DISCLAIMER

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. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

Final Technical Report (FTR)

Cover Page

a. *Federal Agency*	Department of Energy	
b. *Award Number*	DE-EE0009004	
c. *Project Title*	Enabling Solar Cybersecurity Solutions Through State Energy Office and Public Utility Commission Engagement with Private Sector Partners	
d. *Recipient Organization*	National Association of State Energy Officials (NASEO)	
e. *Project Period*	*Start:* 03/01/2020	*End:* 2/28/2025
f. *Principal Investigator (PI)*	Kirsten Verclas Senior Managing Director, Electricity and Energy Security kverclas@naseo.org 703.299.8800 x125	
g. *Business Contact (BC)*	Shemika Spencer Budget and Compliance Officer sspencer@naseo.org 703.299.8800 x115	

K. Verclas July 7, 2025

Signature of Certifying Official *Date*

By signing this report, I certify to the best of my knowledge and belief that the report is true, complete, and accurate. I am aware that any false, fictitious, or fraudulent information, misrepresentations, half-truths, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise. (U.S. Code Title 18, Section 1001, Section 287 and Title 31, Sections 3729-3730). I further understand and agree that the information contained in this report are material to Federal agency's funding decisions and I have any ongoing responsibility to promptly update the report within the time frames stated in the terms and conditions of the above referenced Award, to ensure that my responses remain accurate and complete.

Acknowledgement

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) Solar Energy Technologies Office (SETO) under the Solar Energy Technologies Office Fiscal Year 2019 Funding Program Award Number DE-EE0009004.

Disclaimer

Executive Summary

Between 2020 and 2025, NASEO, together with the National Association of Regulatory Utility Commissioners (NARUC) established and managed the *Enabling Solar Cybersecurity Solutions Through State Energy Office and Public Utility Commission Engagement with Private Sector Partners* project, later informally retitled and recognized as the *Cybersecurity Advisory Team for State Solar* (CATSS). This effort convened State Energy Offices, Public Utility Commissions, and critical private sector and federal partners to inform the development of solar cybersecurity education and action-oriented resources for states. As policy leaders, as well as designers and implementers of solar, cybersecurity, and energy security programs, State Energy Offices were well-suited to support this project involving all three subjects.

The goal of CATSS was to enable state decision-makers to enhance the cybersecurity of photovoltaic (PV) solar systems owned by a variety of stakeholders within their jurisdictions. The project sought to provide state decision-makers with the education, tools, and access to a nationwide network of technical assistance in the form of a collection of subject matter expert-informed resources and working groups. The engagement, education, and information-sharing was designed to:

- Develop actionable solar cybersecurity strategies and roadmaps;
- Facilitate the creation of stronger intra- and interstate relationships and stakeholder communities; and
- Create collaborative frameworks and model approaches that could be formalized in state policy and regulation and easily replicated by other states.

The core element of CATSS was its Solar Cybersecurity Advisory Group (SCAG), which consisted of a dedicated group of State Energy Office and Public Utility Commission staff, a wide variety of energy industry members, and key federal and academic partners. Over the course of three years, the SCAG was able to comprehensively inform the development of educational resources and tools that reflected priorities, interests, and challenges of all stakeholders, which helped to develop an inclusive and approachable community of practice and enabled easy engagement among stakeholders.

Overall, CATSS has enabled (and continues to enable) more cyber-secure generation assets are added to the grid in support of reliability, resource adequacy, and security objectives of states, industry, and the federal government. The key outcomes of CATSS can be organized into the following three categories:

1. **Incorporation of CATSS Content into Formal State Programs, Projects, and Policies –** Several states and partners directly leveraged or referenced CATSS tools in the development of their own resources, projects, plans, and policies.
2. **Knowledge Transfer –** CATSS enabled the sharing of insight and knowledge from technical experts to policy and regulatory staff, and vice versa. CATSS thrived in helping stakeholders from diverse backgrounds and professions translate technical information into policy and programmatic decisions, clarify state and private sector needs, and harmonize understanding of solar cybersecurity issues across states. Additionally, CATSS facilitated knowledge

transfer from more cyber-mature states and industry experts to novice entities, greatly accelerating their learning curve.

3. **Integration of CATSS Findings and Priorities into State and NASEO Programming –** CATSS findings and education have become foundational for all state members of the NASEO Energy Security Committee and have laid the foundation for key new developments of NARUC's Center for Best Practices. Both of their active energy security-focused working groups—the NASEO Energy Security Committee and NARUC Subcommittee on Critical Infrastructure, respectively—continue to share best practices on solar cybersecurity. Because CATSS engaged a wide and diverse stakeholder group, and because the project's period of performance overlapped with new programs, the findings of CATSS were able to inform other projects' priorities, designs, and implementation strategies, which highlighted the compounding benefits of the subject matter.

The CATSS project team adapted to state and partner feedback, staff changes, and the COVID-19 pandemic, which inhibited in-person meetings during the critical development and kickoff stage of the project. Despite these challenges, the findings and principles of CATSS will have lasting impact because of the recognition and incorporation of its findings into formal state and CATSS stakeholder plans, the development of an active and healthy community of practice, and the continuation of CATSS findings and work by other entities. Thanks to initiatives from the U.S. Department of Energy, solar cybersecurity, and local energy asset cybersecurity, generally, has become a fundamental element of state energy security programming.

Table of Contents

Background

The rapid growth of solar energy elevated a critical need among state-level decision makers to evaluate the potential cybersecurity implications of solar deployment and to provide feedback from state officials to the U.S. Department of Energy (DOE) and private sector researchers. Further, new technologies capable of enabling two-way communication and remote grid support have revolutionized the way the grid is operated, but this rapid increase in grid-connected devices and technology has created a system in which grid operators and consumers are potentially more vulnerable to cyber threats.

NASEO and NARUC recognized that states are in an ideal position to address these issues by facilitating and implementing plans, policies, and procedures pertaining to solar cybersecurity within their respective jurisdictions and purviews. There exist baseline best practices that all states can help implement form a top-down approach. Conversely, unique lessons learned from policy and program implementation from individual states can be elevated and shared with peers form a practical, bottom-up perspective. All State Energy Offices run programs that support energy security, facilitate deployment and installation of all types of energy resources, and enable the implementation of new technologies supporting these efforts. As such, many State Energy Offices determined that cybersecurity considerations needed to be provided for the installation, procurement, operation, monitoring, and management of all new energy resources added to the grid, including solar technologies and other local assets.

State Energy Offices also lead the development and maintenance of State Energy Security Plans (SESPs), which encapsulate relevant state energy profile information, state risk assessment and risk mitigation approaches and strategies, and outline state cybersecurity strategies, among other critical content. CATSS objectives and outcomes aligned with those identified by states and ultimately helped many states fulfill the cybersecurity requirements of the SESP.

NASEO, NARUC, State Energy Offices, and Public Utility Commissions have been extensively involved in cybersecurity preparedness and response based on national cybersecurity strategies, state legislative directives, and state energy reliability policy priorities. Much of this work is done in partnership with DOE's Office of Electricity (OE), DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and alongside energy industry members. This work increasingly focused on mitigating the cyber risks and challenges posed by distributed energy resources and local assets.

