Cybersecurity Advisory Team for State Solar (CATSS)
Project Roadmap[1]
Version 1.0

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 mitigate cybersecurity risks and consequences in solar energy developments. With support from the United States Department of Energy Solar Energy Technologies Office (US DOE SETO), the project leverages state, federal and private-sector expertise on cybersecurity, grid and photovoltaic to identify model solar-cybersecurity programs and actions for states to take in partnership with utilities and the solar industry.

Based on extensive research and input from NASEO and NARUC members on how to inform, enable, and support improved cybersecurity in photovoltaic (PV) systems, the two organizations developed this roadmap as a menu of options to further support state considerations of solar cybersecurity. As relevant, tools and resources will touch on cybersecurity aspects of distributed energy resources (DER) in general. These options are outlined in three categories, which can happen simultaneously or in a different order. The list of options is not exhaustive, and inclusion of potential tools does not indicate an endorsement of NASEO, NARUC, or any of the CATSS Advisory or Control Group members. The document is not static, but rather a "living document." NASEO and NARUC might develop some but not all of the tools outlined.

Educate State Energy Offices and Public Utility Commissions

The primary objective will be to provide State Energy Offices and Public Utility Commissions with tools to develop a baseline knowledge of solar cybersecurity to inform their decision-making for relevant policies and programs in the future. NASEO and NARUC will identify relevant existing resources and develop original materials covering topics not included in existing materials.

- ***Resource Library***
  The resource library will provide an overview of material on solar cybersecurity issues, including the relevancy to State Energy Offices and Public Utility Commissions, and serves as a guide to the sequence and progression of the included literature review and discussion of existing cybersecurity maturity models.

- ***Glossary of Key Terms***
  Glossary of relevant cybersecurity and PV terms to provide understanding of commonly used terms.

- ***Engineering and System Overview of PV Systems***
  A simple schematic to understand the cyber components of PV systems (islanded vs. grid-following), batteries, EVs, other DERs, aggregators, interconnections, etc.

- ***Risk Ownership Framework***
  Overview of information needed to assess and determine risk.

Create Tools for State Organizations to Convene and Strategize

Tools will focus on providing states with resources to delve deeper into roles and responsibilities as well as understanding objectives and consequences of potential solar cybersecurity risks and mitigative actions. This will include suggested guidance and resources for states to convene stakeholders, which can assist state agencies in collecting relevant information on solar cyber security issues.

- ***Consequence Forecasting Guidance***
  Develop risk scenarios for solar cybersecurity depending on solar generation in the next decade, aimed to highlight potential consequences of inadequate solar cyber provisions, and determine state objectives.

- ***Objective Mapping Guidance:***
  Guidance on what efforts exist already that states can support; what new issues can/should states address; and what complementary, supportive, or umbrella policies exists?

- ***Organizational Role Chart Template***
  Guidance to determine state-specific and regional responsibilities based on objective(s) pursued, regulatory/policy environment, and tool(s) being used.

- ***Stakeholder Engagement Strategy***
  Strategy on how to best engage stakeholders in the process of developing a response to solar cybersecurity concerns.

Provide Solution Examples to States

The primary objective will be to provide states with policy examples that could be included in their unique and respective policies or programs. Tools will focus on which actions might be performed by states to address concerns raised by stakeholders so that solutions can be "mapped" to specific vulnerabilities or challenges. NASEO and NARUC will leverage existing tools from other sectors for reference and provide them as potential models for adaptation.

Menu of Potential Actions

Policy Tools

- Model guidance to establish state-level homeland security and smart inverter working groups.
- Build on the NARUC Publication *Understanding Cybersecurity Preparedness: Questions for Utilities* by formulating additional questions for state agencies to ask utilities and various stakeholders on an ongoing basis specifically on solar cybersecurity.
- Examples of state legislative options.

Decision Support and Assessment Tools

- DER Criticality Checklist
- Solar cybersecurity requirements cost benefit analysis guidance.
- Access to Qualified Components List (QPL)

Programmatic and Project Supplements/Templates

- Example language for procurement, grant contracts, RFPs.
- Exercise guidance on how to integrate solar cybersecurity issues and stakeholders (i.e., solar installers and manufactures) into energy emergency planning and exercising.
- Workforce support documents for State Energy Offices and Public Utility Commissions (e.g., a list of skills, needs, functions, and competencies).

---

[1] This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office 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.