Exercise Design Guidance for Solar Cybersecurity

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

NASEO
National Association of State Energy Officials

NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS
DEDICATED TO PUBLIC SERVICE
1889

Exercise Design Guidance for Solar Cybersecurity

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.

Introduction

The intent of this resource is to provide recommendations on how State Energy Offices and Public Utility Commissions might design an energy emergency exercise, drill, or other simulation focused on solar cybersecurity themes and concepts. While the primary target audience is State Energy Offices and Public Utility Commissions, any exercise practitioner, planner, or facilitator interested in exploring solar cybersecurity incident response, preparedness, recovery, or mitigation may find this a valuable resource.

This resource is intended to be an advanced supplementary resource for persons or entities with prior exercise experience and knowledge. It should not be used as a baseline educational resource for how to conduct and evaluate an exercise. It is based on a set of standard concepts, terms, and procedures that are common among the exercise community.

This tool should be referenced in conjunction with the ***Solar Cyberattack Consequence Scenarios*** tool within the CATSS Toolkit.

For background information, NASEO and NARUC recommend referring to the following resources prior to reviewing this guidance:

- Homeland Security Exercise and Evaluation Program (HSEEP) – U.S. Department of Homeland Security
- Cybersecurity Tabletop Exercise Guidance - National Association of Regulatory Utility Commissioners

Exercises Overview

Exercises provide opportunities for participants to demonstrate and assess capabilities in specific areas of interest, including cybersecurity risk management. They also facilitate coordination and help clarify organizational roles and responsibilities; foster meaningful interaction and communication across jurisdictions/organizations; assess and validate plans, policies, procedures, and capabilities; and identify strengths and areas for improvement.

For solar cybersecurity stakeholders, exercises offer the opportunity to create and expand networks between solar industry entities, electric utility emergency managers, state energy security and resilience planners and Energy Emergency Assurance Coordinators, federal partners, and others. Further, such exercises can help identify gaps pertaining to solar infrastructure in state resilience plans, emergency management plans, energy security plans, utility emergency response plans, and more.

While exercises can take a variety of forms ranging from procedural walkthroughs to operational drills and full-scale exercises, solar cybersecurity exercises should be limited to more simple executions, such as the options listed below:

- **Seminar** — Seminars are lecture-based exercises that orient participants to provide an overview of the solar cybersecurity risks, and the strategies, plans, policies, or procedures intended to reduce those risks. Seminars are especially useful when an entity has developed a new plan or made changes to existing plans or procedures. For solar cybersecurity stakeholders, a seminar may focus on relevant subjects such as:
  - Newly emerging risks including threats, vulnerabilities, exploits, and consequences
  - New and existing policies, legislation, or standards (e.g., IEEE standards, NERC CIP updates, FERC rules, "Buy American" provisions, supply chain requirements, etc.)
  - Comprehensive State Energy Plans, State Energy Security Plans, and/or Cybersecurity Incident Response plans, and other state plans as they pertain to solar energy goals deployment and cybersecurity
  - Utility or RTO/ISO energy disruption response plans
- **Workshop** — Typically small-group, interactive exercises that focus on idea generation or validation. Built around in-depth, issue-driven discussions, workshops encourage collaboration and joint decision making, which are essential to obtaining consensus and producing effective plans and procedures. For solar cybersecurity stakeholders, a workshop may focus on more discreet issues such as:
  - Basic cybersecurity hygiene and training for solar industry entities
  - Cyber-physical protections
  - Criticality evaluations of and mitigation measures for solar installations (e.g., a solar plus storage microgrid at a hospital vs. rooftop solar without backup power)
  - Solar cybersecurity workforce development
  - Risk ownership of installers, manufacturers, aggregators, utilities, asset owners, etc.

- **Tabletop Exercise (TTX)** — TTXs bring key stakeholders together to work through a scenario for the purpose of testing preplanned actions. This format facilitates a holistic view of strategies and tactics, and allows participants to assess sufficiency and effectiveness, identify gaps, and suggest improvements. For solar cybersecurity stakeholders, this may include:
  - Scenario-based discussions of cyber incidents affecting solar infrastructure IT or OT systems, including generation or asset management
  - Information sharing in the event of a cyber-attack or intrusion
  - Walkthroughs of public and private cyber-incident response plans with specific questions pertaining to solar cybersecurity
  - Roles and responsibilities during an emergency response by the public and private sectors

Why Exercises?

Traditional energy emergency response exercises are common tools of State Energy Offices, Public Utility Commissions, the Federal government, and utility partners. The relatively uniform structure and procedures offered by HSEEP serve as a familiar forum for discussion, collaboration, and action among all participants, regardless of their familiarity with the subject matter. Exercises are generally inclusive and approachable, which makes inclusion of solar cybersecurity topics and stakeholders relatively easy for entities with prior experience planning or participating in exercises.