Given the increased interest and focus on solar cybersecurity and awareness of vulnerabilities, NASEO created the project: *Enabling Solar Cybersecurity Solutions Through State Energy Office and Public Utility Commission Engagement with Private Sector Partners*, later informally retitled as the *Cybersecurity Advisory Team for State Solar (CATSS*). This project leveraged State Energy Officials, Public Regulatory Commissioners and their staff, and key industry, government, manufacturing, and other entities to form the advisory (SCAG or AG) and control (SCG or CG) groups that

developed a suite of resources that addressed the above barriers and enhanced the cybersecurity of solar energy infrastructure at the state level. The SCAG offered strategic guidance and stakeholder perspectives, while the SCG provided structured feedback, piloted resources, and validated the value, practicality, and effectiveness of the toolkit components.

Throughout the duration of CATSS, the project team relied heavily on literature, concepts, and experts in:

- **Energy Resilience Planning**
- **Emergency Response**
- **Energy Policy**
- **Energy Regulation**
- **Industrial Control Systems Engineering**
- **Cybersecurity and Information Security**
- **Academia**
- **Infrastructure Owners and Operators**

Significant Accomplishments and Conclusions:

CATSS has enabled (and continues to enable) more cyber-secure generation assets are added to the grid in support of reliability, resource adequacy, and security objectives of states, industry, and the federal government.

This outcome exceeded the ultimate goal of this project to identify and address challenges, priorities, and mitigative actions for State Energy Offices and Public Utility Commissions in addressing cybersecurity issues associated with solar deployment through a variety of end-users – investor- and consumer-owned utilities, commercial and institutional entities, consumers – and enable critical strategies and solution pathways for state decision-makers to enhance the security of solar systems. State Energy Offices now have a multidisciplinary cache of specific resources to inform their respective energy security and cybersecurity practices.

CATSS successfully met and exceeded this explicit objective, and throughout the natural course of the period of performance, addressed other issues raised by state, industry, and federal stakeholders. Overall, CATSS has informed state policy and programs to enable more abundant and more secure assets to be added to the grid.

CATSS helped to advance new concepts and precedents that support best practices in state solar cybersecurity planning and preparedness. Through regular convenings and deliberate, novel research, CATSS advisory group members emerged as leaders in this space, helping inform one another, federal agencies, private sector representatives, and other states on ways to best coordinate and plan with industry and federal partners on solar cybersecurity issues, and develop meaningful policies, programs, and procedures

to prepare for and respond to solar cybersecurity incidents, and to enable additional energy assets to be securely connected to the grid. CATSS led to the development of reports and resources (see "Products" section below), and helped to inform partner efforts, resources, and events. CATSS is ultimately responsible for solar cybersecurity being more deliberately and formally addressed by states and helped create a more robust and diverse community of practice among state, industry, and federal partners.

Specifically, CATSS outcomes can be summarized into three categories, listed as follows:

Incorporation of CATSS Content into Formal State Programs, Projects, and Policies

CATSS tools, discussions held during CATSS meetings, and external engagements all enabled an awareness of solar cybersecurity vulnerabilities in during State Energy Security Plan updates and formalization of novel processes. Most notably, CATSS tools and findings directly informed several Governor-certified and/or DOE-approved State Energy Security Plans. One specific example is the Massachusetts State Energy Security Plan. This is a sensitive and not publicly available plan and as such is not available for direct reference or quotation.

Multiple state members shared that they had incorporated several of the CATSS Focus Interview Questions into questions that it asks utilities during yearly, informal security meetings. The incorporation of solar-cybersecurity specific questions is a strong and demonstrable indicator of the value that state energy officials and regulators give to solar cybersecurity and to the value of CATSS. Specifically, the Virgina Department of Energy, Missouri Department of Natural Resources (State Energy Office), Minnesota Department of Commerce (State Energy Office), and the Energy Division of the Washington State Department of Commerce (State Energy Office) all leveraged CATSS *Interview Questions for Utilities* and *Hypothetical Solar Cyberattack Scenarios and Impacts* during the development of their cybersecurity sections as part of their state energy security plan working groups.

Lastly, the content from CATSS Cybersecurity Consideration for State Procurement of Solar Assets was leveraged in the development of Idaho National Laboratory's own procurement guidance, titled Securing Digital Energy Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance.

Knowledge Transfer

CATSS also enabled knowledge transfer from state officials and technical experts who had existing solar cybersecurity experience to CATSS participants who did not. This has enhanced the "bottom line" of solar-cybersecurity education among states. For example, California government officials (e.g., from the California Energy Commission and California Public Utilities Commission) have been involved in state initiatives to address solar cybersecurity through the formation of a state cybersecurity standards working group. These officials were connected and prompted to share lessons learned from their own processes with their counterparts in states who do not yet have, but are interested

in, forming similar working groups. These conversations provide informal ways of disseminating lessons learned and promoting a community of practice. State Energy Security Working groups led by State Energy Offices, including in Virginia, Washington, and Pennsylvania, have expanded the scope of their cybersecurity activities to include solar and local asset cybersecurity with the technical assistance provided by CATSS. Many of these states rely on peers from states with more technical maturity to help inform their planning and approach. NASEO continues to help facilitate such information-sharing through programming and ad hoc requests.

Integration of CATSS Findings and Priorities into State Programming
CATSS received significant additional interest in the application of the final tools as states developed new energy programs. State Energy Offices have substantial responsibilities to help with the deployment of energy assets and technologies, including solar systems and local energy assets generally. With growing cybersecurity concerns and requirements, states will need to deliberately consider cybersecurity concerns for solar systems. This new, but expected, task highlights how CATSS has indeed been a proactive and crucial project.

NASEO has integrated CATSS and solar cybersecurity, broadly, into several of our national and regional meetings, including the NASEO Annual Meeting, annual NASEO Energy Policy Outlook Conference, and annual Regional Meetings. The two large national meetings (NASEO Annual Meeting and annual NASEO Energy Policy Outlook Conference) brought together State Energy Office Directors and key personnel, private industry, and federal officials to discuss and strategize on the latest energy policies and programs. NASEO also hosts annual Regional Meetings for each of its six regions. The agendas for each regional meeting align with the specific priorities of that region.

- In October 2023, the CATSS project team presented during a breakout session during the 2023 NASEO Annual Meeting in Portland, OR, alongside a SCAG member from Schneider Electric.
- In April 2024, at the request of the Board of Directors Western Regional Representatives the CATSS project team participated in a discussion among Western State Energy Office Directors focused on the cybersecurity of local energy assets and actions that states can take in partnership with utilities and industry to mitigate local energy assets cybersecurity risks.
- In September 2023 and April 2024, the CATSS project team presented on the CATSS toolkit at the NARUC Cybersecurity Training with each event having over fifty Public Utility Commissioners and staff, State Energy Security Officials, federal and private sector partners.
- In 2024, the CATSS Cybersecurity Consideration for State Procurement of Solar Assets tool was used to inform the development of an Electric Vehicle (EV) procurement tool utilized by State Energy Offices and State Departments of Transportation, which informed state-wide transportation programs including. This resource was directly adopted by the state of Illinois and referenced by other state transportation leads.

Expansion of State Energy Officials and Regulatory Officials Cybersecurity and Industry Networks

Throughout the development of CATSS tools, both in-person and virtual engagements with the SCAG and SCG through educational meetings, the State Solar Cybersecurity Workshop, and a discussion-based tabletop exercise enabled State Energy Officials and Regulatory Officials to connect with industry partners and cybersecurity experts. The expansion of these cybersecurity networks represented a strategic effort to strengthen the resilience of the U.S. energy sector against evolving cyber threats. By fostering collaboration among state-level energy policymakers, utility regulators, and cybersecurity professionals, the networks improved information sharing, aligned best practices, and enhanced incident response coordination. The numerous relationships and connections that were formed and nurtured throughout the duration of the CATSS project are expected to endure well beyond its conclusion.

