Decision Support Tool for Solar Energy Cybersecurity Policy and Regulation

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

Disclaimer:
The CATSS Toolkit is designed to provide states with basic education on cybersecurity issues for solar and enable their efforts to support cybersecurity enhancements efforts for solar. Cybersecurity challenges for solar should not be viewed as unique. All electricity generation technologies are, to varying degrees of potential severity and vulnerability, susceptible to cyberattacks and disruption. As interconnected electricity generation technologies, solar systems—and DERs generally—have a unique advantage to ensure that cybersecurity is incorporated by-design and prior to deployment, rather than applied ex post facto. The recommendations provided within the CATSS Toolkit/this tool were developed to meet the expressed needs of State Energy Offices and Public Utility Commissions during the project, and their respective purviews, priorities, and directives to support cyber-secure solar deployment in their states. While many industry and federal partners were included in the CATSS Advisory Group, it must be noted that neither the states' nor other stakeholders' perspectives collected are exhaustive. The Toolkit represents a snapshot of a quickly evolving and complex area, and should not be treated as a definitive guide, but rather a basis for continued discussion and adaptation of public-private partnerships for solar cybersecurity

NASEO
National Association of State Energy Officials

National Association of Regulatory Utility Commissioners
Dedicated to Public Service
1889

Prepared for the National Association State Energy Officials (NASEO) and National Association of Regulatory Utility Commissions (NARUC)

About This Resource

This material is based upon work supported by the U.S. Department of Energy 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.

ABOUT NATIONAL ASSOCIATION OF STATE ENERGY OFFICIALS

NASEO is the only national non-profit association for the governor-designated energy officials from each of the 56 states and territories. Formed by the states in 1986, NASEO facilitates peer learning among State Energy Officials, serves as a resource for and about State Energy Offices, and advocates the interests of the State Energy Offices to Congress and federal agencies.

Learn more about NASEO at www.naseo.org.

NASEO
National Association of State Energy Officials

ABOUT NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS

NARUC is a national non-profit membership association for state utility regulators (public utility/service/commerce commissions) from all 50 states, DC, and territories. It serves as a resource for and about state utility regulators through topical committees, regional dialogues, and informational events that facilitate peer learning, best practice sharing, and consensus building.

Learn more about NARUC at www.naruc.org.

ABOUT CONVERGE STRATEGIES, LLC

Converge Strategies, LLC (CSL) is a consulting company focused on the intersection of clean energy, resilience, and national security. CSL works with civilian and military partners to develop new approaches to energy resilience policy and planning in the face of rapidly evolving threats, vulnerable infrastructure, and determined adversaries.

Learn more about CSL at www.convergestrategies.com.

CONVERGE STRATEGIES

Table of Contents

Navigation | Users can review the Introduction to understand the Decision Support Tool's purpose and the elements contained inside. Each section can be utilized independently based on a user's specific needs. Sections can also be used comprehensively as a means to identify codes, standards, and policies that can maximize a state's ability to mitigate cyber risk in solar energy assets.

Overview | This Decision Support Tool is a starting point and will not address all the unique roles and responsibilities of each State Energy Office and each utility commission. Users will improve their understanding of current cybersecurity policies, assess their applicability to solar energy systems, and increase their awareness of system risks. Additionally, the tool presents a series of scenarios depicting anticipated impacts of multiple cyber attack methods that target solar energy assets. This information can help users prioritize policy decisions based on risks, and it can also be used to focus discussions or design exercises to explore governance/ policy options that mitigate those risks.

Resources | Links to policies, documents, and assessment frameworks are available in the Annex at the end of the Decision Support Tool to help understand the methods, resources and analytical processes utilized in the development of this content.

Introduction

DECISION SUPPORT TOOL PURPOSE

Overview | The U.S. Energy Information Administration (EIA) projects that solar energy will generate 20% of U.S. electricity by 2050, up from 3% in 2020 (Source: EIA). The rapid proliferation of solar energy presents a challenge to State Energy Officials and state regulators who are faced with ensuring policies and regulations are put in place to keep these assets protected from potential cybersecurity attacks. Given the significant number of physical, hardware, and software components required to safely and reliably operate solar energy systems, new tools are needed to address cybersecurity risk. This Decision Support Tool will help users address four specific challenges:

✓ Complex Requirements

The sheer number and type of codes, standards and regulations in this space impedes the ability of states to draft and evaluate policy that will address risk.

