



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

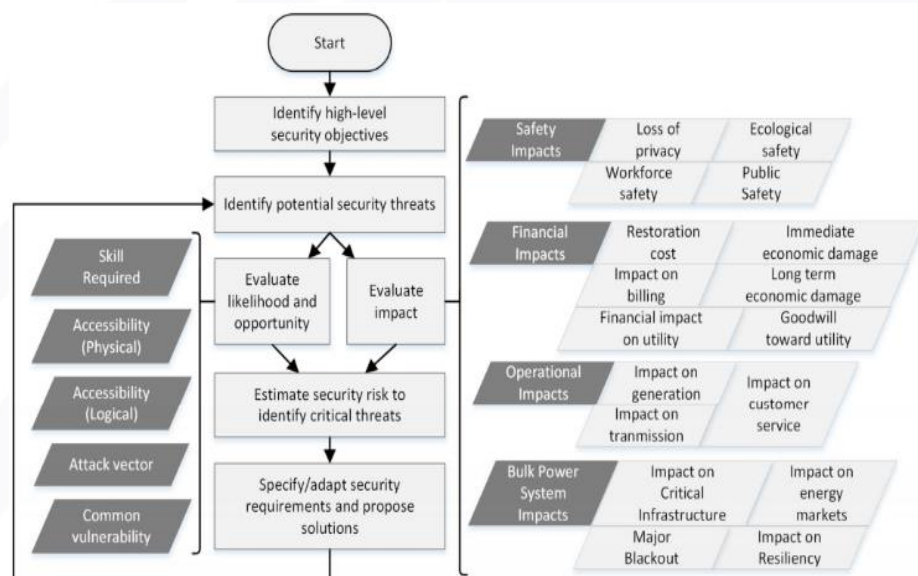
Zero-day attack: An attack that exploits vulnerabilities before the vendor releases a patch for that vulnerability.

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



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.



- 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

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

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>



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.

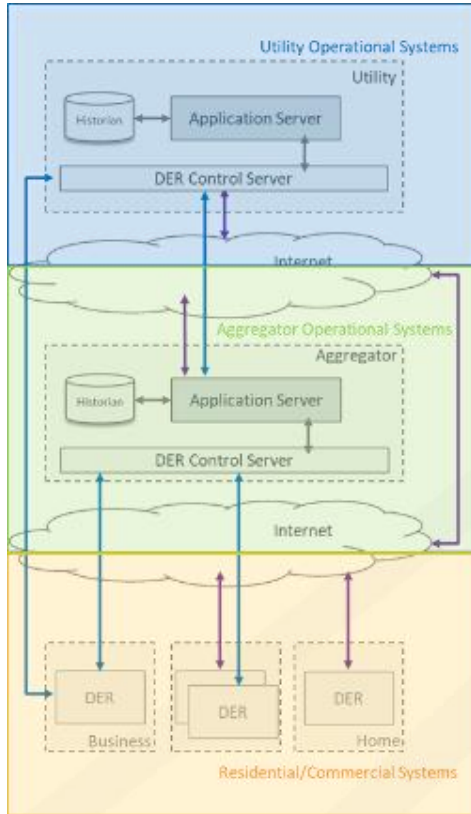


Potential Interconnection Issues

- 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

- 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



Example: Ukraine Power Grid Cyber-Attack

- 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.



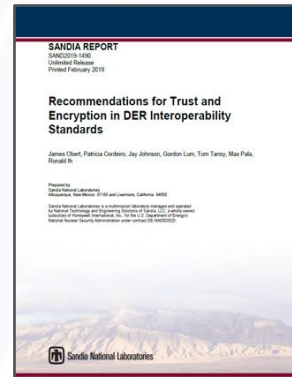
Provides test cases that can be used to check, verify and validate cybersecurity posture of DERs.

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

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

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

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



National Lab Support for Standards Development

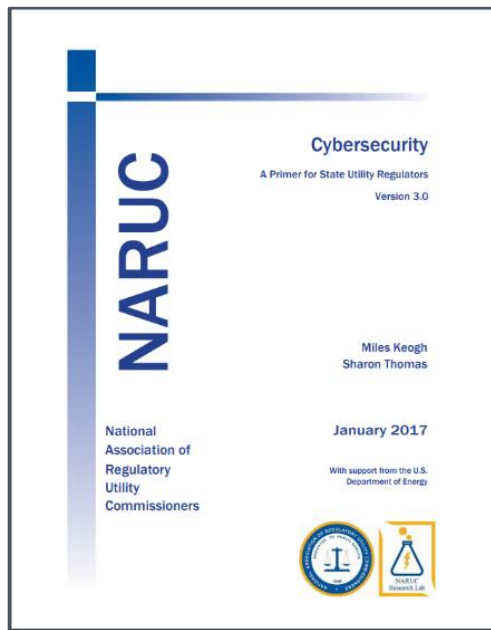
- Help establish a national (or international) standard and a certification program that is tailored specifically to address the cybersecurity concerns of high penetration solar, DER, and inverter-based resources
- Support the development of cybersecurity guides and standards for DERs such as IEEE 1547.3 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.