Project Objectives and Tasks Breakdown

The project was designed to engage state, federal and private cybersecurity, grid, and photovoltaic (PV) expertise to identify model state programs and actions – in partnership with utilities and industry – to mitigate PV-related cybersecurity risks. In the beginning of the project, state and federal leaders were just beginning to evaluate the vulnerabilities and cybersecurity concerns associated with the deployment of these and other local energy asset systems, and the project filled a void by to convening state regulatory and policy leaders and industry and cybersecurity experts.

The project sought to provide these stakeholders with the education, tools, and access to a nationwide network of technical assistance expertise in the form of a collection of resources, hereby known as “the toolkit.” Not only did this engagement, education, and information sharing result in the development of actionable solar cybersecurity strategies and roadmaps; it also facilitated the creation of stronger intra- and interstate relationships and stakeholder communities and created collaborative frameworks and model approaches that can be easily replicated by other states.

Objectives Budget Period 1

- Establish a Multi-Stakeholder Solar Cybersecurity Advisory Group (SCAG) to Assess Challenges and Opportunities
- Complete a Literature Review, Needs Assessment, and Roadmap

Objectives Budget Period 2

- Develop the Comprehensive Solar Cybersecurity Solutions Toolkit
- Create key contact list and Communication Strategy

Objectives Budget Period 3

- Disseminate and conduct outreach of Toolkit through Solar Cybersecurity Education Series
- Establish State Energy Security Feedback Loop between State Energy Directors, Public Utility Commissioners, and Federal Partners and create a sustainable network of cybersecurity experts in local government.

The Go/No-Go (GNG) decision points whose achievement enabled the project to progress from one budget period to the next included:

Budget Period 1:

- **GNG-1A:** External reviews of literature reviews sent to DOE.
- **GNG-1B:** External reviews of needs assessment sent to DOE.
- **GNG-1C:** Partner letters of intent sent to and reviewed with DOE.
- **GNG-1D:** Toolkit Roadmap documenting the results of needs assessment, feedback from experts, and stakeholders, and the proposed toolkit structure presented to DOE.

Budget Period 2:

- **GNG-2A:** Final Risk Assessment/ Maturity Models and feedback from 3 SCG members sent to DOE.
- **GNG-2B:** Final Solar Cybersecurity Options Analysis and feedback from 3 SCG members sent to DOE.
- **GNG-2C:** Finalized summary and feedback sent to DOE on substantive engagement with 3 external working groups.
- **GNG-2D**: 20 letters of Support sent to and reviewed with DOE.

Project Results and Discussion

This section includes a high-level comparison of project outcomes, comparing realized results against anticipated award milestones. It is structured at the task-level of the SOPO and Technical Work Plan, with subtasks providing support for claimed progress.

Budget Period 1

Task 1.0: COMPLETE - Setup of Advisory and Communications Structures and Determination of State Partners
The planned activities for Task 1 included actions to establish a Multi-Stakeholder Solar Cybersecurity Advisory Group (SCAG) to Assess Challenges and Opportunities.

Subtask 1.1 and Subtask 1.2: COMPLETE – Identify SCAG and Host In-Person[1] Kickoff Meeting, Assign SCAG Responsibilities through a Charter and Develop Quarterly Call Schedule. These first two subtasks involved the recruitment and kick-off, and formalizing the structure of the SCAG, which was completed in October 2020. During this reporting period, NASEO and NARUC conducted targeted outreach to recruit interested State Energy Officials, Public Regulatory Commissioners and their staff, and key industry, government, manufacturing, and other entities to comprise the advisory group and control group. The SCAG was initially comprised of 22 state participants from 12 states, and 21 non-state entities. The SCAG first met virtually on September 8, 2020, for a kick-off meeting which included a discussion of project

[1] All in-person meetings were changed to virtual due to the COVID-19 pandemic.

objectives and strategies, and during which the CATSS team reviewed project objectives, timeline, advisory group expectations, and project background. The meeting included a robust attendance and highlighted different perspectives on solar cybersecurity issues, including policy, regulatory, and business priorities and concerns. The final list of SCAG entities is included on the NASEO website. On September 29, 2020, NASEO and NARUC held an inaugural meeting for the Advisory Group alone (i.e., without the Control Group), during which objectives, call schedules, and the charter were discussed. NASEO and NARUC completed the charter by which the SCAG would operate. The charter included general objectives, expected project timeline, engagement frequency, NASEO and NARUC roles, and expectations of the SCAG. The charter also stipulated that the use of all tools created by CATSS would be up to the discretion of individual states.

Subtask 1.3: COMPLETE – Publicize Project through Press Release. NASEO and NARUC conducted a coordinated press release from both NASEO and NARUC to provide early publication of the project as well as socialization of the project and possibly garner additional outside interest. Following this general announcement, NASEO and NARUC received over twenty emails from partners and affiliates indicating their interest in the project and volunteering to participate. NASEO expected and did receive interest from organizations such as the Solar Energy Industry Association (SEIA) and the North American Electricity Reliability Corporation (NERC), but also a number of smaller cybersecurity firms and unaffiliated individuals. NASEO has since added these organizations and individuals to the list of participants for possible engagement. NASEO also reached out specifically to Underwriters Lab, LLC (UL), which had provided an initial letter of support for the project during the original application period at the request of SETO.

Task 2.0: COMPLETE – Conduct Needs Assessment and Review All Existing Publications, Frameworks, and Other Resources to Determine Gaps and to Reduce Duplicate Efforts to Develop Project Roadmap

The planned activities for Task 2 included several actions to develop a baseline needs assessment and literature review, which would lead to a more detailed and better-informed project roadmap and the identification of the necessary tools that CATSS would need to develop.

Subtask 2.1: COMPLETE – Conduct Literature Review. NASEO and NARUC completed the literature review and developed a public-facing Literature Review for the CATSS website, which provided NASEO and NARUC members with an overview of foundational resources and more technical reports. Importantly, the literature review put the resources into context and allowed State Energy Offices and Public Utility Commission staff to look at resources that were relevant to them and matched their expertise as well as highlighted key lessons from each resource for the project. The Literature Review was reviewed by the SCAG and NASEO and NARUC also shared the needs assessments with the NASEO Energy Security Committee and the NARUC Critical Infrastructure Committee for feedback.

Subtask 2.2: COMPLETE – Conduct Needs Assessment and Develop Project Roadmap.. Through voluntary feedback forms from NASEO and NARUC members and feedback from the SCAG, NASEO and NARUC conducted a needs assessment in development of a project roadmap. The needs assessment was reviewed by the SCAG, and NASEO and NARUC also shared the needs assessments with the NASEO Energy Security Committee and the NARUC Critical Infrastructure committee for feedback. The state needs assessment was also reviewed by the Stakeholder Control Group. Both documents reflected the needs of NASEO and NARUC members and provided the basis for a robust project plan going forward.

