SOLAR ENERGY
TECHNOLOGIES OFFICE
U.S. Department Of Energy

NREL
Transforming ENERGY

Cybersecurity of DER Systems

Cybersecurity Training for State Commissions

Jeremiah Miller - jeremiah.miller@ee.doe.gov

Danish Saleem - danish.saleem@nrel.gov

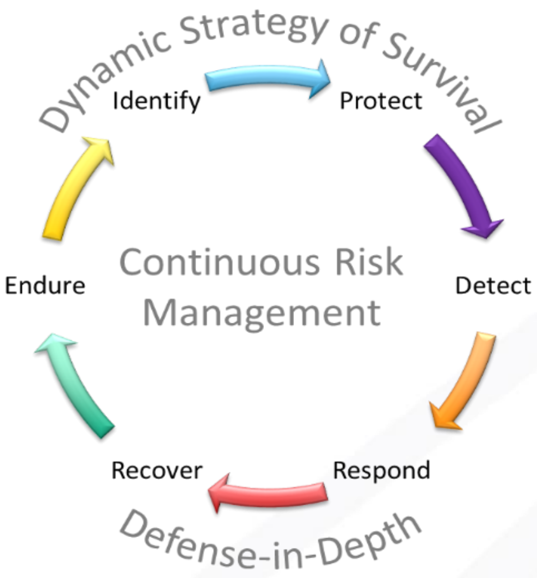
Disclaimer

- The presentation and associated discussion are our personal thoughts and ideas.

- These views are not represented as those of the U.S. Government, the Department of Energy, the Solar Energy Technologies Office, or the National Renewable Energy Laboratory.

Essential DER and Cybersecurity Terms

NIST's Cybersecurity Framework



https://www.nist.gov/programs-projects/cybersecurity-framework
https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

* Note: "Endure" is additive to reflect resiliency needs.
Adapted from Jovana Helms at LLNL

Distributed Energy Resources (DERs) - Controllable electric generation, storage, or load devices that are interconnected to the electric grid and typically are behind a customer's meter. DERs are intelligent energy devices, from smart lighting and thermostats, to electric vehicles and rooftop solar photovoltaics.

Internet of Things (IoT) devices vs DERs - DERs are subject to performance requirements of the Institute of Electrical and Electronics Engineers, the IEEE 1547-2018 standard, and each DER is certified for conformity to interconnect with the grid. Smaller devices, especially adjustable home or business loads and smart phone-enabled home automation devices, are IoT devices. Harmonizing IoT and DER performance requirements, including cyber, is a challenge.

DER Aggregator - An entity that groups together DER resources for the purposes of operating it as a group for grid services.

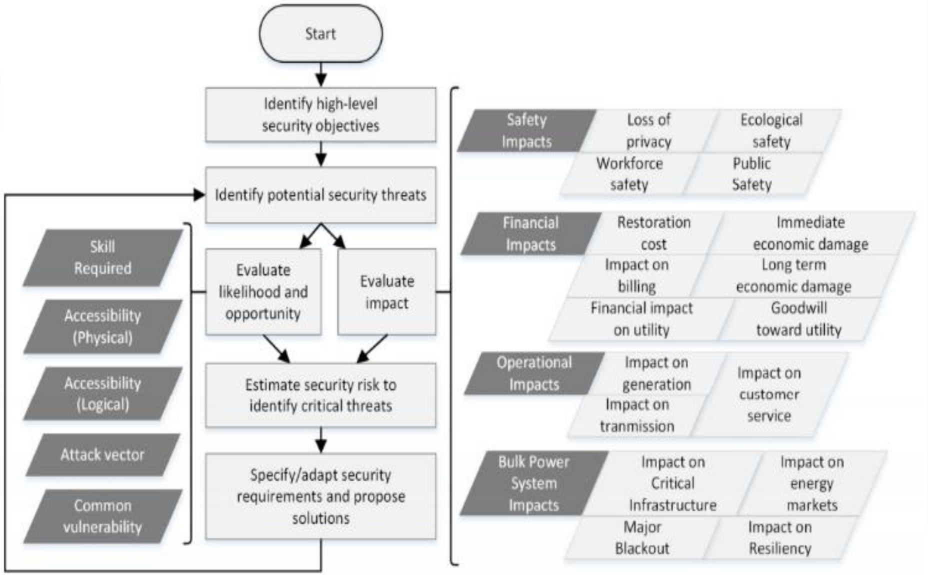
DER Owner/Operators – The entity (or entities) that is responsible for the regular care and maintenance of a particular DER resource or group of resources.

DER Vendor – The entity that originally built the DER resource, or components of the DER resource.

Essential DER and Cybersecurity Terms

Likelihood and Opportunity: Assessment of the “hack value” notion among hackers that something is worth doing.
Vulnerability: Existence of a weakness, design, or implementation error that can lead to an attacker gaining access.
Zero-day attack: An attack that exploits vulnerabilities before the vendor releases a patch for that vulnerability.
DER Ransomware: An attack that takes control of a DER and encrypts its operational software until a ransom is paid. While a financial frustration to the DER owner, a ransomware attack on a single DER is not likely to be noticed by a grid operator.
DER Botnet: An attack infecting enough DER, controlled by the attacker, that enables grid instability at a larger scale than previously possible.
DER Worm: DER attack on a single DER that could propagate to higher level systems belonging to a grid operator or aggregator or laterally to other DER systems.