✓ Technical Complexity of Solar Assets

While each physical or digital component plays an essential role in solar energy, specific components must be identified to develop useful policy.

✓ Undefined Cyber Risk Severity

States need a clear understanding of cyber risk to prioritize their limited technical, economic, and policy resources.

✓ Unclear Roles and Responsibilities

The diversity of relevant public, private, and nonprofit actors requires that the entities with the authority and responsibility to act be clearly identified.

DECISION SUPPORT TOOL ELEMENTS

The Decision Support Tool allows users to access elements of the resource individually or as part of an integrated process. 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.

Resources	Decision Support	Risk Assessment
Background information on the current policy landscape, solar energy components, and cyber attack methods/scenarios	Identify the risk owners, compare codes, standards, and regulation, and use state policies and processes to maximize risk mitigation	A comparative analysis of cyber attack risks that affect specific solar photovoltaics (PV) components, helping users prioritze policy
Policy Quick Guide	**Risk Ownership Framework**	**Risk Assessment Process**
Engineering Overview	**Governance/ Policy Options**	**Risk Scoring Methodology**
Cyber Attack Scenarios	**Implementation Process**	**Probabilistic Risk Assessment Results**

Policy Quick Guide

The Cybersecurity Imperative | The DOE report *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid* states that, “the high deployment of solar energy and other DER pose emerging cybersecurity challenges for the electric grid.” State officials have an important role in identifying, implementing, and enforcing policy that will help mitigate this risk.

Overview | This quick guide is intended to enhance State Energy Office and Public Utility Commission understanding of existing resources and to provide policy ideas for improving the cybersecurity of solar energy systems and system components. The Policy Quick Guide contains a list of relevant standards, codes, or regulations developed (or in development) for the cybersecurity of solar energy systems and components. It outlines different types of mandatory and voluntary policies ranging from planning frameworks to guidance documents.The role of state agencies in scoping, developing, implementing, and enforcing policies varies depending on factors such as the issuing organization and the requirements of state legislation. A summary of the guide’s contents is included below. The full Guide can be found in Annex A.

SOURCES OF CODES, STANDARDS, AND REGULATIONS

Industry

- ❏ Developed by Subject Matter Experts (SME) through an interactive process of draft, debate, test, and refine
- ❏ Organizations include Institute of Electrical and Electronics Engineers (IEEE) and International Electrotechnical Commission (IEC)
- ❏ Includes a peer-review process to ensure accuracy and efficacy of proposed standards

Government

- ❏ Developed by federal and state regulatory bodies and with input from state working groups (**See** *Case Studies and Model Guidance for Establishing for Solar Cybersecurity Working Groups*)
- ❏ Enforced through regular auditing and review of systems and policies of regulated companies
- ❏ Engaged through public comments and task forces

Academic

- ❏ Guidance documents produced through research of cyber threats and testing of technical components that assess their efictiveness in mitigating risks
- ❏ Issued by universities, independent bodies, think tanks, national laboratories, Federally Funded Research and Development Centers (FFRDCs), and governments

Questions for Policymakers

- Which codes, standards, or regulations are applicable to the solar PV components under consideration?
- How effective are they in reducing risk?
- Should they be mandatory or voluntary? Does a state have the authorities (e.g., legislative authority) required to enact and enforce them?
- What outside organizations need to be engaged?

Definitions

Code: A principle developed to establish a minimum criteria for operation or design

Standard: Established by authority, custom, or general consent as a model, example, or point of reference

