurity guide published in December 2023 after being approved by the working group and standards coordination committee.
- It was added to the IEEE 1547 standard revision timeline.

IEEE Std 1547.3™-2023
(Revision of IEEE Std 1547.3-2007)

IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems

Developed by the
Distributed Generation, Energy Storage, and Interoperability Standards Committee
and the
Power System Communications and Cybersecurity Committee
of the
IEEE Board of Governors
and the
IEEE Power and Energy Society

Approved 5 June 2023

IEEE SA Standards Board

Publications



Certification Procedures for Data and Communications Security of Distributed Energy Resources

Danish Saleem¹ and Cedric Carter²

¹ National Renewable Energy Laboratory
² The MITRE Corporation



Supply Chain Cybersecurity Recommendations for Solar Photovoltaics

Ryan Cryar, Vikash Rivers, Jennifer Guerra, Chelsea Quilling, Zoe Dormuth, and Danish Saleem

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-AC36-06OR22308

Technical Report
NREL/TP-690+67115
August 2013



Cybersecurity Recommendations for Distributed Energy Resource Management Systems

Chelsea Quilling, Ryan Cryar, Danish Saleem, and Jennifer Guerra

National Renewable Energy Laboratory



Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources

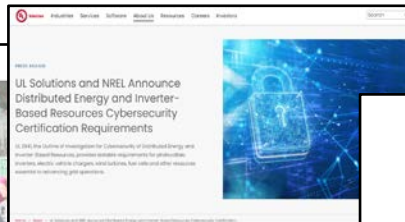
Ryan Cryar, Danish Saleem, Jordan Peterson, and William Hupp

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-AC36-06OR22308

Technical Report
NREL/TP-690+67115
February 2013



IEEE Solutions and NREL Announce Distributed Energy and Inverter-Based Resources Cybersecurity Certification Requirements

On 2013, the Office of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources (OICDER) announced requirements for distributed energy resources (DERs) to achieve cybersecurity certification for their DERs.

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE SA Standards Board

IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems

Developed by the
Distributed Generation, Energy Storage, and Interoperability Standards Committee
and the
Power System Communications and Cybersecurity Committee
of the
IEEE Board of Governors
and the
IEEE Power and Energy Society

Approved 5 June 2013

IEEE SA Standards Board

SANDIA REPORT
SAND2012-1116
Printed January 2012

Distributed Energy Resource Cybersecurity Standards Development – Final Project Report

Jay Johnson, Neoma Onunkwe, Danish Saleem, William Hupp, Jordan Peterson, Ryan Cryar



Cybersecurity in Photovoltaic Plant Operations

Andy Walker,¹ Jal Desai,¹ Danish Saleem,¹ and Thrushara Gunda²

¹ National Renewable Energy Laboratory
² Sandia National Laboratories

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-AC36-06OR22308

Technical Report
NREL/TP-690+67115
March 2011



Cyber Security for Distributed Energy Resources and DER Aggregators

NERC Cyber Integration and Technology Enablement Subcommittee (CITES) White Paper
December 2012

Purpose
This report provides industry with information regarding activities underway to further secure the electricity system under rapid transformation, specifically in the area of cyber security efforts for distributed energy resources (DERs) and DER aggregators. NERC is working with industry stakeholders to address cyber security concerns for DERs as the penetration of these resources continues to grow in many areas across North America. This paper is informational and seeks to help provide clarity and guidance to industry stakeholders in the area.

Defining DER and DER Aggregator
The NERC Cyber Planning project from the Working Group (CITES) defines a DER as "any source of electric power located on the distribution system." This definition specifically focuses on these resources in the distribution system that can produce electric power, i.e., a generating resource, and does not include end-use loads or demand response as part of the DER definition. Conversely, the Federal Energy Regulatory Commission (FERC) DER definition excludes the FERC CITE 2237 from consideration, including demand response, energy efficiency, and demand response. The expanded NERC definition includes all DER types able to participate in regional organized wholesale electricity markets through aggregation (DER aggregators).

This document will generally refer to DERs with the NERC definition while acknowledging that DER aggregators may include DERs (with the FERC definition) that are load resources and not generating elements where used. This language does not critically impact the key points being made in this paper.