Cyber Risk Assessment



Start

Identify high-level security objectives

Identify potential security threats

Evaluate likelihood and opportunity

Evaluate impact

Estimate security risk to identify critical threats

Specify/adapt security requirements and propose solutions

Skill Required

Accessibility (Physical)

Accessibility (Logical)

Attack vector

Common vulnerability

Safety Impacts: Loss of privacy; Ecological safety; Workforce safety; Public Safety

Financial Impacts: Restoration cost; Immediate economic damage; Impact on billing; Long term economic damage; Financial impact on utility; Goodwill toward utility

Operational Impacts: Impact on generation; Impact on tranmission; Impact on customer service

Bulk Power System Impacts: Impact on Critical Infrastructure; Impact on energy markets; Major Blackout; Impact on Resiliency

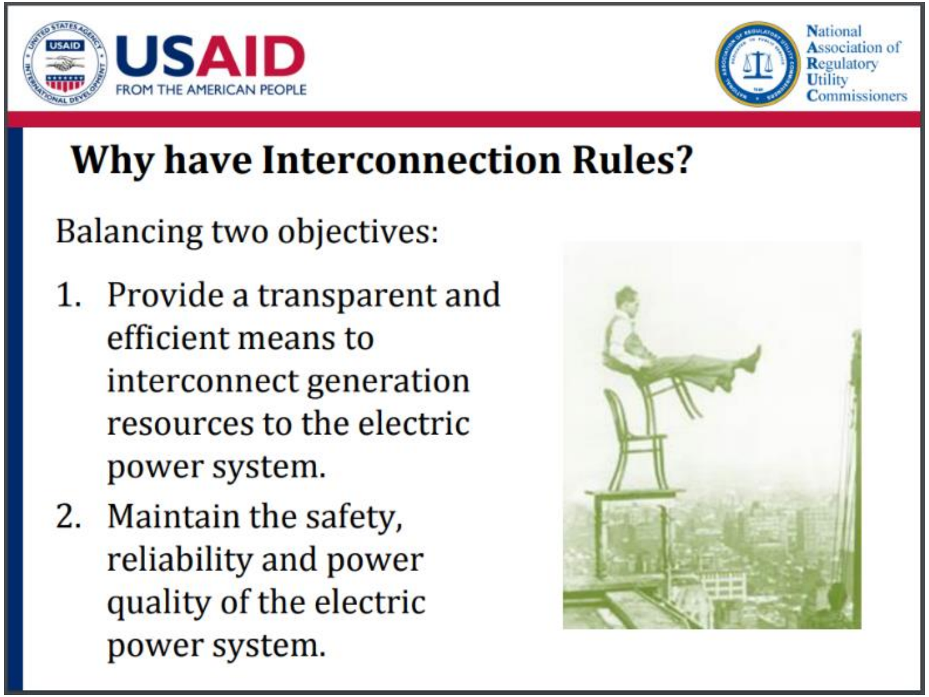
NREL (2019) Risk Assessment at the Edge: Applying NERC CIP to Aggregated Grid-Edge Resources
https://doi.org/10.1016/j.tej.2019.01.018

But Solar is 3% of Today's Electricity Generation

- **Should Solar/DER care about cyber *now*?**
- **Should State Utility Commissions care about DER cyber *now*?**

- An Example: An order of magnitude comparison
- Western Interconnection Grid (i.e. west of the Rockies)
- Loss of Palo Verde 2,000 MW: Largest contingency event
- Rooftop/small solar in the West: ~30,000 MW
  - This represents about 65% of all solar in the West, none of which is required to follow NERC CIP
  - And there is no widely recognized alternative cyber compliance standard for rooftop solar/DER

What links solar and cyber? *Interconnection*



USAID
FROM THE AMERICAN PEOPLE

National Association of Regulatory Utility Commissioners

Why have Interconnection Rules?

Balancing two objectives:

1. Provide a transparent and efficient means to interconnect generation resources to the electric power system.
2. Maintain the safety, reliability and power quality of the electric power system.

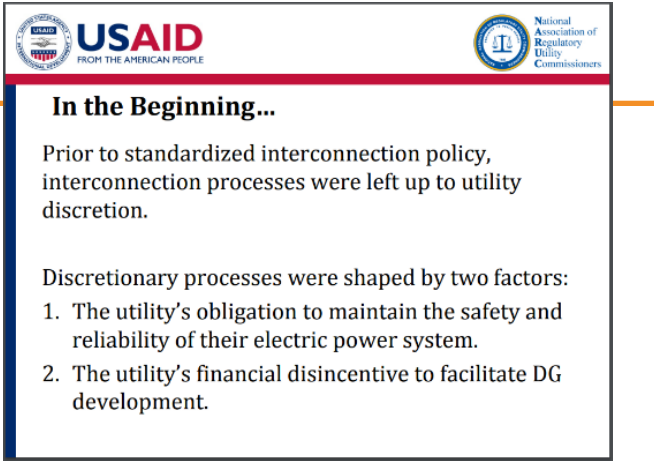
https://pubs.naruc.org/pub.cfm?id=5375FAA8-2354-D714-51DB-01C5769A4007

- Interconnection standards
- Maintain safety, reliability, power quality, and *security*
- IEEE 1547 was just revised for grid support capabilities from DER: e.g., voltage ride-through
- But there are no “shall have” cybersecurity requirements
- IEEE 1547.3 is a draft guideline with “may have” cyber requirements

Utility Commission Role?