Task 3.0: COMPLETE: Establish Stakeholder Control Group (SCG) and Engage External Working Groups for Toolkit Validation. NASEO and NARUC established the Stakeholder Control Group (SCG) with 8 members total, including six different states, 3 PUCs, 3 State Energy Offices, NERC, and a NASEO Senior Advisor. The SCG included at least 1 State Energy Official and 1 Public Utility Commissioner (or deferred staffer) who were asked to review tools at key points throughout the project.

Subtask 3.1: COMPLETE – Solicit External Feedback from SCG on Tools throughout the Project. NASEO and NARUC engaged the SCG on multiple occasions throughout the duration of the project, and solicited its input on the Needs Assessment, Literature Review, Project Roadmap, and all CATSS Toolkit Tools. The intent of the SCG reviews relative to the SCAG reviews was to ensure an objective and blind review of the intended end-users and beneficiaries.

Subtask 3.2: COMPLETE – Engage External Working Groups. NASEO and NARUC participated and presented to various (minimum two) external cybersecurity working groups, including the following:

- NASEO and NARUC presented on CATSS at the NARUC innovation webinar on April 15, 2021, this engaged an additional audience on the project.
- SunSpec/Sandia National Laboratory DER Cybersecurity Working Group – May 2022
- Solar to Grid (S2G) Working Group – Ongoing

Budget Period 2

Task 4.0: COMPLETE - Develop the Comprehensive Solar Cybersecurity Solutions Toolkit

The planned activities for Task 4.0 in BP3 included the development of solar cybersecurity tools based on the needs assessment and feedback from the SCAG.

Subtasks 4.1, 4.2, 4.3, and 4.4: COMPLETE – Solar Cyber Risk Assessment/Maturity Models Development and Validation. With the support of a subcontractor, Converge Strategies, NASEO developed and validated a Solar Cybersecurity Risk Assessment and Maturity Model, as well as a number of supplemental and priority resources identified by the SCAG during the needs

assessment. Part of this effort was developing and implementing a concurred strategy for feedback between the most relevant stakeholders and CATSS members. This was used to ensure that appropriate feedback was duly evaluated and incorporated. All final solar cybersecurity tools can be found on the CATSS website, listed below:

- User Guide for CATSS Tools
- Photovoltaic Solar Engineering and System Overview
- Standards Quick Guide
- Assessing Solar Cybersecurity: Questions for States to Ask Electric Utilities
- Hypothetical Solar Cyberattack Scenarios and Impacts
- Decision Support Tool for Solar Energy Cybersecurity Policy and Regulation
- Case Studies and Model Guidance for Establishing Solar Cybersecurity Working Groups
- Cybersecurity and the Solar Workforce: Considerations for States
- Cybersecurity Considerations for State Procurement of Solar Assets
- Exercise Design Guidance for Solar Cybersecurity
- State Legislative Options to Enhance Solar Cybersecurity

The development and release of the solar cybersecurity tools built on the previously conducted needs assessment, literature review, and feedback and validation from the SCAG. The CATSS project team issued a joint press release on September 29, 2023, which announced and promoted the release of the CATSS Toolkit to public and private sector partners.

Task 5: COMPLETE – Develop Key Contacts List and Communications Strategy.
The CATSS project team developed and presented the Key Contact List and Communication Strategy during a SCAG meeting. This strategy outlined the CATSS project team proposed outreach efforts, timeline, and stakeholders we planned to engage. During the meeting, the group reviewed and affirmed the communication expectations and protocols. The SCAG provided additional suggestions to promote and socialize the CATSS toolkit including creating a shorter video to walk through the basics of the toolkit, host a webinar discussing the tools' application for Public Utility Commissions and Emergency Management Agencies, and creating a one pager discussing the tools application to DOE's State and Tribal Grid Resilience Formula funding.

Task 6.0: COMPLETE –Engage External Working Groups for Toolkit Validation. Subtask 4.2 and 4.4. Task 6.0.
Upon completion of the draft tools of the CATSS toolkit, NASEO engaged several entities to solicit feedback and validate the technical findings of the tools. NASEO incorporated critical relevant feedback into the final versions. In addition to the SCAG CG, NASEO shared draft versions with the following groups:

- Sandia National Lab
- National Renewable Energy Laboratory
- Solar Energy Industries Association
- NASEO Energy Security Committee

- NARUC Subcommittee on Critical Infrastructure
- NASEO Solar Working Group

Budget Period 3

Task 7.0: COMPLETE - Dissemination and Outreach through Solar Cybersecurity Education Series
Task 7.0 included the dissemination of the completed CATSS project deliverables and tools to NARUC and NASEO members, relevant committees, and other appropriate stakeholders.

Subtask 7.1 and 7.2: COMPLETE –Dissemination and Outreach of the toolkit and project findings. This task involved dissemination of CATSS materials at NASEO and NARUC meetings and 2 External Working Group meetings**.** In support of these milestones, NASEO and NARUC presented at various virtual and in-person meetings throughout the budget period, including:

- In October 2023, the CATSS project team presented during a breakout session during the 2023 NASEO Annual Meeting in Portland, OR, alongside SCAG member Jeff Morris from Schneider Electric.
- In April 2024, at the request of the NASEO Board of Directors Western Regional Representatives the CATSS project team participated in a discussion among Western State Energy Office Directors focused on the cybersecurity of local energy assets and actions that states can take in partnership with utilities and industry to mitigate local energy assets' cybersecurity risks.
- In September 2023 and April 2024, the CATSS project team presented on the CATSS toolkit at the NARUC Cybersecurity Trainings with each event having over fifty Public Utility Commissioners and staff, State Energy Security Officials, federal and private sector partners attending.
- On October 5, 2023, the CATSS project team presented the toolkit and finding of the CATSS project to the Solar Energy Industries Association (SEIA) Utility Scale Division during a monthly call to an audience of over five hundred private sector partners.
- On October 23, 2023, the CATSS project team presented the toolkit and finding of the CATSS project to the Solar Energy Industries Association (SEIA) Distributed Generation Division during a monthly call to an audience of over one hundred and engaged in conversation with the attendees. Attendees were curious about the cost considerations when implementing cybersecurity best practices and how to best increase awareness and understanding on the importance of cybersecurity for stakeholders.
- On September 26, 2024, the CATSS project team presented the CATSS toolkit at the American Clean Power's (ACP) monthly PowerCast program series, accessible to their 800 member companies across the power sector. This engagement allowed NASEO to share the education and action oriented solar cybersecurity resources developed and highlight the ongoing work of State

Energy Office with a new audience of private industry companies. Additionally, this speaking engagement fostered a relationship with a new partner, ACP.

Subtask 7.3: COMPLETE – Technical Assistance/Walkthrough Webinars with States.. In support of this milestone, CATSS project team hosted 3 webinars to help states understand how to utilize the tools to advance their solar cybersecurity goals and share evolving solar cybersecurity landscape. The first webinar guided states through the content of the published Solar Cybersecurity Toolkit, highlighting how these resources can enhance cybersecurity for distributed energy systems. The second webinar featured Megan Culler from Idaho National Laboratory, who shared insights on solar cybersecurity supply chain risks, ongoing laboratory initiatives, available resources, and guidance on how State Energy Offices can get involved. The third webinar reviewed the findings and recommendations from CATSS program, discussed ongoing state-level challenges and needs, and explored how NASEO and State Energy Offices plan to continue supporting PV solar cybersecurity through current and future initiatives.

