User Guide for CATSS Tools

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

NASEO
National Association of State Energy Officials

User Guide for CATSS Tools

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

Contents

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.

Background/Introduction

The Cybersecurity Advisory Team for State Solar (CATSS) project is an effort led by the National Association of State Energy Officials (NASEO) and the National Association of Regulatory Utility Commissioners (NARUC) to identify model solar cybersecurity programs and actions at the state level that can enhance the security of solar deployments. Supported by the U.S. Department of Energy's (DOE) Solar Technology Office (SETO), the CATSS project includes an Advisory Group, made up of representatives from state and federal agencies, utilities, and members of the solar industry, to inform the development of tools and technical assistance to support the effective, compatible solar cybersecurity strategies for State Energy Offices and Public Utility Commissions.

Over the course of two years, NASEO and NARUC conducted extensive research and stakeholder engagement to assess the needs of states as they pertain to solar cybersecurity. These needs were grouped into three categories: education, cost-recovery and valuation, and policy and regulatory guidance. Based on those needs, NASEO and NARUC developed ten tools—together hereafter referred to as "the toolkit"—which can serve as foundational educational resources for State Energy Offices and Public Utility Commissions seeking to mitigate cybersecurity risks and consequences in solar energy infrastructure, and support industry cybersecurity programs and other efforts. Through the Advisory Group, the project leveraged state, federal and private-sector expertise on cybersecurity, grid and photovoltaic (PV) to identify model solar cybersecurity programs and actions for states to take in partnership with utilities and the solar industry.

To guide the user of the toolkit developed under CATTS, this document provides a high-level overview of the issues which inspired the development of CATSS. It also provides an overview of the tools within the CATSS Toolkit, and basic instructions for intended users, including a suggested order of reading the tools.

Overview of Issues

The power grid in the U.S. is in the midst of historic, transformational change. Ambitious state and federal climate goals nationwide and federal legislation like the Infrastructure Investment and Jobs Act (IIJA) and the Inflation Reduction Act (IRA) is leading to the rapid adoption of clean and often distributed sources of energy. PV systems are among the technologies leading this transition. According to the Solar Energy Industry Association (SEIA), solar PV capacity in the U.S. reached 121.4 GWdc, enough to power 23.3 million American homes. Solar accounted for 46% of all new electricity-generating capacity added in the U.S. in 2021 and, for the third year in a row, solar has made up the largest share of new capacity.[1] The Energy Information Administration forecasts solar energy will provide 22% of U.S. total electricity generation by the year 2050.[2] Advances in technology and the adoption of operational and interoperability standards facilitate this growth.

Today's advanced PV systems play an active role in electric grid stabilization, reliability, and system-level energy efficiency via two-way communications between aggregators and grid operators, usually over the public internet. Yet, these benefits come with risks, particularly around the potential for cybersecurity attacks. To date, these concerns have not been fully addressed.

The Impetus for CATSS

The rapid growth and importance of solar energy has elevated the critical need among state-level decision makers to evaluate the potential cybersecurity implications of solar deployment and work with federal and private-sector stakeholders to mitigate those risks. Newer two-way communication technologies and remote grid support are revolutionizing how the grid operates, but also result in a system more exposed to cyber vulnerabilities.

Cybersecurity remains a constant and evolving threat for the energy sector writ large. While most cybersecurity mitigation efforts, studies, and technologies have focused on legacy assets and bulk power, less attention has been given to distributed energy resources (DER), including solar. Given the significant forecasted growth of solar (and other DERs) within future generation mixes, and the increasing reliance on solar assets to support critical facilities and functions, such as backup generation, it is only prudent that due attention be given to ensure that increasingly important solar infrastructure assets are developed and deployed with reasonable cybersecurity considerations. Further, state clean energy goals should be accompanied by proactive policies, programs, and regulations which ensure that new assets are secure and reliable.