- In general, utility commissions work to assure that utilities provide reasonable, adequate and efficient service at just and reasonable prices
- Utility regulation takes many forms, including price regulation, resource planning and acquisition, reliability and quality of service regulation
- Rooftop solar and DERs are starting to provide grid services
- What cyber issues would you consider during interconnection?

https://pubs.naruc.org/pub.cfm?id=5375FAA8-2354-D714-51DB-01C5769A4007



USAID FROM THE AMERICAN PEOPLE

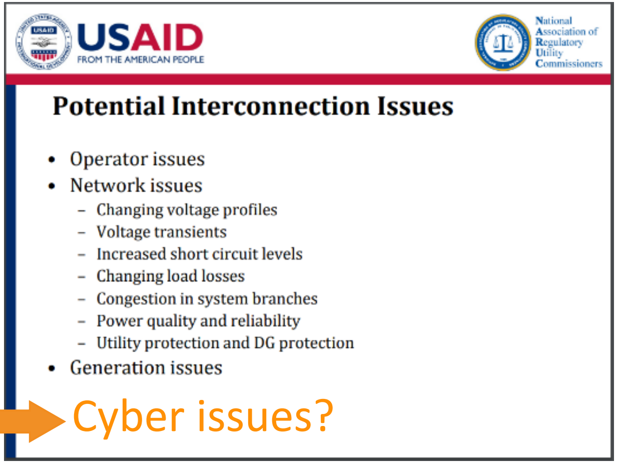
National Association of Regulatory Utility Commissioners

In the Beginning…

Prior to standardized interconnection policy, interconnection processes were left up to utility discretion.

Discretionary processes were shaped by two factors:

1. The utility's obligation to maintain the safety and reliability of their electric power system.
2. The utility's financial disincentive to facilitate DG development.



USAID FROM THE AMERICAN PEOPLE

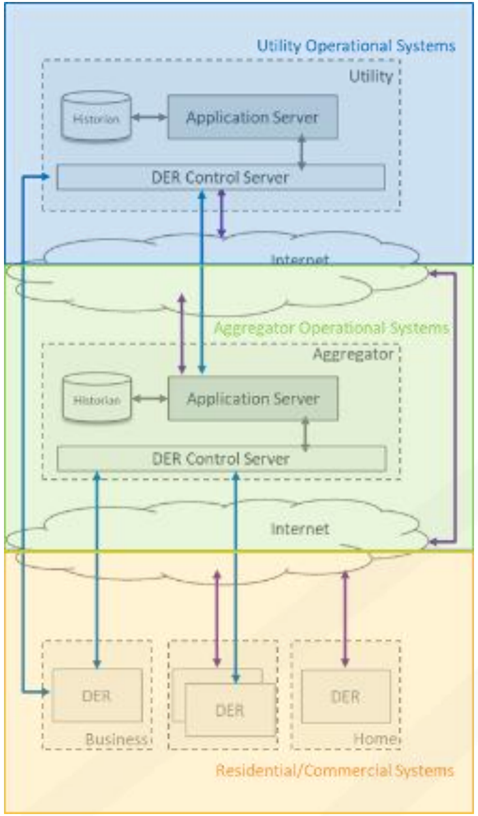
National Association of Regulatory Utility Commissioners

Potential Interconnection Issues

- Operator issues
- Network issues
  - Changing voltage profiles
  - Voltage transients
  - Increased short circuit levels
  - Changing load losses
  - Congestion in system branches
  - Power quality and reliability
  - Utility protection and DG protection
- Generation issues

Cyber issues?