Subtask 7.4: COMPLETE – Host State Solar Cybersecurity Workshop and Discussion-Based Tabletop Exercise.. At the workshop, NASEO assessed the effectiveness of various tools and concepts developed thought the CATSS project. The exercise scenarios leveraged existing CATSS tools and emphasized opportunities for two-way information-sharing on response plans, procedures, and protocols for cybersecurity incidents affecting solar photovoltaic (PV) systems amongst state, local, tribal, territorial (SLTT) communities and industry partners. Additionally, through presentations from subject matter experts and peer-to-peer exchanges, states identified strategies and recommendations for integrating solar cybersecurity planning into formal state plans, policies, and procedures, such as State Energy Security Plans.

Task 8.0: COMPLETE - Strategy to integrate SCAG into NASEO and NARUC Communities
Task 8.0 included the development of memo outlining the SCAG integration into relevant NASEO and NARUC programming.

Subtask 8.1: COMPLETE – Produce a Final Memo. The memo “Cybersecurity Advisory Team for State Solar Integration into the National Association of State Energy Officials Programming,” details NASEO’s past and planned efforts to integrate CATSS and solar cybersecurity into its programming, including national and regional meetings, the NASEO Energy Security Committee, and the NASEO Energy Security Committee’s quarterly newsletter. To facilitate the adoption of CATSS insights and best practices in state policies, programs, and procedures, NASEO incorporated the resources developed under CATSS into existing committee structures, activities, and events. For example, is in April 2024, at the request of the Board of Directors Western Regional Representatives, the CATSS project team participated in a discussion among Western State Energy Office Directors focused on the cybersecurity of local energy assets and actions that states can take in partnership with utilities and industry to mitigate local energy assets’ cybersecurity risks. Additionally, in September 2023 and April 2024, the CATSS project team presented

on the CATSS toolkit at the NARUC Cybersecurity Training with each event having over fifty Public Utility Commissioners and staff, State Energy Security Officials, federal and private sector partners.

Project Challenges

The CATSS project navigated a series of challenges that shaped both the pace and shape of the initiative. These challenges reflect broader tensions in long-term public-private cybersecurity initiatives—especially those attempting to span technical, policy, and sectoral boundaries in a rapidly evolving environment.

1. Virtual Convening and Engagement Constraints During COVID-19
Launching CATSS amid the COVID-19 pandemic made effective stakeholder engagement more challenging. The inability to host an in-person kickoff initially hindered the formation of strong working relationships and collaborative momentum. It was difficult to build trust between diverse stakeholders who had not yet met in-person through virtual meetings—particularly in a space as specialized as cybersecurity, where informal relationship-building and nuanced discussions are often critical. The lack of organic conversation and hallway-side dialogue limited the advisory group's ability to dive deeply into sensitive or complex issues and likely contributed to initially lower overall engagement.

2. Overly Prescriptive Long-Term Planning in a Dynamic Landscape
At the outset, the project outlined a highly structured and detailed SOPO that was intended to guide work over a multi-year period. While this was useful for scoping the initial vision, it ultimately proved to be a constraint. The cybersecurity and solar landscapes evolved rapidly during the project, with new federal guidance, emerging threats, and evolving sector-specific developments. The rigidity of the initial workplan left little room to pivot or adapt organically, leading to tension between pre-set deliverables and emergent needs that could not have been anticipated at project launch.

3. Staff Turnover and Institutional Knowledge Loss
As with many long-term initiatives, CATSS was impacted by staff turnover among both the project team and advisory group participants. Transitions in key roles led to the loss of institutional knowledge and, in some cases, the departure of champions who had driven momentum. Onboarding new staff and reestablishing continuity required time and energy that hampered forward progress and increased the project timeline. In some cases, relationships and institutional trust built over time were disrupted, slowing down collaboration and decision-making.

4. Challenges Translating Technical Concepts into Policy-Relevant Language
One of the project's core goals was to bridge the gap between technical cybersecurity knowledge and state-level energy policy. This proved especially difficult in a virtual setting, where real-time clarification and collaborative iteration were constrained. Translating highly technical threat landscapes, mitigation strategies, and industry best practices into terms that were actionable for state policymakers required significant

back-and-forth, which was harder to facilitate in virtual-only environments. This language and framing gap often led to misunderstandings and constrained the project.

5. Stakeholder Diversity and Engagement in the Solar Industry
The decentralized and highly varied nature of the solar industry presented major challenges for engagement. From small installers and inverter manufacturers to utility-scale developers and asset managers, there is no single "solar sector," and few stakeholders see themselves as primarily responsible for cybersecurity or are speaking for the entire sector. Identifying companies—or specific individuals within companies—who were both knowledgeable about and invested in cybersecurity proved time-intensive and yielded mixed success. Many prospective participants either lacked the resources to engage or were focused on other pressing operational or regulatory challenges.

Despite these obstacles, the CATSS initiative made important strides in raising awareness, building cross-sector connections, and surfacing valuable insights for state energy and cybersecurity planning. The challenges described above underscore the need for adaptable structures, sustained engagement mechanisms, and tailored communication strategies when tackling interdisciplinary and fast-moving issues like cybersecurity in emerging energy sectors.

Recommendations for Future Projects

1. Begin with a Flexible, Iterative Project Structure
Challenge Addressed: Overly prescriptive long-term SOPO in a dynamic environment
Recommendation:
Design the project around modular phases rather than a rigid multi-year SOPO. Include built-in checkpoints for periodic reassessment and reprioritization to account for evolving technology, threat landscapes, and external initiatives. Documenting key decision points will also aid continuity if staff changes occur.

2. Prioritize In-Person Engagement Early in the Process
Challenge Addressed: Virtual convening limitations during COVID
Recommendation:
Budget and plan for an **in-person kickoff or early convening**, even if most of the work will be remote. Early in-person meetings foster trust, encourage cross-sector engagement, and build the informal relationships that support sustained virtual collaboration over time.

3. Integrate Stakeholder Mapping and Engagement Design at the Outset
Challenge Addressed: Difficulty identifying motivated solar industry participants
Recommendation:
Include a deliberate stakeholder mapping phase at the start of the project to identify which industry players (e.g., developers, vendors, aggregators, trade groups) are most relevant, motivated, and available to engage on cybersecurity. Use this mapping to

tailor engagement formats and communications and consider using intermediaries like industry associations or regional working groups to broker participation.

4. Create a Clear, Shared Vocabulary for Technical-Policy Translation
Challenge Addressed: Difficulty translating technical cybersecurity content for policy audiences
Recommendation:
Develop a living glossary or translation guide that defines key cybersecurity and grid technology terms in policy-relevant language. Pair technical experts with State Energy Office staff during advisory group meetings and use visual models (e.g., system diagrams, risk matrices) to reinforce understanding across audiences.

5. Anticipate and Plan for Staff Turnover
Challenge Addressed: Loss of institutional knowledge and momentum
Recommendation:
Consider developing onboarding materials for new project members and attain buy-in from State Energy Office and advisory group member leadership, not necessarily only individual staff.

Key Findings and Path Forward

The following represent key findings reiterated during the final phase of CATSS. The findings are consolidated categorically into the following groups: **Vulnerabilities, Risk Assessments, Preparedness and Planning, Information Sharing, Incident Response, Procurement,** and **Standards.** These findings will be used to inform future State Energy Office efforts as part of or related to CATSS and the cybersecurity of solar assets, generally. Unless specifically identified or hyperlinked toa public-facing resource, many of the following insights were disclosed under Chatham House Rules. As such, specific individuals or entities will not be identified.