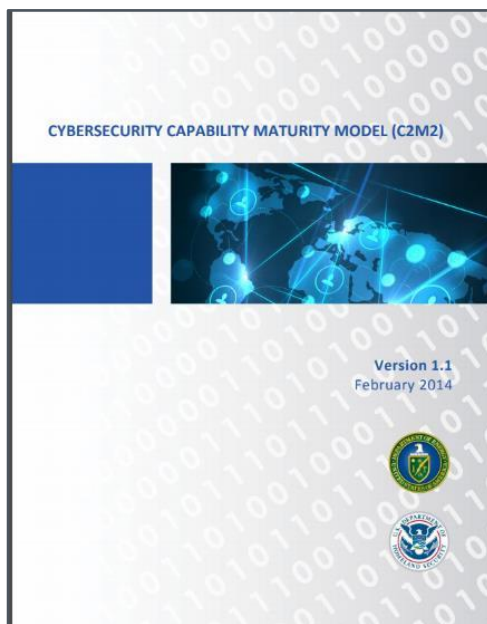
The Cybersecurity Information Sharing Act of 2015 authorizes and encourages private companies to take defensive measures to protect against and mitigate cyber threats.

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

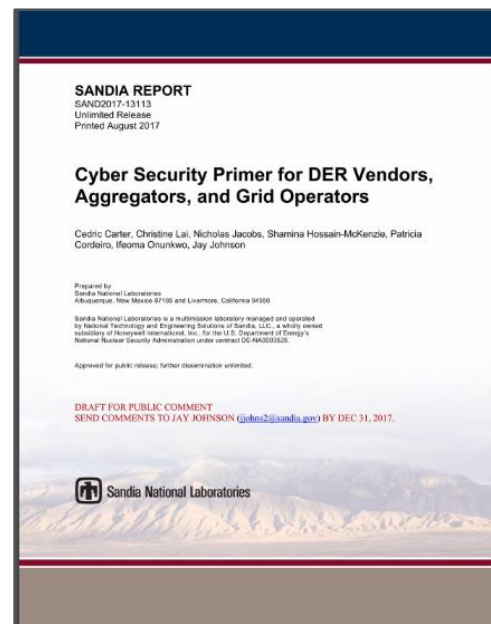
Build Off of Existing Resources



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



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



<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 policies 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

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

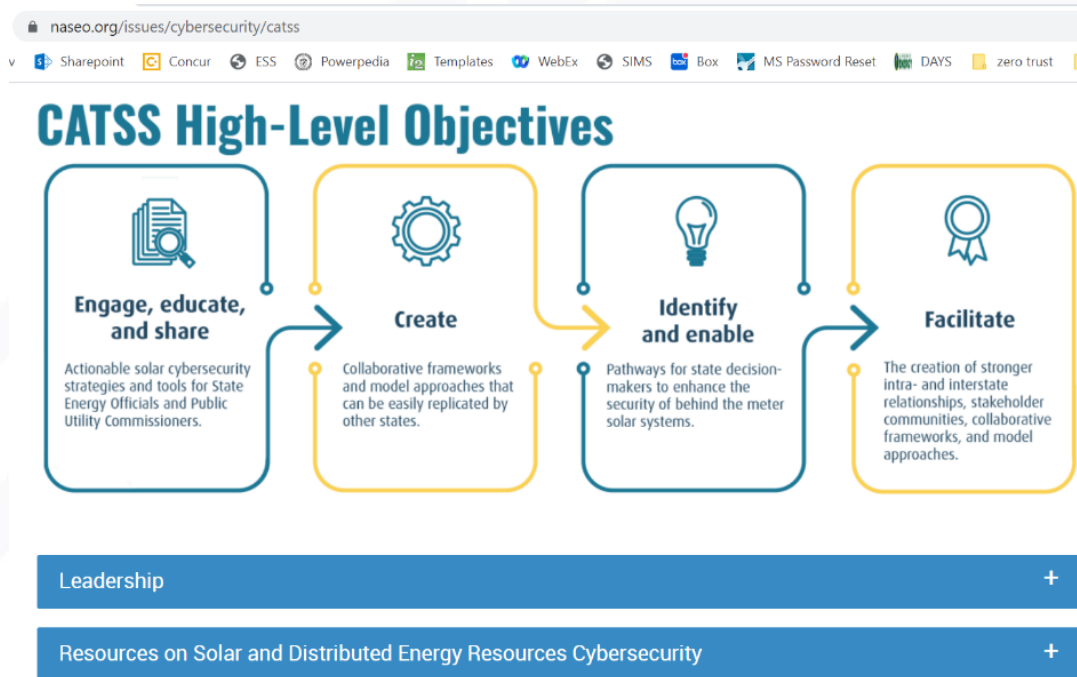
1. Isolate internal and external communication from each other.
2. Use of signature and context-based firewalls, gateways, and secured ports to separate the security domains. Consider disabling unused ports and services.
3. Use of authentication to ensure correct identities of personnel, customers, and 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>



Questions?

Thank You!

Let's Work together!

jeremiah.miller@ee.doe.gov

danish.saleem@nrel.gov

NREL/PR-5R00-80666