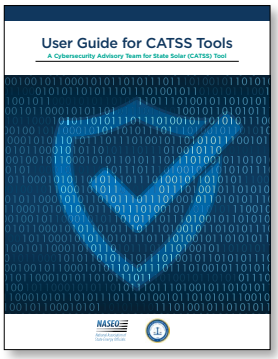
As public servants, subject matter experts, and stewards of state energy security and grid resilience planning and funding, states are appropriately positioned to lead and support cybersecurity mitigation programs, policies, and regulations in support of the aforementioned objectives. Through CATSS, NASEO and NARUC have sought to support states in proactively addressing cyber threats in solar infrastructure, though it is important to note that many of the lessons learned from CATSS are applicable to DERs in general.

Guidance to Use the Toolkit

The following disclaimer should be noted by readers up front and is listed in each of the CATSS tools:

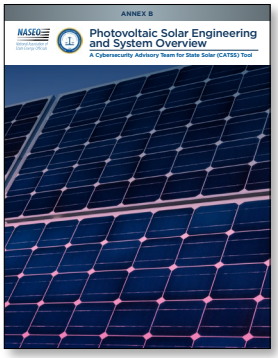
The CATSS Toolkit is designed to provide states with basic education on cybersecurity issues for solar and enable their efforts to support cybersecurity enhancements efforts for solar. Cybersecurity challenges for solar should not be viewed as unique. All electricity generation technologies are, to varying 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 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.

Suggested Order of Reading and Tool Overview



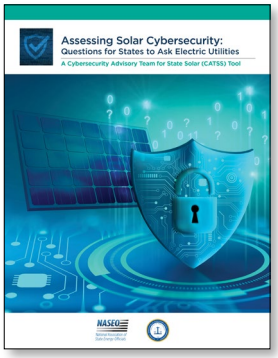
1. **User Guide (You Are Here!)**
   This tool provides context on the founding of the CATSS project and provides a user guide to the toolkit, including an outline of all tools and a suggested order of reading the tools.

   Tools 2-5 are education and risk-awareness resources, while tools 6-11 outline more approachable, practical, and entry-level actions that states can take to support cybersecurity for PV systems.



2. ***Photovoltaic Solar Engineering and System Overview***
   This tool depicts local PV components, interdependencies with the grid, and local two-way communication pathways. It identifies physical and virtual risks and delineates between PV and grid scale components. It provides readers with a fundamental overview of the most relevant and critical physical components and serves as a basic educational resource for readers. It is suggested as the second tool to review because it provides the reader with key terminology and basic risk information that is referenced in subsequent tools.

3. ***Standards Quick Guide***
   This tool contains a list of relevant standards developed or in development for the cybersecurity of solar energy resources. It outlines different types of standards, such as industry standards, enforceable regulations, and conceptual relevant cybersecurity studies. This resource should be viewed as an additional educational tool. Users may use this quick guide as a tool to enhance understanding of existing standards and for brainstorming new ideas to help states improve the cybersecurity of solar energy resources in their jurisdiction through innovative policy.



4. ***Assessing Solar Cybersecurity: Questions for States to Ask Electric Utilities***
   To help State Energy Officials and Public Utility Commissions 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, this tool outlines discussions prompts for these discussions. By using the questions in this tool states can explore aspects of utilities' cybersecurity risk management programs that target solar devices, systems, and communication pathways. Such discussions help states identify cybersecurity gaps and assist in emergency response planning, as well as general risk awareness.

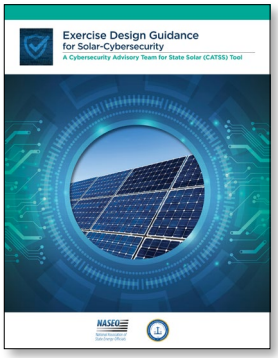
5. ***Hypothetical Solar Cyberattack Scenarios and Impacts***
This tool offers approachable, plausible scenarios of cyberattacks affecting PV assets and interconnected infrastructure. It may be used by State Energy Officials and Public Utility Commission Staff to educate themselves on the potential consequences of these scenarios and the practical, high-level actions that may be implemented now to mitigate future impacts. It highlights plausible consequences of inadequate cyber provisions for PV systems and offers potential state actions to alleviate the identified risks.