Understanding DER Systems Roles is Critical



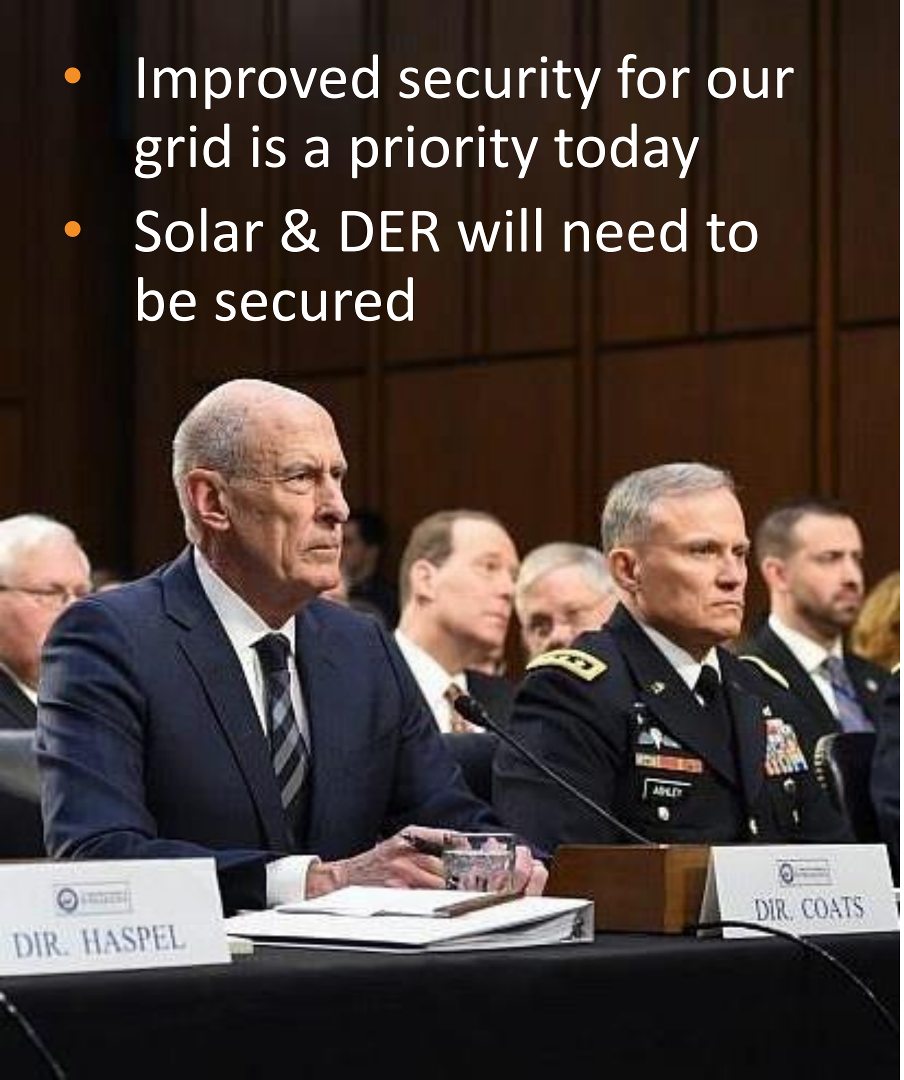
- **Utility Systems** need operational data from devices they do not own and operate

- **DER Aggregators** are becoming 3rd party grid services providers, sending control requests to DERs

- **Customers** are not skilled at securing their DER devices

SOLAR ENERGY TECHNOLOGIES OFFICE
U.S. Department Of Energy

- Improved security for our grid is a priority today
- Solar & DER will need to be secured



"Our adversaries and strategic competitors will increasingly use cyber capabilities to seek political, economic, and military advantage over the United States and its allies and partners."

*"**China has the ability** to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure in the United States."*

*"**Russia has the ability** to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure…. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage."*

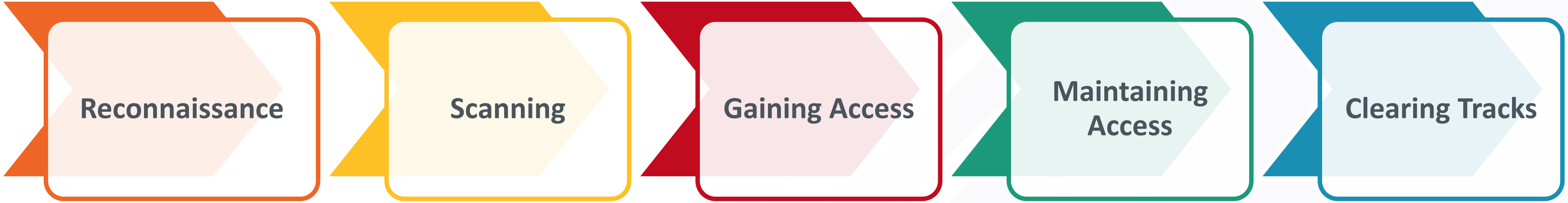
Daniel R. Coats, Former Director of National Intelligence Testimony to Senate Select Committee on Intelligence, January 29th 2019

https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Relevant Big Trends in the Industry

- Speed and scale of grid transformation in the era of solar/wind/storage/EVs/inverter-based resources
- Converging information technology and operational technology (IT/OT)
- Insider threat represents a majority of OT attacks
- Accelerated use of cloud-based systems
- DERs are growing fast; DER Aggregators are new grid services operators
- Recent cyber attacks demonstrated how they can be used to cripple operations by causing outages, financial damage, potential injuries, and even environmental disasters
- Early autonomous grid pilots demonstrate cyber-physical convergence
- Need for cradle-to-grave secure supply chain
- Artificial intelligence and big data analysis becoming crucial to monitor operations and recognize threats