Vulnerabilities

- CATSS members noted that rural cooperatives and small municipal utilities are particularly vulnerable to cyberattacks and ransomware, as they generally do not have the financial means to sustain a robust cybersecurity program and are therefore more vulnerable. It was suggested that enhanced financial and technical assistance provided by State and Federal partners may be helpful to support small utilities in addressing these vulnerabilities.
- Discontinuation of services after solar companies go out of business can lead to significant vulnerabilities, as there are no longer service providers to advise on the installation of updates or patches for IT and OT systems.

Threat Assessments

- Some risk assessment studies developed by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA) are protected and unable to be shared with state stakeholders. States have asked to see this information and have been denied. NASEO will be exploring

opportunities for improved information sharing between CISA, state fusion centers, State Energy Offices, Public Utility Commissions, and the E-ISAC.
- There is a need to perform risk assessments for local and county-level critical energy infrastructure, but questions remain regarding which entity/entities would lead such an effort, what would be done with information gathered, and who might have the authority to collect and protect this information. There is an opportunity for State Energy Offices to fold this information into their State Energy Security Planning efforts.
    - Local organizations, such as the National League of Cities and the National Association of Counties, may be able to assist with this effort.

Preparedness and Planning

- It was noted that there is not a regular convening of local energy asset operators, other industry members (e.g., bulk battery storage manufacturers, vendors), and state and federal partners on security, cybersecurity, supply chain vulnerabilities, and applicable regulations, standards, and policy. Some industry groups are having these discussions but are interested in more regular and formal engagement with public partners and are seeking more information how they can get engaged with states and be apprised of their priorities.

Incident Notification and Information-Sharing

- There is an apparent knowledge gap among State Energy Offices regarding reporting requirements for behind the meter microgrids and, more broadly, local energy assets.
- It was unclear where various entities in the solar industry—specifically, local energy asset aggregators, independent power producers, and microgrid operators—would or could be plugged into cybersecurity incident notification processes or incident command structures.
- It was noted that informal relationships and information-sharing avenues can be developed and leveraged for incident response. Proactive, informal, and trust-based information-sharing can be extremely valuable, but there currently aren't enough strong informal relationships between state incident responders and the solar industry to enable this.

Incident Response

- For some types of cybersecurity incident responses, it may be possible to leverage trained members of the national guard to provide hands-on operational support or technical assistance to electric utilities, but questions remain as to the legal and contractual enablers for such support. Further, additional questions were raised pertaining to the type of state and federal support that might be provided to private entities involved in solar energy generation.
- Public communications and crisis communications were discussed in depth. Participants suggested that a template or "canned" resource on solar industry operations, functions, and terminology could be developed to better inform the public and State officials during future incidents. Participants noted that the System Engineering Guide was helpful for a basic knowledge of these terms and

functions, but a more extensive resource, inclusive of supply chain and interconnected infrastructure systems, would be welcome. This resource would help level-set expectations and understanding and reduce risks of misinformation. The Oil and Natural Gas Subsector Coordinating Council (ONG SCC) has developed a similar resource that may be used as a mode.

Procurement

- There are significant opportunities for State Energy Offices to support cybersecurity in the solar industry by enhancing cybersecurity provisions in state procurement standards. As recipients and directors of significant state and federal funding to support solar (and local energy asset) deployment, State Energy Offices have discretion to raise the cybersecurity standards of assets procured and contractors hired by the state. It was noted that the CATSS Cybersecurity Procurement Guidance for States was leveraged to develop enhanced cybersecurity procurement language for existing state programs. Such successes can inform enhanced cybersecurity procurement guidance for states.

Standards and Best Practices

- Participants noted it was unclear if there exists guidance or standards for specific types of solar installations (e.g., solar, solar-plus-storage, solar-plus-microgrids, etc.). It was also unclear if there were any behind the meter standards or best practices. State participants noted their interest in updated guidance to determine which standards are most applicable to various types of systems.
- Participants suggested that industry-informed voluntary standards or guidelines might be an effective way to address associated vulnerabilities. Voluntary standards or guidelines that are not subject to lengthy update, review, and consensus processes allow infrastructure owners and operators to remain flexible enough to address evolving threats.

Next Steps and Potential Future Efforts

There is significant interest State Energy Offices for additional education, technical assistance, resources, and other guidance from NASEO and SETO regarding solar cybersecurity. There is a need to more directly involve and better coordinate with additional entities and agencies involved in traditional security resilience, such as state emergency management agencies, rural utilities, and energy trade associations. Future endeavors may propose additional and supplementary work to the CATSS toolkit to better assist State Energy Offices with their solar cybersecurity posture and maturity.

To that end, the NASEO Energy Security Program will continue to work through existing structures such as virtual and in-person NASEO committee engagements, the NASEO Board of Directors, annual and regional events, and specific energy security related events to integrate findings from CATSS and the topic of local energy assets' cybersecurity more broadly. There are several opportunities for engagement with NASEO's and NARUC's committees through monthly virtual calls, committee hosted webinars, and in-person committee meetings during larger annual events. The CATSS

project team is committed to including solar cybersecurity during at least two committee efforts per year for the next two years, and at the request of members.

Beyond normalization of CATSS findings and identified priorities in NASEO programming, there is a clear demand from State Energy Offices, as well as other market actors and key stakeholders, for additional education, technical assistance, resources, and other guidance on cybersecurity for solar systems. State Energy Offices are lead implementers and funders of a variety of different solar or solar-inclusive programs supported by state funds, as well as programs through DOE, EPA, and FEMA. State Energy Offices have ambitious energy goals and maintain State Energy Security Plans, which contextualize energy security data, paradigms, networks, and strategies within each state. Ultimately, robust solar cybersecurity is key to ensuring that solar programs supported by State Energy Offices can be implemented reliably and effectively.

Through a continuation of CATSS, future efforts may consider updating the four most useful tools (Photovoltaic Solar Engineering and System Overview, State Legislative Options to Enhance Solar Cybersecurity, Exercise Design Guidance for Solar Cybersecurity, and Cybersecurity Considerations for State Procurement of Solar Assets) from the original CATSS toolkit, develop two new tools based on evolving state needs, and host an in-person convening to revitalize an active SCAG focused on public-private solutions for enhanced solar cybersecurity driven by states.

Opportunities and Gaps to Inform Future Work

The following are specific opportunities and gaps that may help inform future efforts that build on or are developed to compliment CATSS.

- While continuous and improved education is always necessary, action and implementation-oriented resources are needed to further solar-cybersecurity concepts and best practices at the state level.
- There are opportunities to incorporate solar cybersecurity into State Energy Security Plans as formal components of each state's energy security risk mitigation strategy, which will help institutionalize solar cybersecurity issues into energy security planning.
- Industry entities need to be more involved in traditional state energy security and cybersecurity efforts, in order to establish state-specific public-private relationships, networks, and plans, which are more effective and nuanced than national frameworks. Existing relationships between industry partners and states, specifically developed to address solar cybersecurity, are rare and have significant opportunity to mature and be replicated in other states.
- There are disparate efforts to ensure that local energy assets are cyber-secure across federal agencies and among the national labs. NASEO and State Energy Offices can serve as coordinators of these various efforts to support practical implementation.

