ANNEX C

NASEO
National Association of State Energy Officials

Hypothetical Solar Cyberattacks Scenarios and Impacts

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

Hypothetical Solar Cyberattacks Scenarios and Impacts

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.

About the Project

The Cybersecurity Advisory Team for State Solar (CATSS) is a project implemented by the National Association of State Energy Officials (NASEO) and the National Association of Regulatory Utility Commissioners (NARUC) to aid in mitigating cybersecurity risks and consequences in solar energy developments. With support from the United States Department of Energy Solar Energy Technologies Office, the project leverages state, federal and private-sector expertise on cybersecurity, grid and photovoltaic to identify and model solar cybersecurity programs, policies, and actions for states to take in partnership with utilities and the solar industry.

Acknowledgements

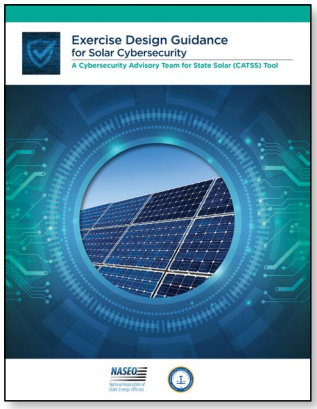
The authors of this paper are Dakota Roberson from the University of Idaho and Shoshana Cohen, Jack Graul, Jonathon Monken, and Alex Pina, from Converge Strategies, LLC (CSL). The authors would like to gratefully acknowledge the input and feedback from the project Advisory Group.

The authors also thank Sarah Trent and Kirsten Verclas from National Association of State Energy Officials (NASEO), their partners at the National Association Regulatory Utility Commissioners (NARUC), and at the Department of Energy (DOE) Solar Energy Technology Office (SETO) for their leadership and guidance.

Executive Summary

The intent of this resource is to offer approachable, plausible scenarios of cyberattacks affecting solar PV assets and interconnected infrastructure. It may be used by State Energy Officials and Public Utility Commission Staff to educate themselves on the potential consequences of these scenarios and the practical, high-level actions that may be implemented now be needed to mitigate future impacts.

The following risk scenarios are based on a variety of hypothetical variables pertaining to levels of installed solar generation and different ownership structures. These scenarios aim at highlighting potential consequences of inadequate cyber provisions for PV solar systems and offer potential state actions to alleviate the identified risks. This document outlines potential consequences and how a breach might affect stakeholders (e.g., utility, aggregator, consumer) and provides an understanding of PV vulnerabilities and attack types.



This resource should be referenced in conjunction with the Exercise Design Guidance for Solar Cybersecurity tool within the CATSS Toolkit.

RISK SCENARIO 1

Overview	Description
Attack Type	Distributed Denial of Service (DDoS)
Component Targeted	Remote Terminal Unit (RTU)
Component Damage	Minimal
Grid Impact	Moderate

SCENARIO: A distributed denial-of-service attack (DDoS) on a solar aggregator prohibits the aggregator from viewing the status of 500MW of solar in one ISO/RTO territory. No generation interruptions are initially reported by the aggregator to the utility, but residential customers are experiencing power quality issues. The aggregator must act to regain situational awareness, determine the extent of the cyberattack, and take appropriate mitigation actions.

Real World Example Reference:

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

Stakeholders and Consequence

- PV Asset Owners: Potential impact on payment from aggregator
- Aggregators: Unable to view asset status to determine functionality
- Grid Operators: No impact unless operator needs aggregator to shed generation
- Distribution Utilities: No immediate impact but could be a safety concern if there is an outage with live conductors due to unknown solar asset status
- Residential customers are experiencing power quality issues and may have damage to connected electronic devices.
- State Energy Offices and Public Utility Commissions: Depending on information-sharing requirements within the state and established relationships (i.e., formal or informal) between the state and the affected entities, the state may be notified of the incident and may have certain details shared with them

Potential State Actions to Alleviate Risk

- Develop policy requiring DDoS protection for solar assets
- Develop policy requiring solar asset owners and aggregators to notify operators when solar asset status is unknown or uncontrolled
- Develop or enforce any contract provision related to this event for which State Energy Offices or Public Utility Commissions may have authority.
- Develop policy for manual operation of system if remote/automated connectivity is lost

RISK SCENARIO 2

Overview	Description
Attack Type	Insider Threat
Component Targeted	String Combiners
Component Damage	Moderate
Grid Impact	Minimal

SCENARIO: A solar maintenance contractor with significant financial debt is recruited by a cybercrime organization to provide access to solar assets connected to critical facilities. The contractor plugs a USB drive into the solar PV string combiner for a microgrid that serves a hospital and fire station. Since the string combiner wasn't updated recently, the USB automatically uploads malware that grants the cybercrime organization access to the microgrid controller network through a known vulnerability. The attackers use their network access to block communication between items on the microgrid, shutting down the microgrid's ability to produce power. The microgrid operators must act to regain control of the microgrid, determine the source of the cyberattack, and take appropriate mitigation actions.