Exercise Planning Recommendations

The exercise should be designed by an exercise planning team. Given the relatively new concept of a solar cybersecurity exercise, planners should seek to leverage existing exercise programs or templates and involve stakeholders familiar with the exercise planning and development process as part of the planning team and participant group.

The planning team should include representatives from the intended participants. That is, if the intended players consist of state players, solar manufacturers, solar asset owners, and distribution utilities, then there should be at least one representative from each of those groups present on the planning team to verify that the assumptions about each group are correct, and that questions and objectives are relevant and approachable for their respective players. In addition, if the exercise is based on a disruption to a specific device, system or facility the owner and operator of those should also be involved to assure that there is buy-in to the event and to help ensure that the scenario is reasonable and plausible.

Participants should include a mix of players with previous exercise experience, and players who are new to participating in exercises.

Potential participants in solar cybersecurity exercises can include:

- Key State Officials (State Energy Office, Public Utility Commission, Emergency Management Agency, Governor's Office Representatives, Transportation Agency, Information Technology [IT] Officials, State Homeland Security Office, Fusion Center, National Guard Cyber Unit, State Administration Agency)
- Distribution Utility Owners/Operators
- Transmission Grid Owners/Operators (RTOs/ISOs)
- Solar Installers
- Solar Manufacturers
- DER Aggregators
- PV System/Asset Owners (e.g., hospitals, microgrid owners with PV systems)
- Federal Partners (U.S. Department of Energy, Power Administrations, U.S. Department of Homeland Security, Federal Emergency Management Agency, Federal Bureau of Investigation, etc.)
- Key local government officials
- Tribal Nations
- First Responders

Not sure who to invite or how to reach them? Check out the "Leadership" tab on the CATSS Homepage to see which organizations are involved in CATSS. For additional suggestions or introductions, contact Kirsten Verclas at kverclas@naseo.org or Sarah Trent at strent@naseo.org.

Example Tabletop Scenarios

Any postulated exercise scenario should be founded in fact and remain within possible parameters. Scenarios are oftentimes developed based on real incidents or plausible hypothetical events, with certain elements or variables being created or exaggerated to achieve specific goals or direct exercise conversation in a targeted direction.

The following scenarios are example scenarios that could be explored by a TTX:

Example Scenario #1:

A denial-of-service attack (DoS) on a solar owner's system prohibits the owner from viewing the asset status. Though no generation interruptions are initially reported by the grid operator, the asset owner must act to regain situational awareness, determine the extent of the cyberattack and intrusion, and take appropriate mitigative actions.

Real World Example Reference: https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/

Sample Objectives

- Identify the guiding cybersecurity incident reporting and response requirements (i.e., who does the asset owner contact and when should they be contacted?).
- Evaluate asset owner cybersecurity incident response plans.
- Assess the associated risks of generation loss and other economic and human consequences and interdependencies which may compound the situation.

Sample Questions for Participants

- What are the first steps taken by an asset owner in this scenario? Do they align with the expectations around state and federal reporting and response requirements?
- Depending on the scenario would you engage law enforcement agencies and if so, who?
- What can and should be done prior to an incident like this? How can states work with industry and the federal government to ensure that risks, vulnerabilities, threats, and software patches are shared in a timely manner?

Suggested Players

- PV asset owners (e.g., rooftop solar owner, community solar owner, microgrid owner, utility, etc.)
- State Energy Office and Public Utility Commission
- Aggregator
- Grid Operator
- Distribution Utility

Example Scenario #2:

A coordinated cyberattack targeting PV installations within a multi-state region via internet-connected inverters occurs during peak sunshine hours. Over the course of a half hour, the attacker triggers multiple failures of PV systems providing 20% of the RTO's power, causing numerous GW swings per minute. The attack follows no expected pattern, and the attacker can control the flow faster than the grid operators, leading to an unmanageable power flow and subsequent regional grid failure and cascading impacts.

Real World Example Reference: https://horusscenario.com/

Sample Objectives

- Identify the relevant cybersecurity incident reporting and response requirements (i.e., who does the asset owner contact and when should they be contacted?).
- Define type of cybersecurity incidents, such as inability to monitor or control versus loss of information.
- Determine roles and responsibilities of each person involved in the response team; specify who the decision makers will be.
- Identify the types and criteria of information that should and should not be respectively reported to law enforcement, emergency response, senior management, cybersecurity experts, legal counsel, suppliers, or insurance providers.
- After the event has been resolved, as part of an After-Action report, determine near-, mid-, and long-term mitigation actions that solar asset owners, manufacturers, and installers can take to ensure reliability of solar generation assets.

Sample Discussion Questions

- How is relevant information shared?
- What are the requirements for reporting?
- What are the restrictions on sharing sensitive information?

