State Legislative Options to Enhance Solar Cybersecurity

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

NASEO
National Association of State Energy Officials

State Legislative Options to Enhance 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

As State Energy Offices and Public Utility Commissions (PUCs) seek to advance solar cybersecurity efforts within their states, legislation can serve as one tool to facilitate, guide, or require actionable policy and program development. Legislation can reinforce the criticality of protecting energy infrastructure from cyber threats in several ways that can have long lasting impacts. These include allocating funding to cybersecurity planning, preparedness, and response activities; forming task forces or working groups that engage relevant stakeholders; requiring utilities to publish annual cybersecurity plans; or setting other requirements for government agencies, utilities, and developers that will proactively guard electric systems against cyber threats such as limiting foreign contracts or developing a state-wide communication strategy for reporting cyber-attacks. These potential avenues of advancing solar cybersecurity efforts on the state level can make sure that information is not compromised, and that critical infrastructure is protected. An outage triggered by a cyber-attack can have widespread impacts as demonstrated by the cyber-attack on the Colonial Pipeline in 2021. A cyber-attack on a solar farm could lead to blackouts that can have ripple effects on a variety of individuals and businesses, including vulnerable populations.

How State Energy Offices and PUCs can support the development of legislation will, of course, vary state to state, especially depending on the nature of the relationship that exists between the state legislature and state agencies, and the amount of funding being allocated by the legislature. Funding can allow for adequate staffing to engage in data collection, community outreach, and resource development of policy roadmaps or frameworks for the state. State Energy Offices and PUCs can provide insights into pending legislation and make policy recommendations that can ensure the language of potential laws is actionable and correctly defined.[1] Having an established relationship with the state legislature can make sharing recommendations and relevant information easier for both agencies.

Although cyber-attacks on a solar system are a credible threat, there does not appear to be any discreet efforts to pass legislation designed to enhance cybersecurity and distributed energy resources (DERs). State legislation instead focuses more on cyber threats to the entire energy system, broadly.

Recent Legislation and Related Activity

State agencies, developers, and utilities are well aware of the cyber risks posed by the confluence of an aging electric grid lacking stringent control systems and advanced technologies, such as smart inverters, utilized by solar and storage systems. According to the National Conference of State Legislatures (NCSL) most recent legislation related to mitigating energy system cyber threats centers around four main areas: (1) establishing task forces and committees (2) establishing standards and reporting requirements (3) expanding open records exemptions to include cyber vulnerabilities and (4) directing and authorizing governors and state agencies to prepare for and respond to cyber-attacks.[2] Examples of these areas are shared in the next section. These kinds of actions can bring consistency to the industry by requiring utilities to follow similar guidelines and ensure each state is prepared to handle a no-notice cyber-attack while identifying and mitigating threats before they arise.

State-level working groups and task forces can make policy recommendations and share resources on the importance of protecting solar energy technologies from cyber threats and vulnerabilities. For example, **Texas SB 475** established an Electric Grid Security Council as a result of public interest in mitigating cyber and physical threats to the energy system.[3] Some of the responsibilities of the council will include developing a set of grid security best practices and amending the state emergency management plan to include information on coordinated response efforts when the electric grid's security is threatened.[4] Members of the council will include the governor or a representative designated by the governor, a representative from the Electric Reliability Council of Texas (ERCOT), and a member of the state legislature. The council will also coordinate with other organizations including the Texas Division of Emergency Management, U.S. Department of Energy, and other state and federal agencies. The council members must all have or be able to obtain secret security clearance. This can be a challenge for State Energy Offices and PUCs as they do not always have the resources on hand to get this type of clearance or are not prioritized in getting clearances.

It is also helpful for DER developers to have access to utility system data. Having this data on hand makes it easier for developers to identify opportunities to connect solar projects to the grid and any cost considerations that might influence the siting of the project. The Minnesota Department of Commerce brought on Synapse Energy Economics Inc. to develop a report, *Hosting Capacity Analysis and Distribution Grid Security*, in April 2021, that looked at potential solutions for protecting data from a cyber attacker. The state was looking for ways to increase the amount of distributed energy resources (DERs), including solar, in the state while managing concerns about data access and customer privacy and maintaining a secure grid.[5] A suggestion was to develop two frameworks: the Cost-Benefit framework to weigh the costs/benefits of sharing grid information publicly to the ratepayer and the Risk-Benefit Framework to look at potential risk that would accompany information being shared on a particular DER asset. Additional conclusions included requiring the utility to create non-disclosure agreements when sharing private information and unblurring the host capacity analysis map on the utility website for more information on distribution line locations. Synapse argues that a lot of this information is needed by developers and that a potential bad actor would be able to obtain that information in different ways.[6] Other states should consider conducting similar studies and State Energy Offices may recommend that legislation be passed to fund such a study.

Example Legislative Activity

In 2020, there was some legislative activity related to cybersecurity in energy systems. According to NCSL, states considered over 35 measures in this space which was a significant drop from 2019 (30%). In 2021, 46 measures were considered related to cybersecurity of energy systems. Opportunities for legislation will vary state to state, but most are aware of the role the state government can and should play in protecting the electric grid. Still, there are concerns about a lack of financing options for utilities to protect against cyber threats.[7] There have been attempts by states to rectify this concern. For example, Maryland SB 810 was introduced in February 2022 to establish a Critical Infrastructure Cybersecurity Grant program to make cybersecurity improvements and add more staffing requirements to the Public Service Commission around cyber. The Commission would be required to have one or more staff dedicated to cybersecurity policy, strategy, auditing, and reporting.[8] While the bill was subsequently withdrawn, these remain potential avenues to strengthen cybersecurity.