6. ***Decision Support Tool for Solar Energy Cybersecurity Policy and Regulation***
The Decision Support Tool helps users address four discrete challenges: (1) complex requirements of relevant codes and standards, (2) technical complexity of solar assets, (3) undefined cyber risk severity, and (4) unclear roles and responsibilities. Content includes an analysis of cyber vulnerability risks, a decision support resource for policymakers to mitigate cyber risks to solar PV systems, and background resources for informing policy development. A key component of this tool is the Probable Risk Assessment (PRA), based on established, formal variables, models, and consequences, which helps users understand the determined risk and assigned ownership of the physical components listed in the *Photovoltaic Solar Engineering and System Overview*. It helps states draw logical lines between vulnerabilities and mitigative solutions, of which some have been further detailed as CATSS tools.

7. ***Case Studies and Model Guidance for Establishing Solar Cybersecurity Working Groups***
This tool outlines actions that states can take to establish state-level working groups, which can be a critical first step to establishing state cybersecurity programs and efforts to support cybersecurity in DERs. Specifically, these working groups can lead the development of cybersecurity task forces focused around DERs, formal recommendations for policy makers and regulators, and the creation of a response strategies and plans for cybersecurity impacts or incidents in solar photovoltaic systems.

8. ***Cybersecurity and the Solar Workforce: Considerations for States***
This tool identifies workforce competencies and requisite skill sets for the solar cybersecurity workforce, and highlights tactics that State Energy Offices and Public Utility Commissions can employ to amplify current solar workforce training initiatives and build partnerships that help develop this workforce. It highlights policies and pathways that can foster the growth of solar cybersecurity workforce. Critically, it also identifies internal solar cyber expertise that State Energy Offices and Public Utility Commissions should consider to further develop their roles and responsibilities in this space.

9. ***Cybersecurity Considerations for State Procurement of Solar Assets***
This tool provides an overview of existing procurement programs and example language that prioritizes cybersecurity language and references that can readily be applied to state solar cybersecurity practices. The tool also identifies sample language for procurement agreements, contracts, and grants which can serve as lower entry points for state officials interested in pursuing this subject matter more immediately. As this approach may be novel for many states, the information therein should be considered as a model only. The programs and example language included are not exhaustive and should be evaluated in accordance with state processes and policies.



10. ***Exercise Design Guidance for Solar Cybersecurity***
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 scenarios. Exercise practitioners, planners, or facilitators interested in exploring solar cybersecurity incident response, preparedness, recovery, or mitigation may find this a valuable resource. This is 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 may be referenced in conjunction with the *Hypothetical Solar Cyberattack Scenarios and Impacts* tool within the CATSS Toolkit.

11. ***State Legislative Options to Enhance Solar Cybersecurity***
One of the mitigative solutions to solar cybersecurity risks is to proactively develop legislation which can 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. This tool outlines relevant state cybersecurity legislation examples which can apply to solar cybersecurity and can serve as frameworks for future legislation by states seeking legislative options to help mitigate these risks.

The Role of Technology and Standards

Interconnecting solar and other DERs with the electric distribution grid has not always been easy. Early on, the variable nature of solar raised grid reliability concerns. The variety of manufacturer-specific functionality in PV power electronics (i.e., inverters) caused interconnection challenges for utilities and, conversely, utility-specific interconnection requirements burdened DER developers. That changed in 2003 with the release of IEEE Standard 1547,[3] which established detailed technical rules for the interconnection of DERs with the grid. The result was a wave of DER development, which, over time, sparked newer grid stability and reliability concerns. This time, advances in inverter technology provided answers.