Phases of a Successful Cyberattack



Reconnaissance

Scanning

Gaining Access

Maintaining Access

Clearing Tracks

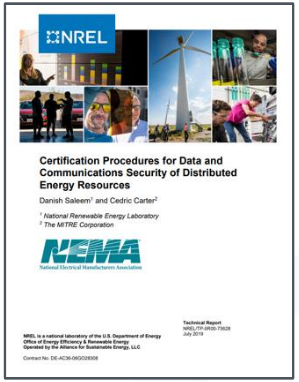
<u>Example: Ukraine Power Grid Cyber-Attack</u>

- Started with a spear-phishing campaign to deliver “BlackEnergy3” malware through malicious email to Ukrainian electricity distribution company
- Conducted extensive reconnaissance and scanning over several months
- Gained access to Windows Domain Controllers to steal credentials
- Launched attack by sending simultaneous trip commands to multiple circuit breakers
- Disabled backup power supplies while trying to maintain access for as long as they could
- Launched denial-of-service attack against customer call centers to prevent customers from calling in to report the outage.

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

Outcomes of Cybersecurity Standards Initiatives

Provides test cases that can be used to check, verify and validate cybersecurity posture of DERs.



NREL

Certification Procedures for Data and Communications Security of Distributed Energy Resources

Danish Saleem[1] and Cedric Carter[2]

[1] *National Renewable Energy Laboratory*
[2] *The MITRE Corporation*

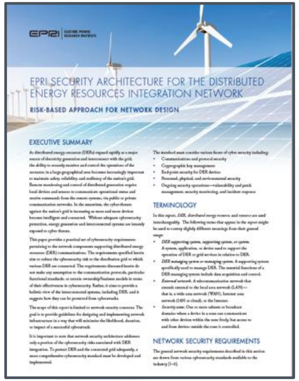
NEMA
National Electrical Manufacturers Association

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

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-73628
July 2019

Provides practical cybersecurity requirements pertaining to the network components supporting DERs.



EPRI | ELECTRIC POWER RESEARCH INSTITUTE

EPRI SECURITY ARCHITECTURE FOR THE DISTRIBUTED ENERGY RESOURCES INTEGRATION NETWORK

RISK-BASED APPROACH FOR NETWORK DESIGN

EXECUTIVE SUMMARY

As distributed energy resources (DERs) expand rapidly as a major source of electricity generation and interconnect with the grid, the ability to securely monitor and control the operations of the resources in a large geographical area becomes increasingly important to maintain safety, reliability, and resiliency of the nation's grid. Remote monitoring and control of distributed generation require local devices and sensors to communicate operational status and receive commands from the remote systems, via public or private communication networks. In the meantime, the cyber-threats against the nation's grid is increasing as more and more devices become intelligent and connected. Without adequate cybersecurity protection, energy generation and interconnected systems are intensely exposed to cyber threats.

This paper provides a practical set of cybersecurity requirements pertaining to the network components supporting distributed energy resources (DER) communications. The requirements specified herein aim to reduce the cybersecurity risk to the distribution grid to which various DER are connected. The requirements discussed herein do not make any assumption to the communication protocols, particular functional standards, or certain ownership/business models in terms of their effectiveness in cybersecurity. Rather, it aims to provide a holistic view of the interconnected systems, including DER, and it suggests how they can be protected from cyberattacks.

The scope of this report is limited to network security concerns. The goal is to provide guidelines for designing and implementing network infrastructure in a way that will minimize the likelihood, duration, or impact of a successful cyberattack.

It is important to note that network security architecture addresses only a portion of the cybersecurity risks associated with DER integration. To protect DER and the connected grid adequately, a more comprehensive cybersecurity standard must be developed and implemented.

The standard must consider various facets of cyber security including:

- Communications and protocol security
- Cryptographic key management
- End-point security for DER devices
- Personnel, physical, and environmental security
- Ongoing security operations—vulnerability and patch management, security monitoring, and incident response

TERMINOLOGY

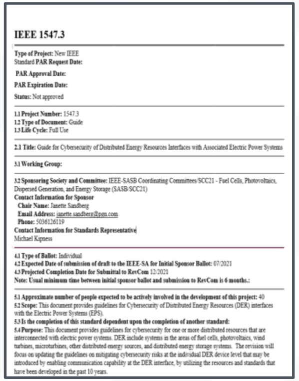
In this report, *DER, distributed energy resource,* and *resource* are used interchangeably. The following terms that appear in the report might be used to convey slightly different meanings from their general usage.

- *DER supporting system, supporting system, or system.* A system, application, or device used to support the operation of DER or grid services in relation to DER.
- *DER managing system or managing system.* A supporting system specifically used to manage DER. The essential functions of a DER managing system include data acquisition and control.
- *External network.* A telecommunication network that extends external to the local area network (LAN)—that is, a wide area network (WAN), Internet area network (IAN or cloud), or the Internet.
- *Security zone.* One or more subnets or broadcast domains where a device in a zone can communicate with other devices within the zone freely but access to and from devices outside the zone is controlled.

NETWORK SECURITY REQUIREMENTS

The general network security requirements described in this section are drawn from various cybersecurity standards available to the industry [1–6].

Provides guidelines for cybersecurity for DERs that are interconnected with electric power system.



