Assessing Solar Cybersecurity:
Questions for States to Ask Electric Utilities

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

NASEO
National Association of State Energy Officials

Assessing Solar Cybersecurity: Questions for States to Ask Electric Utilities

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

Disclaimer:
The CATSS Toolkit is designed to provide states with basic education on cybersecurity issues for solar and enable their efforts to support cybersecurity enhancements efforts for solar. Cybersecurity challenges for solar should not be viewed as unique. All electricity generation technologies are, to varying degrees of potential severity and vulnerability, susceptible to cyberattacks and disruption. As interconnected electricity generation technologies, solar systems—and DERs generally—have a unique advantage to ensure that cybersecurity is incorporated by-design and prior to deployment, rather than applied ex post facto. The recommendations provided within the CATSS Toolkit/this tool were developed to meet the expressed needs of State Energy Offices and Public Utility Commissions during the project, and their respective purviews, priorities, and directives to support cyber-secure solar deployment in their states. While many industry and federal partners were included in the CATSS Advisory Group, it must be noted that neither the states' nor other stakeholders' perspectives collected are exhaustive. The Toolkit represents a snapshot of a quickly evolving and complex area, and should not be treated as a definitive guide, but rather a basis for continued discussion and adaptation of public-private partnerships for solar cybersecurity.

This material is based upon work supported by the U.S. Department of Energy (DOE) under award number DE-EE0009004. 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.

Cybersecurity Considerations for States

It is imperative that utilities and solar industry participants work together to ensure the grid remains reliable and safe. Solar industry participants must ensure the devices and systems they seek to connect to the grid support those goals. Cybersecurity is a key enabler of both. State Energy Officials and Public Utility Commissions should consider engaging investor-and consumer-owned utilities and the solar industry in topical discussions about their cybersecurity practices and priorities in general, and for interconnected solar systems, specifically. Understanding how utilities are identifying emerging solar-related threats, mitigating vulnerabilities, and training staff to effectively detect and respond to cyber incidents when they occur is helpful in developing complimentary policy and regulations. Such discussions help identify cybersecurity gaps and assist in emergency response planning. These discussions may be facilitated by States through a number of approaches, including public hearings and forums, working group discussions (See Case Studies and Model Guidance for Establishing Solar Cybersecurity Working Groups for further information), and other formal planning processes including utility coordination on State Energy Security Plans.

Questions for States to Ask Electric Utilities

The following questions serve as discussion prompts for states wishing to explore aspects of utilities' cybersecurity risk management programs that target solar devices, systems, and communication pathways. This list is not exhaustive. For convenience, they are organized according to the five risk management steps defined in NIST's Cybersecurity Framework.

1. Identify

- Have you established security requirements for solar systems and devices to interface with utility systems? If so, are these requirements captured in interconnection agreements, service level agreements or other types of contractual agreement?
- Do you have updated maps or a GIS system that contains all points of interconnection with solar systems and devices?
- Have communications and data flows between and among utility and solar systems and devices been documented?
- Does your risk management policies and plans include solar assets? Do cybersecurity risk assessments include threats, vulnerabilities, and impacts specific to solar systems and devices?
- How are threats and vulnerabilities specific to solar systems identified? What is the periodicity of threat and vulnerability assessments? Are they communicated to solar operators/aggregators?

2. Protect

- Do you use Multi-factor Authentication?
- Is the access principle of least privilege enforced?
- Do you require testing and certification from the solar operator/aggregator that cybersecurity practices and security technologies are implemented? How does the solar operator/aggregator ensure that they are using equipment from vetted equipment manufacturers?
- What controls are in place to ensure only vetted and approved access to devices, control systems, and communication channels is allowed? Is two factor authentication enabled?
- Are special access controls in place that permit making modifications to security settings for access points and communications networks protocols between utility and solar systems? Are change control protocols in place and all changes planned and documented?
- Are security patches programs in place for utility and solar aggregator owned devices? How are patches verified? Are roll-back procedures in place?
- Are internal and external communication networks segregated using firewalls, secure gateways, and similar technologies? Are unused ports and services closed, such that only permitted software functions are allowed?
- Are redundant communications paths in place?
- Can systems be physically updated? For example, can storage, central processing units or networking components be replaced? If so, what security controls are in place to prevent unauthorized physical access?
- What technologies are in place to protect data at rest and in transit? How is data authenticity and integrity ensured?

3. Detect

- Do you have analysis and visualization software that provides situational and operational awareness of solar devices and systems?
- Are cyber intrusion detection systems and/or intrusion prevention systems in place? Is communication network traffic monitored for signs of cyber intrusion? How are anomalous behaviors identified and reported?
- Are detailed activity logs created and preserved? If so, how are logs reviewed? How long are logs preserved?
- How are solar operators/aggregators notified of suspicious activity? Are policies and technologies in place to support information sharing?

4. Respond

- As part of all-hazards energy assurance/security planning, are cyber incident response policies and plans in place for minimizing the effects of a cyber incident involving an interconnected solar system? Are operational consequences well understood?
- Are event notification procedures in place? If so, are escalation criteria defined? Are thresholds for notifying external parties defined?
- How are software and hardware vulnerability remediation activities tracked? Are those activities shared with third parties? If so, who is such information shared with and how?
- Are roles and responsibilities for cyber incident response defined and coordinated with solar operators/aggregators? Does the solar operator/aggregator have a workforce trained to undertake a rapid response to a cyber incident?
- Are exercises conducted that test and validate cybersecurity incident response plans? If so, how often are exercises conducted? Are solar operators/aggregators included in those exercises?

5. Recover

- Do restoration plans reflect solar assets based on their priority designation?
- Are restoration plans communicated to and coordinated with third parties including solar operators/aggregators?
- Are cyber mutual aid agreements in place with other entities?
- Do you have cybersecurity insurance that covers DER assets and related communications systems?

Key Terms

Commissioning testing – The evaluation of a DER system after installation, but before final energization to inspect the system and verify that it was installed properly and to confirm that it functions as designed. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-32.pdf.

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. https://www.nrel.gov/docs/fy22osti/80666.pdf.

DER Aggregator - An entity that groups together DER resources for the purposes of operating it as a group for grid services. https://www.nrel.gov/docs/fy22osti/80666.pdf

DER Owner/Operator – 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. https://www.nrel.gov/docs/fy22osti/80666.pdf

Evaluation – The review of the design of the DER system and/or a review of the "as-built" DER system, typically performed by a utility engineer. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-32.pdf

Interconnection rules – Regulations that govern the processes required for generating facilities to connect to the grid; also called "interconnection standards" or "interconnection procedures." https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-32.pdf

Interoperability – The capability of two or more different systems, networks, or technologies to communicate and exchange information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-32.pdf

Point of Common Coupling – The point of connection between the DER customer and the utility, typically at the utility revenue meter. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-32.pdf


NASEO
National Association of
State Energy Officials
NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS
DEDICATED TO PUBLIC SERVICE
1889