Some of the most relevant enacted legislation from the last two years include:

- Alaska SB 123: required interconnected electric utilities to provide reliable operation of the interconnected transmission network by providing protection from cybersecurity incidents. The text defines these incidents as "a malicious act or suspicious event that disrupts or attempts to disrupt the security of data or the operation of programmable electronic devices and communication networks, including hardware and software that are essential to the reliable operation of the interconnected electric energy transmission network".[9]
- Colorado SB236: required utilities to plan for addressing cybersecurity risks in distribution planning.
- Kentucky SB 55: established a Blockchain Technology Working Group which would evaluate the feasibility of and efficacy of using blockchain technology to enhance critical infrastructure protections for the electric grid and other critical infrastructure systems. The Kentucky Public Service Commission is part of the working group as required by law.
- Georgia HB156: requires the Georgia Emergency Management Agency and Homeland Security Agency to receive reports from all government agencies and utilities on any cyber-attacks. If there is an information sharing prohibition federally, the information must be shared only when that is lifted or expired. Notification of the event must be conducted within two hours of first detecting the cyber-attack.
- North Dakota SB 2313: requires electric public utilities to report to the public service commission on their cybersecurity preparedness efforts including how they have assessed and improved their system security.
- Tennessee SB2282: requires that certain utilities prepare and implement a cyber security plan to provide for the protection of the utility's facilities from unauthorized use, alteration, ransom, or destruction of electronic data. This will be enforced by the Tennessee Public Utility Commission.

- Texas SB 2116: prohibits contracts with foreign-owned companies relating to energy and cybersecurity systems.
- Texas SB 475: (2019) Texas Electric Grid Security Council "composed of a governor's appointee, a member of the Public Utilities Commission and the chief executive officer of Electric Reliability Council of Texas — will be tasked with developing grid security standards, preparing for grid related security threats and amending the state emergency plan to ensure coordinated response and recovery efforts." Called the state's "first grid protection bill."
- Texas SB 936: (2019) Public utility commission is to contract w/ an entity to do basic best practices regarding cybersecurity, monitoring, outreach, etc.
- Utah HB 280: creates a Cybersecurity Commission with 24 members including a representative designated by the governor and a representative of the Public Service Commission. The Cybersecurity Commission will gather information on cybersecurity and establish guidelines and best practices related to multiple sectors including energy. The Utah Office of Energy Development offered support in the development of the legislation.
- Washington RCW 19.280.100: Section 2.g, requires: "(g) Include a high level discussion of how the electric utility is adapting cybersecurity and data privacy practices to the changing distribution system and the internet of things, including an assessment of the costs associated with ensuring customer privacy."

Conclusion

While discourse on the issue of cybersecurity protections for solar have been limited to non-existent, there are more and more opportunities under consideration regarding cybersecurity protections for the electric grid writ large. This is a critical time for State Energy Offices and PUCs to share their own lessons learned and information on the importance of targeting legislation to DERs as well. State Energy Offices, PUCs, and state legislatures are key players in gathering information, funding research projects, and putting protections in place that guard DERs from cyber threats and vulnerabilities and they should work together to put the best processes in place for utilities and developers to follow to safeguard solar and other DER projects. By putting standards and requirements in place for utilities on cybersecurity protections and reporting, it can help protect the system against attacks. Addressing these risks is not a simple process, but state legislatures can pass laws that support State Energy Offices and PUCs in identifying potential vulnerabilities or help the public after a cyber-attack that could lead to fuel shortages or blackouts.

References

1 National Conference of State Legislatures (NCSL, October 2019). Engagement Between Public Utility Commissions and State Legislatures. https://www.ncsl.org/research/energy/engagement-between-public-utility-commissions-and-state-legislatures.aspx

2 Shea, Daniel (January 2020). "Cybersecurity and the Electric Grid | The state role in protecting critical infrastructure." National Conference of State Legislatures. https://www.ncsl.org/research/energy/cybersecurity-and-the-electric-grid-the-state-role-in-protecting-critical-infrastructure.aspx

3 Ibid.

4 Texas Utilities Code 39.917 – Texas Electric Grid Security Council. LawServer. https://www.lawserver.com/law/state/texas/tx-codes/texas_utilities_code_39-917#:~:text=The%20Texas%20Electric%20Grid%20Security%20Council%20is%20established,Texas%20Electric%20Grid%20Security%20Council%20is%20composed%20of%3A

5 Synapse Energy Economics, Inc. Hosting Capacity Analysis and Distribution Grid Security in Minnesota. https://www.synapse-energy.com/hosting-capacity-analysis-and-distribution-grid-security-minnesota

6 Ibid.

7 Shea, Daniel (January 2020). "Cybersecurity and the Electric Grid | The state role in protecting critical infrastructure." National Conference of State Legislatures. https://www.ncsl.org/research/energy/cybersecurity-and-the-electric-grid-the-state-role-in-protecting-critical-infrastructure.aspx

8 Maryland State Legislature. 2022 Regular Session. Senate Bill 810. https://legiscan.com/MD/text/SB810/2022

9 The Alaska State Legislature. 31st Legislature. 2019-2020. Enrolled Senate Bill 123. https://www.akleg.gov/basis/Bill/Text/31?Hsid=SB0123Z


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