Understanding Security of the Electricity Ecosystem
The full power system (EPS) includes any interconnected power plants with power flowing across the transmission system, down through the distribution networks, and then to end-use consumers. A significant portion of this system is operated either with analog controls or with digital control systems. However, the power system of today is undergoing a rapid transformation, the generation base is moving towards clean energy resources interconnected through power lines. Large synchronous generation sites are being retired and replaced with smaller wind and solar resources, battery energy storage, and hybrid power plants. DERs connected resources are also being added with DERs that connect to the distribution system, some of which are behind-the-meter and owned and operated by end-use consumers or third parties. Many of these systems are now connected directly to the internet, digitalization, and the associated connectivity concern to expand exponentially. Grid planners, designers, and operators are faced with managing a grid with a significant portion of the resource base connected to the internet.



Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources

William Hupp, Danish Saleem, and Jordan T. Peterson
National Renewable Energy Laboratory

Kenneth Boyce
Underwriters Laboratories

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-AC36-06OR22308

Technical Report
NREL/TP-690+67115
November 2012

Industry Engagement: Publications

- Cybersecurity Guidance for DERMS ([Link to be added](#))
- UL 2941 Testing Guidance ([Link to be added](#))
- S2G Final Report ([Link to be added](#))
- Privacy and Security Impacts of DER and DER Aggregators
 - https://www.nerc.com/comm/RSTC_Reliability_Guidelines/JointWhitePaper_PrivacyAndSecurityImpactsOfDERAggregators.pdf
- Supply Chain Cybersecurity Recommendations For Solar Photovoltaics
 - <https://www.nrel.gov/docs/fy23osti/87135.pdf>
- Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources
 - <https://www.nrel.gov/docs/fy23osti/84752.pdf>
- Design of Distributed Energy Resource Cybersecurity Certification Programs
 - https://www.researchgate.net/publication/371904823_Design_of_Distributed_Energy_Resource_Cybersecurity_Certification_Programs
- Cyber Security for Distributed Energy Resources and DER Aggregators
 - https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf
- Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter-Based Resources
 - <https://www.nrel.gov/docs/fy22osti/80581.pdf>
- Distributed Energy Resource Cybersecurity Standards Development
 - <https://www.osti.gov/servlets/purl/1843109/>
- A Multidimensional Holistic Framework for the Security of Distributed Energy and Control Systems (*not S2G funded*)
 - <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8755282>
- Cybersecurity in Photovoltaic Plant Operations
 - <https://www.nrel.gov/docs/fy21osti/78755.pdf>
- Certification Procedures for Data and Communications Security of Distributed Energy Resources
 - <https://www.nrel.gov/docs/fy19osti/73628.pdf>
- Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources
 - <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8972000>

Industry Engagement: Presentations

- Standards and Certification Panel at S2G annual workshop at hosted by RE+ in Anaheim (9/12/2024)
- Supply chain cybersecurity workshop, hosted by NREL (8/01/2024)
- S2G Panel at IEEE PES GM, hosted by IEEE in Seattle (7/24/2024)
- Cybersecurity training for FERC hosted virtually by FERC (04/25/2024)
- SETO peer review 2024 _hosted by DOE SETO in Washington DC (03/27/2024)
- S2G Industry Advisory Board Meeting hosted virtually by NREL and INL (03/14/2024)
- RE+ 2023 Securing Solar for the Grid (S2G) Workshop in Las Vegas (09/14/2023)
- IEEE PES General Meeting _hosted by IEEE PES in Orlando (07/19/2023)
- IEEE 1547 Interoperability and Cybersecurity Working Group presentation delivered by NREL (05/31/2023)
- NERC RSTC meeting in Clearwater, Florida (03/24/2023)
- FY2023 Industry Advisory Board Meeting _hosted by NREL (02/27/2023)
- NERC DER workshop _hosted virtually by NERC and the SPIDERWG (12/14/2022)
- Wind Cybersecurity Workshop _hosted by NREL in Washington DC (09/27/2022)
- Re+ (Previously SPI) _Panel session with UL (09/22/2022)
- Cybersecurity training for state commissioners _hosted by NARUC (09/08/2022)
- Security Integration and Technology Enablement committee _hosted by NERC (08/10/2022)
- King Abdullah City for Atomic and Renewable Energy _Delegation from Saudi Arabia (07/25/2022)
- Securing Solar for the Grid Workshop _hosted by NREL (07/20/2022)
- Cybersecurity and Technology Innovation Conference _hosted by DOE CIO (06/15/2022)
- Cybersecurity Advisory Team for State Solar (CATSS) _hosted by NASEO (01/24/2022)

Past Workshops/Meetings

July 2022



September 2024



September 2023