IEEE 1547.3

Type of Project: New IEEE Standard **PAR Request Date:**

PAR Approval Date:

PAR Expiration Date:

Status: Not approved

1.1 Project Number: 1547.3
1.2 Type of Document: Guide
1.3 Life Cycle: Full Use

2.1 Title: Guide for Cybersecurity of Distributed Energy Resources Interfaces with Associated Electric Power Systems

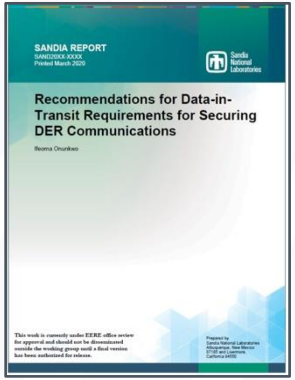
3.1 Working Group:

3.2 Sponsoring Society and Committee: IEEE-SASB Coordinating Committees/SCC21 - Fuel Cells, Photovoltaics, Dispersed Generation, and Energy Storage (SASB/SCC21)
Contact Information for Sponsor
Chair Name: Janette Sandberg
Email Address: janette.sandberg@pgn.com
Phone: 5036126119
Contact Information for Standards Representative
Michael Kipness

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 07/2021
4.3 Projected Completion Date for Submittal to RevCom 12/2021
Note: Usual minimum time between initial sponsor ballot and submission to RevCom is 6 months.:

5.1 Approximate number of people expected to be actively involved in the development of this project: 40
5.2 Scope: This document provides guidelines for Cybersecurity of Distributed Energy Resources (DER) interfaces with the Electric Power Systems (EPS).
5.3 Is the completion of this standard dependent upon the completion of another standard:
5.4 Purpose: This document provides guidelines for cybersecurity for one or more distributed resources that are interconnected with electric power systems. DER include systems in the areas of fuel cells, photovoltaics, wind turbines, microturbines, other distributed energy sources, and distributed energy storage systems. The revision will focus on updating the guidelines on mitigating cybersecurity risks at the individual DER device level that may be introduced by enabling communication capability at the DER interface, by utilizing the resources and standards that have been developed in the past 10 years.

Examines the cybersecurity requirements for DER comms protocols, per IEEE 1547-2018 revision.



SANDIA REPORT
SAND20XX-XXXX
Printed March 2020

Sandia National Laboratories

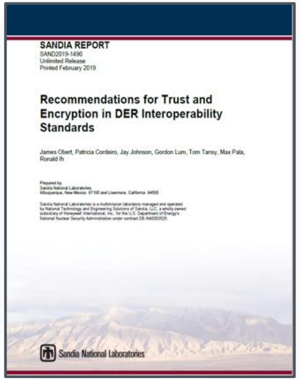
Recommendations for Data-in-Transit Requirements for Securing DER Communications

Ifeoma Onunkwo

This work is currently under EERE office review for approval and should not be disseminated outside the working group until a final version has been authorized for release.

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

Provides near and long-term recommendations to improve trust and encryption mechanisms for DER comms.



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

National Lab Support for Standards Development

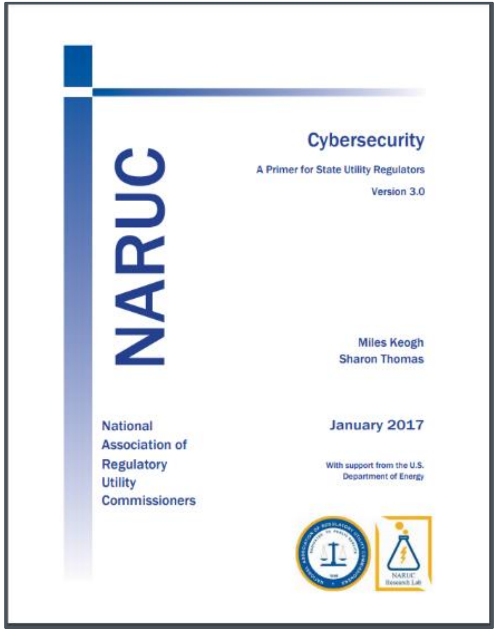
- Help establish a national (or international) standard and a certification program that is tailored specifically to address the cybersecurity concerns of high penetration solar, DER, and inverter-based resources
- Support the development of cybersecurity guides and standards for DERs such as IEEE 1547.3 and P2800
- Support the development of cybersecurity requirements for state energy officials
- Continue accelerating industry engagement for drafting technology standards packages
- Perform vulnerability assessments and studies, penetration testing for quantifying high penetration solar, IBR, and DER scenarios
- Support industry involvement in readiness testing and exercises for workforce development

Note: NREL is working with five other national labs to support industry in accelerating cybersecurity standards for DER.

The **Cybersecurity Information Sharing Act of 2015** authorizes and encourages private companies to take defensive measures to protect against and mitigate cyber threats.

Source: Cybersecurity Information Sharing Act of 2015. 2015. S. 754, 114th Congress.