Hypothetical Example Reference:

- https://www.justice.gov/opa/pr/russian-national-indicted-conspiracy-introduce-malware-computer-network

Stakeholders and Consequence

- Solar components manufacturers: News of vulnerability may decrease sales
- Solar maintenance contractors: Reputation will decrease and may incur fines based on contract language
- PV asset/microgrid owners: Critical loads will lose power
- Microgrid customers: Critical operations will not have power and power may be injured
- Emergency management agencies: Need to execute power outage response plans
- State Energy Offices and Public Utility Commissions: No immediate impact

Potential State Actions to Alleviate Risk

- Develop policy for component manufacturers to push automatic updates to software
- Develop policy requirement contractors to conduct insider threat training
- Develop policy for firewalls between solar components and control/SCADA equipment
- Develop policy for manual controls of microgrid if remote/automated controls are unresponsive
- Review and update criteria for backup power and additional generation resources

RISK SCENARIO 3

Overview	Description
Attack Type	Ransomware
Component Targeted	Data Acquisition System (DAS)
Component Damage	Moderate
Grid Impact	Moderate

SCENARIO: A cyber attacker gains access to a data acquisition system and begins monitoring all the network traffic for a 100MW solar asset to identify the command-and-control signals. After decoding the signals, the attacker modifies access commands to lock all users out of the system and modifies operating commands to open the programmable repeaters bringing the system offline. The cyber attacker notifies the asset owner they have 1 hour to send 3,000 Bitcoin to the attackers' cryptocurrency wallet, or the attacker will initiate a command to destroy the solar asset control hardware. The solar asset owner must act to avoid destruction of the solar asset and reconnect the asset to the grid.

Real World Example Reference:

- https://www.theguardian.com/world/2018/oct/04/how-russian-spies-bungled-cyber-attack-on-weapons-watchdog
- https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

Stakeholders and Consequence

- Solar asset owner/operators: Potential to lose over $60M or the asset
- Utility providers: May see voltage and frequency instability on lines with outages to local customers
- Grid operators: Unplanned outage of large generation asset requiring spinning reserve
- FBI: Need to support asset owner and protecting systems and finances
- State Energy Offices and Public Utility Commissions: The State Emergency Operations Centers and ESF-12 staff would likely be activated. There would be widespread concerns about additional attacks on other parts of the power grid, and questions would be directed towards the state government. The State should have a fundamental understanding of the situation and appropriate contacts to share relevant and shareable (i.e., non-sensitive) information with the public.

Potential State Actions to Alleviate Risk

- Develop policy to ensure all large solar owners and operators contact FBI, grid operator, and utility provider after the cyberattack
- Develop policy for solar operators to have method to manually recover compromised equipment (i.e., "gold disk")
- Assure all operators should have disaster recovery plans to allow the rapid restoration of system hardware and software should they be compromised
- Develop a policy requiring "zero-trust" environments for control networks

RISK SCENARIO 4

Overview	Description
Attack Type	Advanced Persistent Threat, Zero-day Vulnerability
Component Targeted	Smart Inverters
Component Damage	Moderate
Grid Impact	Severe

SCENARIO: A nation-state identifies a zero-day vulnerability and an exploit that could be used to affect internet-connected inverters used by most solar developers due to interconnection requirements from utilities and state energy officers or public utility commissions. Many months after identifying this vulnerability, the nation-state coordinates a massive cyberattack targeting PV installations within a multi-state region during peak sunshine hours. Over the course of a half hour, the attacker cycles the inverters on PV systems providing 20% of the RTO's power, causing numerous GW swings over the course of seconds causing instability. The attack follows no expected pattern, and the attacker is capable of controlling the output of the solar assets by the second, which is much faster than the grid operators who are able to respond in the order of minutes. Ultimately, this leads to an unmanageable power flow and subsequent regional grid failure and cascading impacts. These impacts can cause physical damage to generation assets. Grid operators must identify and isolate the cyberattack while restoring the bulk power system.

Real World Example Reference:

- https://horusscenario.com/

Stakeholders and Consequence

- Inverter manufacturer: News of vulnerability may decrease sales
- PV asset owners/operators: Equipment may be damaged, and assets will not generate revenue
- Grid operators may have damage to their equipment and systems
- Distribution Utilities: Staff will not be able to restore local power and conductors and equipment until grid generation is under control. Other utility assets may also suffer damage.
- Grid Operators: Need to begin black start process to re-energize the grid after isolating solar assets to avoid further issues.
- State Energy Offices and Public Utility Commissions: The State Emergency Operations Centers and ESF-12 staff would likely be activated. There would be widespread concerns about additional attacks on other parts of the power grid, and questions would be directed towards the state government.

Potential State Actions to Alleviate Risk

- Immediate development and distribution to affected stakeholder a software patch to eliminate the vulnerability and exploit capability.
- Improve the State cyber response plans and capabilities in both the public and private sectors.
- Develop a policy with lockout times for equipment to avoid cycling faster than grid operators can respond
  - Develop a policy requiring installers and aggregators to identify commons components in each build into a national database
  - Develop a policy limiting the concentration of any single specific component in a region
  - Develop a policy encouraging "white hats" to identify vulnerabilities in the most common pieces of equipment