Potential Players

- PV asset owners (PV plant operators)
- Aggregators
- Solar manufacturers
- Solar installers
- State Energy Offices and Public Utility Commissions
- Grid Operators, ISO, and RTO
- Distribution Utilities
- State energy agencies in the region affected by the scenario
- DOE/CESER, DHS/CERT, FBI, other

Example Scenario #3:

A cyber actor gains control of a utility system controlling a microgrid, which serves load to a number of local critical facilities, including a hospital and fire station, through an exploitable vulnerability in the PV system's remote management system. The actor alters the conditions that determine when a utility has permission to disconnect a pre-established microgrid from the grid. This modification prevents the microgrid from disconnecting during an unrelated outage, leaving the hospital and fire station vulnerable to electricity service interruptions that would otherwise not occur during a grid disruption if the microgrid were able to disconnect.

Hypothetical Example Reference: https://smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf

Sample Objectives

- Identify the relevant cybersecurity incident reporting and response requirements (i.e., who does the asset owner contact and when should they be contacted?)
- What actions are taken to restore any loss of power? Who is responsible for these actions? How long will they take?
- Determine immediate mitigation actions that solar asset owners and installers can take to ensure reliability of solar generation assets.
- Define type of cybersecurity incidents, such as inability to monitor or control versus loss of information.
- Determine roles and responsibilities of each person involved in the response team; specify who the decision makers will be.
- Identify the types and criteria of information that should and should not be reported to law enforcement, emergency response, senior management, cybersecurity experts, legal counsel, suppliers, or insurance providers.
- Identify protective measures that can be used to prevent future breaches.

Sample Discussion Questions

- How is relevant information shared?
- What are the requirements for reporting?
- What are the restrictions on sharing sensitive information?

Potential Players

- PV asset owners (e.g., microgrid owners)
- Direct customers of affected microgrid (e.g., hospital emergency managers)
- Solar manufacturers
- Solar installers
- State Energy Offices and Public Utility Commissions
- Emergency Management

Additional Scenarios

The Electric Power Research Institute's (EPRI) *Electric Sector Failure Scenarios and Impact Analyses – Version 3.0*, has outlined a number of different plausible scenarios identified by industry partners for purposes of risk assessment, planning, procurement, training, tabletop exercises and security testing, and may be considered for further scenario development by the solar cybersecurity community. There is an entire section dedicated to Distributed Energy Resource (DER) scenarios. A few notable examples are as follows:

- (1) The DER owner fails to change the default password or not set a password for the DER system user interface. A threat agent (inept installer, hacker, or industrial spy) gets access through the user interface and changes the DER settings so that it does not trip off upon low voltage (anti-islanding protection) but continues to provide power during a power system fault.
- (2) An industrial or large commercial DER system is configured for local operational access through a wireless network but is erroneously connected to the company's wireless corporate network, thus exposing the DER system to the Internet. Through the incorrect connection to the Internet, a threat agent gains control of the DER system and alters the operation of the DER functions to make them ignore utility commands and to turn off the "acknowledge command" interaction with the utility. The DER system may no longer limit power output during critical situations.
- (3) A threat agent, possibly a disgruntled employee of the DER vendor or a DER implementation company, makes malicious software changes to equipment software or firmware. This malware causes large numbers of DER systems to ignore certain critical commands from the utility. For example, after some future date, it prevents the DER systems from limiting their energy output when so commanded and then locks out any other commands.
- (7) A utility-owned DER system is located in a substation with the primary purpose of providing additional power during a critical peak. A threat agent changes the time clock in the DER system through a false time-synchronization message, so that either the DER system believes that the critical peak event is over or that all time- stamped messages to it are invalid, so it goes into default shut-down mode.
- (20) A threat agent accesses the DERMS system and modifies the weather data being used to forecast loads and DER generation/storage. Consequently, less than optimal requests are sent to DER systems, causing financial impacts to the utility.
- (23) A threat agent obtains control of the DER management system of a Retail Energy Provider (REP) (who might be a department within a utility or could be a Third Party). The REP then provides invalid information to the utility grid operators on the future availability of large amounts of DER energy and ancillary services. This causes the grid operator to make less-than-optimal market decisions on purchasing energy and ancillary services.
- (24) A Retail Energy Provider (REP) that manages a group of DER systems normally receives commands from the DERMS on what energy levels and ancillary services that group of DER systems should provide. A threat agent accesses confidential or private information in the DERMS DER database on customers who own DER systems and uses that information to "market" to those customers.

Resources and References

Cybersecurity in Photovoltaic Plant Operations, National Renewable Energy Laboratory & Sandia National Laboratories, 2021: https://www.nrel.gov/docs/fy21osti/78755.pdf

Electric Sector Failure Scenarios and Impact Analyses – Version 3.0, Electric Power Research Institute (EPRI), 2015: https://smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf

The Horus Scenario, William Westerhof, https://horusscenario.com/

Walton, Robert. (November 2019). *First Cyberattack on Solar, Wind Assets Revealed Widespread Grid Weaknesses, Analysts Say.* Utility Dive. https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/.


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