Build Off of Existing Resources



NARUC

Cybersecurity

A Primer for State Utility Regulators

Version 3.0

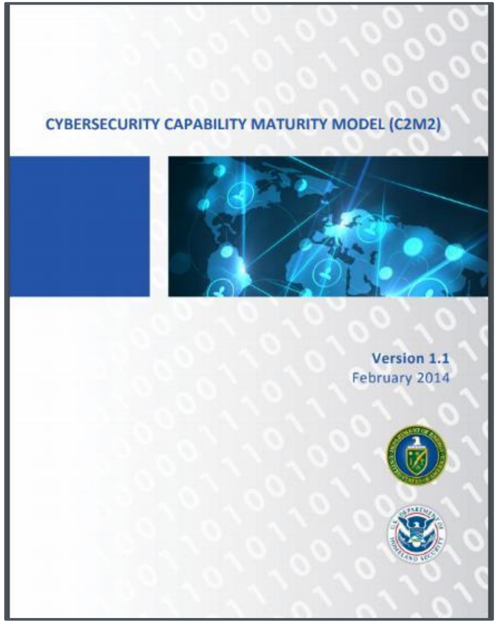
Miles Keogh
Sharon Thomas

National
Association of
Regulatory
Utility
Commissioners

January 2017

With support from the U.S.
Department of Energy

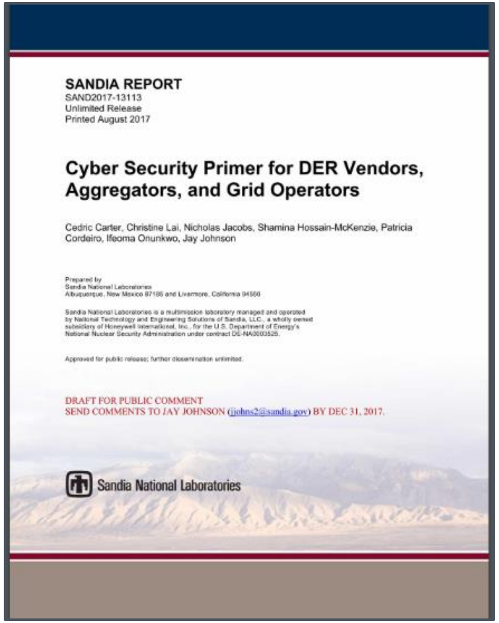
https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F



CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Version 1.1
February 2014

https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program



SANDIA REPORT
SAND2017-13113
Unlimited Release
Printed August 2017

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

Cedric Carter, Christine Lai, Nicholas Jacobs, Shamina Hossain-McKenzie, Patricia Cordeiro, Ifeoma Onunkwo, Jay Johnson

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.

Approved for public release; further dissemination unlimited.

DRAFT FOR PUBLIC COMMENT
SEND COMMENTS TO JAY JOHNSON (jjohns2@sandia.gov) BY DEC 31, 2017.

Sandia National Laboratories

https://www.osti.gov/servlets/purl/1761987

Important Cybersecurity Principles

1 Incorporate security at the design level

2 Advance security updates and vulnerability management

3 Build on proven security measures

4 Prioritize security measures according to potential impact

5 Promote transparency across the grid

6 Connect carefully and deliberately

Source: U.S. Department of Homeland Security. 2016. *Strategic Principles for Securing the Internet of Things*.

DER Testing, Certification, and Commissioning

What is impact of creating a DER cybersecurity certification standard?

- Ensures DER devices have all five pillars of cybersecurity: confidentiality, integrity, availability, authentication and non-repudiation
- Mandates DER devices pass cybersecurity certification to introduce a minimum level of cybersecurity to the electric grid, to prevent future cyberattacks and strengthen overall electric power system cybersecurity posture
- Creates an environment where the baseline security posture of the DER industry will be elevated

How can state energy offices support cybersecurity standard development efforts?

- Support cyber risk mitigation and resiliency
- Support and promote the implementation of best practices and cybersecurity polices with good governance, such as NIST CSF and/or NERC CIP
- Coordinate within state government and across the public-private nexus
- Respond to a cyberattack affecting energy infrastructure through consequence management as part of all-hazards energy assurance
- Contribute and/or actively support the development of DER cybersecurity certification standards and other relevant industry efforts

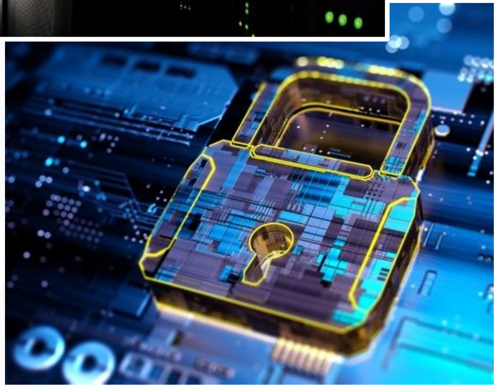
Source: Cybersecurity Information Sharing Act of 2015. 2015. S. 754, 114th Congress.

DER Testing, Certification, and Commissioning – Contd.