To close these gaps and build upon the success of CATSS, future efforts may consider performing the following specific activities:

Proposed Activity 1: Create and Maintain Existing Solar Cybersecurity Tools

This activity may enhance ***existing*** CATSS tools to make them more actionable and action oriented. These tools were identified by State Energy Offices as the most useful and as having the most potential for expanded or updated content.

Tool 1: Engineering, System, and Supply Chain Overview

- Update the original CATSS Solar Engineering and System Overview to include ***new*** overviews of the solar supply chain, manufacturing, interconnections, and key solar industry partners (e.g., IPPs, aggregators, installers, manufacturers). This tool will expand upon the success of the original tool by providing a more comprehensive and approachable overview of the solar industry through a cybersecurity and risk perspective. The tool's content will be presented in a graphic and narrative form. Such an effort should engage Idaho National Laboratory (INL), the National Renewable Energy Laboratory (NREL), and Sandia National Laboratory (SNL), and other lab partners as identified by SETO.

Tool 2: Workforce Development Strategies

- Expand upon the Cybersecurity and the Solar Workforce: Considerations for States tool to explore ways that State Energy Offices can support the growth of a cyber-informed solar industry workforce, as well as support existing workforce development programs to give greater consideration to relevant topics. Such an effort should include industry partners, such as the Solar Energy Industries Association (SEIA), the ACP, community colleges, trade schools, and universities. Such an effort may explore how State Energy Offices can assist with:
    - Cybersecurity education programs for small utilities with solar assets
    - Cybersecurity training for solar industry generally (e.g., cybersecurity education for installers and other entity types)
    - Cybersecurity education opportunities with academia
    - Inventory of relevant cybersecurity, local energy assets, and solar-cybersecurity training courses

Tool 3: Cybersecurity Procurement Action Plan (CPAP)

- Expand upon the Cybersecurity Considerations for State Procurement of Solar Assets tool to include more specific examples and guidance of cyber-informed procurement documents that State Energy Offices have used to procure solar assets or fund the procurement of solar assets for grant sub awardees through various programs, including but not limited to 40101(d), GRIP, SEP, Solar for All, and others. Such an effort should provide specific language, examples, and state insights in this guidance. It should involve SETO, CESER, DHS, and various national labs to inform this guidance and ensure it is actionable, practical, and specific to State Energy Office

programs. We also recommend this effort engage with StateRAMP to assist with approaches to vendor monitoring and compliance.

Tool 4: State Legislative Options 2.0

- Update the State Legislative Options to Enhance Solar Cybersecurity by reviewing new state legislation pertaining to solar-cybersecurity, local energy assets' cybersecurity, solar energy reliability mandates, and other relevant topics. NASEO will engage the National Conference of State Legislatures (NCSL) to streamline this process. This enhanced resource will provide an updated guidebook of legislative solar-cyber options.
- Provide an action-oriented template and/or example language that State Energy Offices can use to support legislation that would enhance solar cybersecurity.

Proposed Activity 2: Develop New Tools to Supplement the CATSS Toolkit

This activity may develop *new* action-oriented CATSS tools. Future efforts should consider developing the following tools:

Tool 1: State Energy Security Plan Inclusion Guidance for Solar Cybersecurity

- This tool would help guide states to more easily include solar-cybersecurity provisions in their SESPs. This may adapt existing federal SESP requirements and resources and may include specific guidance on:
  - Solar Energy Cybersecurity Risk Profile Guidance
  - Solar-Cybersecurity Risk Assessment Approaches
  - Solar-Cybersecurity Risk Mitigation Strategies

Tool 2: Solar Industry Cybersecurity Discussion Guidance

- This tool would provide talking points and discussion questions for State Energy Offices to engage industry partners on solar cyber issues, extract information to inform planning efforts, and build relationships. This guidance may consist of entity-specific chapters for the following types of industry partners:
  - Regional Solar trades
  - Independent Power Producers
  - Aggregators
  - Installers
  - Investor-Owned Utilities
  - Consumer-Owned Utilities
  - Community Solar Owners
  - Microgrid Owner/Operators

Proposed Activity 3: Host a State Solar Cybersecurity Workshop

Future efforts may consider building on the success of the final CATSS workshop by hosting a national workshop to help inform the development of the enhanced CATSS tools, expand state and industry networks and partnerships, and inform State Energy Offices of the newest solar cybersecurity risk elements, mitigation strategies, technologies, and approaches. The workshop should be open to a diverse array of states and industry stakeholders.

Such an event should be aligned with RE+/Secure Renewables (hosted by SETO and SEIA), or other related events, to inform the development or progress of each tool, and to further connect state officials with industry and federal partners.

Project Team and Roles

CATSS was led by subject matter experts at NASEO and NARUC and supported by a diverse, volunteer-led SCAG. The project team also included a small Control Group and various engagements with a disparate and fluctuation cadre of external working groups, committees, and other entities.

The core CATSS team, composed of NASEO and NARUC staff, with frequent input from National Lab staff—namely Sandia National Laboratory, National Renewable Energy Laboratory, and Idaho National Laboratory—provided overall program oversight and budget management; developed research, technical assistance offerings, and other resources to support State Energy Office and Public Utility Commission understanding of solar cybersecurity issues; coordinated the CATSS SCAG; and used its platforms to increase visibility and understanding of CATSS goals and activities among external stakeholders.

The CATSS Toolkit was in part completed with support from Converge Strategies, which was subcontracted to develop more technical tools

The individuals and entities that were critical to the completion and success of CATSS include members of the SCAG and are listed as follows:

- NASEO Staff:
    - Kirsten Verclas, Senior Managing Director, NASEO
    - Campbell Delahoyde, Senior Program Director, NASEO
    - Sarah Trent, Senior Program Manager, NASEO
- NARUC Staff
    - Lynn Costantini
    - Ashton Raffety
- SETO:
    - Marissa Morales Rodriguez
    - Shay Banton
    - Jeremiah Miller
- State Energy Offices and Public Utility Commissions
    - California Energy Commission
    - New Hampshire Department of Energy
    - Energy Programs Office, Pennsylvania Department of Environmental Protection
    - Florida Public Service Commission
    - California Public Utilities Commission
    - Maryland Energy Administration
    - New Hampshire Public Utilities Commission

  - Louisiana Department of Energy and Natural Resources
  - Illinois Commerce Commission
  - Public Service Commission of Wisconsin
  - Maryland Public Service Commission
  - Massachusetts Department of Energy Resources
  - Massachusetts Department of Public Utilities
  - Office of Energy Innovation, Public Service Commission of Wisconsin
  - Missouri Public Service Commission
  - Office of Energy, Florida Department of Agriculture and Consumer Services
  - District Department of Energy and Environment
  - Puerto Rico Energy Bureau
  - Vermont Public Utility Commission
  - North Carolina Utilities Commission
  - Michigan Department of Environment, Great Lakes, and Energy
  - Washington State Energy Office
  - Nevada Governor's Office of Energy
- Converge Strategies
- The CATSS SCAG comprised of various levels of participation from the following organizations:
  - American Public Power Association
  - Archer International
  - Edison Electric Institute
  - Electric Power Research Institute
  - Idaho National Lab
  - National Electrical Manufacturers Association
  - National Institute of Standards and Technology
  - National Renewable Energy Lab
  - National Rural Electric Cooperative Association
  - PJM Interconnection
  - Protect our Power
  - Sandia National Lab
  - Schneider Electric
  - Solar Energy Industries Association
  - Sunrun
  - SunSpec
  - Tesla
  - Underwriter's Lab
  - US Department of Energy: Solar Energy Technologies Office, Office of Cyber Security, Energy Security, and Emergency Response, and Office of Electricity