The introduction of smart inverters[4] has allowed solar to play a more active role in distribution system stabilization, power system reliability, and overall energy efficiency, accelerating increasing levels of adoption. Smart inverters perform functions that can autonomously contribute to grid support such as dynamic reactive/real power support and voltage and frequency ride-through. They also are equipped with technology that enables two-way communication for control and monitoring.

In 2018, IEEE released an update to Standard 1547[5] to address these new grid-related inverter capabilities, requiring DERs to be capable of performing specific grid support functions. Before 1547-2018, some state energy policy makers started developing their own requirements because of the significant amount of DERs already feeding into their utility grids. For example, in June 2016, the California Public Utilities Commission (CPUC) issued Rule 21,[6] requiring smart inverters be managed by utilities or DER operators/aggregators for grid reliability purposes.

Standard 1547-2018 and interconnection rules such as California Rule 21 enhance the safety, reliability, power quality, and other operational aspects of power systems, particularly those with high penetrations of DER systems. As these standards have changed, state regulators have also begun modifying their rules that define the administrative and technical requirements for connecting DER, including solar, with the grid. The National Renewable Energy Laboratory (NREL) reports that most public utility commissions have adopted IEEE 1547 in the development of their interconnection rules.[7] In 2020, NARUC passed a resolution encouraging state utility regulators to adopt the updated IEEE Standard 1547-2018 into their interconnection rules.[8]

The Cybersecurity Challenge

As the use of solar and other DER expands, the electric grid is increasingly comprised of independently owned, interconnected cyber-physical devices that rely on two-way data communications and power flows to operate safely and reliably. The inherently sophisticated communications capabilities built into each of those devices expose potential cyber security vulnerabilities. For example, to perform their grid-enabled functions, smart inverters communicate with DER aggregators and utility operators, typically over the internet. A cyberattack aimed at disrupting or manipulating DER communications at any point along the communications path could affect electricity delivery on the grid.[9] Similarly, software vulnerabilities could allow malicious actors to gain access to a smart inverter and change settings that affect the voltage or electrical current delivered to the grid. With the increasing prevalence of DER devices, common-mode vulnerabilities run the risk of simultaneously disconnecting massive quantities of generation, which could lead to power disruption.[10]

Although updating is underway, current versions of IEEE 1547-2018 and CA Rule 21 offer little guidance on cybersecurity, opting to focus on operational and interoperability requirements instead. Nonetheless, the security of the electric grid now and in the future remains a high priority for utilities, the solar industry, and state and federal agencies alike. The desired end state, suggest researchers from Sandia National Laboratory, is one where grid operators, PV owners, and aggregators communicate with interoperable, secure-by-design systems using safe, resilient networks with high availability, data integrity, and confidentiality.[11] Standards alone, however, may not be enough to achieve this end state amid rapidly evolving technology advances and increasingly sophisticated cyber threats.

Cybersecurity Practices for Solar

A comprehensive approach is necessary to secure the electric grid, inclusive of interconnected solar systems, from potentially damaging cyber incidents. Conducting end-to-end risk assessments, employing defense-in-depth strategies, following good cyber security hygiene, and addressing supply chain risks across the DER ecosystem is essential – for both utilities and solar providers. NIST, DOE, and others have produced invaluable cybersecurity best practice guides for cybersecurity risk management generally, and for DER specifically.[12,13,14] The table below captures some best practice guidance.