- Publish certification recommendations report for DER and IBR (Done)
- Publish the outline of investigation for DER cybersecurity testing protocols and carry that forward to a U.S. consensus certification standard. E.g., UL 9540 – Standard for Energy Storage Systems and Equipment
- Support the development of appropriate third-party conformity assessment programs for DER cybersecurity testing and certification
- Organize and host a DER cybersecurity summit by engaging thought leaders and key stakeholders to promote awareness and to establish practical and actionable plans to move forward
- Host informative industry webinars and perform related activities to drive awareness of DER cybersecurity requirements and conformity assessment programs

Recommended General Cybersecurity Policies

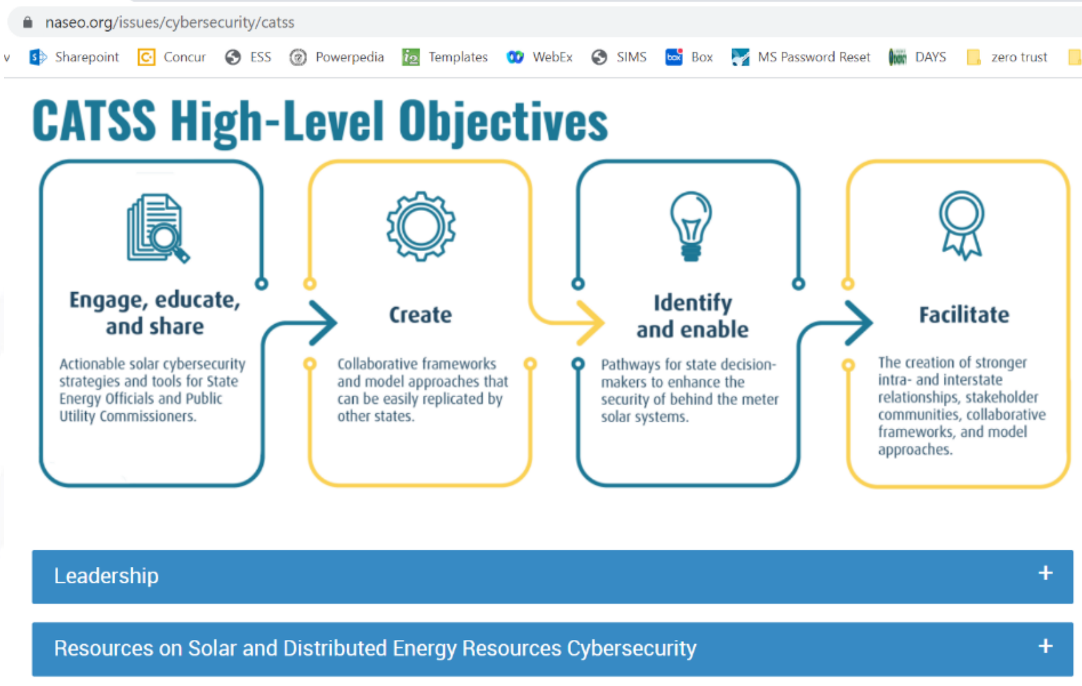
1. Isolate internal and external communication from each other.
2. Use of signature and context-based firewalls, gateways, and secured ports to separate the security domains. Consider disabling unused ports and services.
3. Use of authentication to ensure correct identities of personnel, customers, and vendors.
4. Use of Transport Layer Security to ensure encryption, authentication, and data integrity.
5. Use of intrusion detection systems and/or intrusion prevention systems to monitor communication network traffic.
6. Validation of all application software patches and software data updates with roll-back capabilities (if applicable).
7. Use of role-based access control for all communications, human-machine interface, and other places as appropriate.



Example project: NASEO & NARUC CATSS

Cybersecurity Advisory Team for State Solar (CATSS)

https://naseo.org/issues/cybersecurity/catss



CATSS High-Level Objectives

Engage, educate, and share

Actionable solar cybersecurity strategies and tools for State Energy Officials and Public Utility Commissioners.

Create

Collaborative frameworks and model approaches that can be easily replicated by other states.

Identify and enable

Pathways for state decision-makers to enhance the security of behind the meter solar systems.

Facilitate

The creation of stronger intra- and interstate relationships, stakeholder communities, collaborative frameworks, and model approaches.

Leadership +

Resources on Solar and Distributed Energy Resources Cybersecurity +

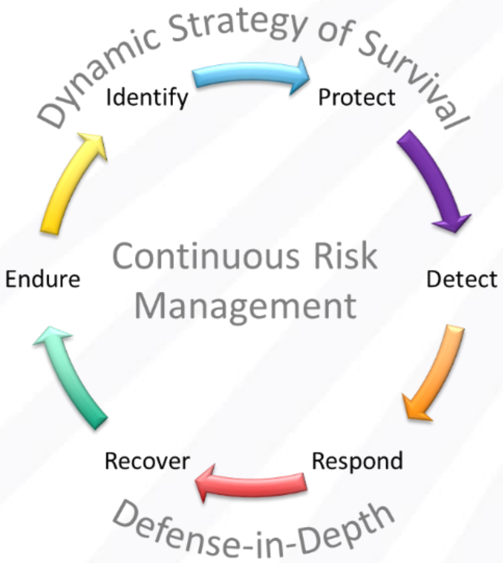
Questions?

Thank You!

Let’s Work together!

jeremiah.miller@ee.doe.gov

danish.saleem@nrel.gov



NREL/PR-5R00-80666