CATSS Final Products

Publications and resources produced under CATSS include (available NASEO's website at www.naseo.org/publications) include:

- **CATSS Literature Review: Resources for Solar Cybersecurity** (2021)

  - **Summary**: This review compiles and categorizes key reports and research related to solar and DER cybersecurity. It includes interconnection resources, cybersecurity frameworks, primers, state case studies, and roadmaps—such as NREL's DER cybersecurity framework and Sandia's DER roadmap for photovoltaic security—offering a foundational reference list for State Energy Offices and regulators.
  - **URL**: https://www.naseo.org/Data/Sites/1/media/issues/cybersecurity/catss-literature_review.pdf
- **CATSS Project Roadmap** (2021)
  - **Summary**: The Project Roadmap provides a structured overview of the CATSS initiative timeline, tool roll-out plan, strategic phases, stakeholder engagement strategy, and intended milestones. It helps states understand sequencing, coordination points, and dependencies across advisory group activities and tool launches.
  - **URL**: https://www.naseo.org/Data/Sites/1/documents/tk-news/catss-roadmap-public-version-september-2021.pdf
- **Toolkit User Guide** (2024)
  - **Summary**: This introductory guide provides context on the CATSS initiative, explains the motivations behind the project, and presents a suggested roadmap for engaging with the toolkit's ten tools. It categorizes tools into educational/risk-awareness and policy-oriented/actionable tools and offers guidance on the order of use and target audiences.
  - **URL**: https://www.naseo.org/Data/Sites/1/documents/tk-news/catss-user-guide_v1.pdf
- **Photovoltaic Solar Engineering and System Overview** (2023)
  - **Summary**: Provides a schematic overview of PV system components—including inverters, batteries, EVs, DER aggregators—and their interconnections. Highlights cyber-physical risks, differentiates between grid-following vs. islanded operations, and helps establish core terminology and risk contexts for non-technical stakeholders.
  - **URL**: https://www.naseo.org/Data/Sites/1/documents/tk-news/annex-b_catss-engineering-and-systems-overview_v2.pdf
- **State Legislative Options to Enhance Solar Cybersecurity** (2023)
  - **Summary**: Presents a range of legislative approaches and policy frameworks that states can adopt to improve cybersecurity posture for solar deployments. Includes sample statutory language, references to existing state laws, and suggestions for enabling regulatory and policy levers tailored to solar/DER risks.
  - **URL:** https://www.naseo.org/Data/Sites/1/documents/tk-news/catss-user-guide_v1.pdf
- **Exercise Design Guidance for Solar Cybersecurity**(2024)

  - **Summary**: Offers recommendations for designing emergency preparedness exercises focused on solar cybersecurity—including tabletop, workshop, and seminar formats. Includes scenario examples, suggested participants, planning considerations, and sample discussion prompts to test incident response and coordination.
  - **URL:** https://www.naseo.org/Data/Sites/1/documents/tk-news/catss_exercise_design_guidance_final.pdf
- **Cybersecurity Considerations for State Procurement of Solar Assets** (2023)
  - **Summary**: Provides template language and strategic guidance for state procurement processes (e.g., RFPs, grants, contracts) to integrate cybersecurity requirements. Covers supply chain risks, software bill of materials (SBOM), sourcing transparency, and aligning with federal supply chain policies.
  - **URL**: https://www.naseo.org/Data/Sites/1/documents/tk-news/catss-procurement_v2.pdf
- **Cybersecurity and the Solar Workforce: Considerations for States** (2023)
  - **Summary**: This tool identifies workforce competencies and requisite skill sets for the solar cybersecurity workforce and highlights tactics for State Energy Offices and Public Utility Commissions to amplify training initiatives and build partnerships. It offers policy pathways to foster growth of the solar cybersecurity workforce and outlines internal cyber expertise state agencies should consider to support their roles.
  - **URL**: https://www.naseo.org/Data/Sites/1/documents/tk-news/catss-workforce-development-guide_v2.pdf
- **Case Studies and Model Guidance for Establishing Solar Cybersecurity Working Groups** (2023)
  - **Summary**: Describes real-world examples and models for establishing state-level cybersecurity working groups focused on solar and DERs. It profiles different stakeholder roles (utilities, installers, homeland security offices, etc.) and outlines pathway models based on existing groups such as California's smart-inverter working group.
  - **URL:** https://www.naseo.org/Data/Sites/1/documents/tk-news/catss-case-studies-and-model-guidance_v4.pdf
- **Decision Support Tool for Solar Energy Cybersecurity Policy and Regulation** (2024)
  - **Summary**: A robust decision-support resource designed to assist state officials in evaluating policy, regulatory, and programmatic options related to solar cybersecurity. It includes frameworks for cost–benefit analysis, criticality checklists, procurement guidance, and assessments of component reliability.

    - **URL:** https://www.naseo.org/Data/Sites/1/documents/tk-news/decision-support-tool-for-solar-energy-cybersecurity-policy_v3.pdf
- **Hypothetical Solar Cyberattack Scenarios and Impacts** (2024)
    - **Summary**: Features illustrative cyberattack scenarios focused on solar energy infrastructure—such as coordinated inverter disruptions, DER aggregation impacts, and microgrid takeover events. Designed to support planning, exercises, and stakeholder dialogue around solar cybersecurity vulnerabilities.
    - **URL:** https://www.naseo.org/Data/Sites/1/documents/tk-news/annex-c_catss-consequence-scenarios_v3.pdf
- **Assessing Solar Cybersecurity: Questions for States to Ask Electric Utilities** (2023)
    - **Summary**: Builds on existing NARUC utility cybersecurity questionnaires by adding solar/DER-specific questions. It provides a checklist-style tool to guide state agencies in ongoing utility oversight, risk ownership evaluation, and vendor accountability on solar cybersecurity practices.
    - **URL:** https://www.naseo.org/Data/Sites/1/documents/tk-news/catss-user-guide_v1.pdf
- **Standards Quick Guide** (2023)
    - **Summary**: Offers a concise listing of industry standards, regulatory frameworks, and emerging cybersecurity protocols relevant to solar energy (DERs). It introduces the Probabilistic Risk Assessment (PRA) model and helps states map vulnerabilities to mitigative actions and policy considerations.
    - **URL**: https://www.naseo.org/Data/Sites/1/documents/tk-news/annex-a_catss-standards-quick-guide_v2.pdf

External References to CATSS

- Utility Dive - NARUC, NASEO team up to tackle distributed solar cyber risks as vulnerabilities grow
- U.S Department of Energy Roadmap for Wind Cybersecurity
- EPRI Security Network for the Distributed Energy Resources Integration Network
- NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0
- NREL - An Overview of Distributed Energy Resource (DER) Interconnection: Current Practices and Emerging Solutions
- NREL - Guide to the Distributed Energy Resources Cybersecurity Framework
- NREL – Cybersecurity in Photovoltaic Plant Operations
- Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators
- Cyber Security Assessment of Distributed Energy Resources

- Roadmap for Distributed Energy Resource Cyber Security
- Roadmap for Photovoltaic Cybersecurity