Sample Best Practices for Solar Cybersecurity[15]

Industry Best Practices **(Grid Operators and Aggregators)**	- Implement risk management plan - Implement cyber security maintenance and hygiene practices - Use role-based access controls - Implement defense-in-depth approaches to cyber security	- Implement situational awareness and intrusion detection systems at the grid operator and aggregator levels - Conduct continuous security monitoring with warning and alarm systems	- Document and eradicate intrusion footholds - Design and implement response, recovery, and contingency plans - Work with government to conduct investigations - Document & share lessons learned
Industry Best Practices **(PV Industry)**	- Harden PV inverters through aggressive in-house and external testing - Create patching release methodology and assign personnel to rapidly respond to new vulnerabilities	- Establish anti-tamper mechanisms - Participate in information sharing programs to determine if vulnerabilities detected in other products or networks affect PV equipment	- Design PV equipment to fail in predictable, safe manner - Maintain trusted gold master firmware for re-flashing equipment after cyber attack - Respond to newfound vulnerabilities with patches

References

1 Solar Energy Industries Association (June 8, 2023). *U.S. Solar Market Insight*. https://www.seia.org/us-solar-market insight.

2 U.S. Energy Information Administration (March 3, 2022). *Annual Energy Outlook 2022*. https://www.eia.gov/outlooks/aeo/narrative/electricity/sub-topic-01.php.

3 Institute of Electrical and Electronic Engineers (July 28, 2003). *IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems,* in *IEEE Std 1547-2003* , vol., no., pp.1-28, doi: 10.1109/IEEESTD.2003.94285. https://ieeexplore.ieee.org/document/1225051

4 The Association of Edison Illuminating Companies (October 2018). *Enabling Smart Inverters for Distribution Grid Services*. https://www.pge.com/pge_global/common/pdfs/about-pge/environment/what-we-are-doing/electric-program-investment-charge/Joint-IOU-SI-White-Paper.pdf

5 Institute of Electrical and Electronic Engineers (April 6, 2018). *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*. in *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)* , vol., no., pp.1-138, doi: 10.1109/IEEESTD.2018.8332112. https://ieeexplore.ieee.org/document/8332112

6 California Public Utilities Commission (2017). Rule 21 Interconnection. https://www.cpuc.ca.gov/Rule21/

7 Basso, Thomas (December 2014). *IEEE 1547 and 2030 Standards for Distributed Energy Resources Interconnection and Interoperability with the Electricity Grid*. National Renewable Energy Laboratory, https://www.nrel.gov/docs/fy15osti/63157.pdf

8 National Association of Regulatory Utility Commissioners (February 2020). *Resolutions Proposed for Consideration at the 2020 Winter Policy Summit of the National Association of Regulatory Utility Commissioners.* https://pubs.naruc.org/pub/49A6A319-155D-0A36-3140-EFAD21E48B50

9 McCarthy, James, et al. (February 2022). *Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/1800-32/final

10 Carter, Cedric, et al. (2017) *Cyber Security Primer for DER Vendors Aggregators and Grid Operators*. Sandia National Laboratory. U.S. Department of Energy Office of Scientific and Technical Information. https://doi.org/10.2172/1761987. https://www.osti.gov/servlets/purl/1761987.

11 Johnson, Jay Tillay (2017). *Roadmap for Photovoltaic Cyber Security*. Sandia National Laboratory. U.S. Department of Energy Office of Scientific and Technical Information. https://doi.org/10.2172/1782667. https://www.osti.gov/servlets/purl/1782667.

12 National Institute of Standards and Technology (April 23, 2023). *Cybersecurity Framework*. https://www.nist.gov/cyberframework

13 U.S. Department of Energy. *Cybersecurity Capability Maturity Model*. Office of Cybersecurity, Energy Security, and Emergency Response. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

14 McCarthy, James, et al. (February 2022). *Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/1800-32/final

15 Carter, Cedric, et al. (2017) *Cyber Security Primer for DER Vendors Aggregators and Grid Operators*. Sandia National Laboratory. U.S. Department of Energy Office of Scientific and Technical Information. https://doi.org/10.2172/1761987. https://www.osti.gov/servlets/purl/1761987.

16 Department of Homeland Security. “Safeguarding and Securing Cyberspace”. *Cybersecurity Assessment Tools.* https://www.dhs.gov/xlibrary/assets/pso-safeguarding-and-securing-cyberspace.pdf


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