Regulation: A rule or directive made and maintained by a regulatory authority

Engineering and Systems Overview

SCHEMATIC OF SOLAR PV AND GRID COMPONENTS

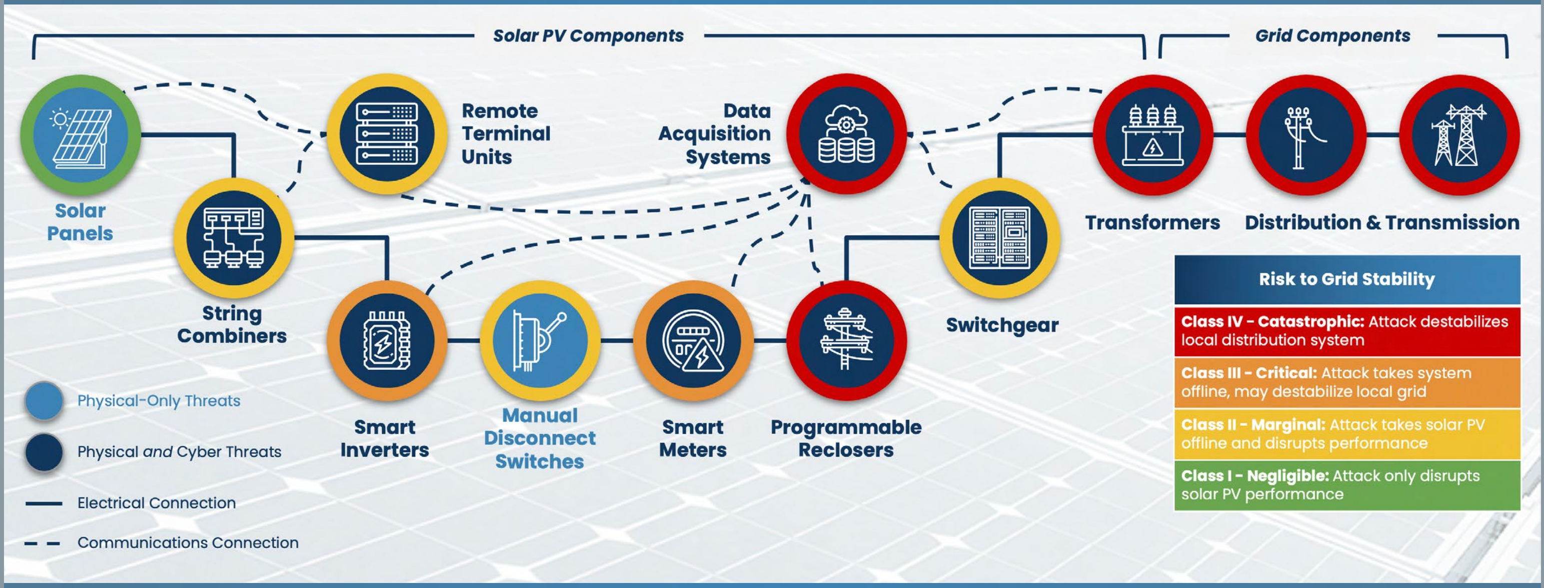
Overview | This element of the toolkit is designed to familiarize State Energy Officials and Public Utility Commission staff with the components found in solar energy systems. The schematic visualizes communications pathways to show how components are connected to one another for data transfer and controllability (both key factors for consideration in cybersecurity). The classification of risk in the Engineering and System Overview shows which components, if disrupted or compromised by a cyber attack, are capable of causing grid instability events. The risk assessments that follow later in the Decision Support Tool will assess the risk of individual components to cybersecurity threats and tools. This overview will inform state officials as they identify where risk is most prevalent in the grid, which components are specifically vulnerable, and what entities have the responsibility to mitigate those risks.

ADDITIONAL RESOURCES

A full version of the schematic can be found in Annex B. This includes the diagram below, in addition to helpful information about PV and grid components, such as:

- ❏ **Background:** The component's detailed function
- ❏ **Owner:** Who can execute changes in the component and assumes responsibility for secure operation from cyber risk
- ❏ **Vulnerability:** How the component is susceptible to a cyber threat
- ❏ **Risk to Grid Stability:** The degree to which an attack on this component affects grid operation

RISKS TO GRID STABILITY



COMMUNICATING RISK

Stakeholders | In addition to being included in State Energy Security Plans (SESP), solar cybersecurity risk information should be shared with state agencies including Emergency Management, the Department of Military Affairs/National Guard, and Homeland Security, which compile risk information into the Threat and Hazard Identification and Risk Assessment (THIRA). Additionally, this information can be used to support utilities and grid operators as they develop Energy Emergency Alert (EEA) criteria.

Cyber Attack Scenarios

Overview | Scenarios highlight potential consequences of inadequate cyber provisions for PV solar systems and propose state objectives to reduce the outlined risk. They reflect a variety of industry trends, such as how solar generation will be installed and what ownership structures may look like during the next decade. The guidance provides an understanding of PV vulnerabilities and attack types by outlining the consequences of an attack and how a breach might affect each stakeholder (e.g., utility, aggregator, consumer). State energy officials can use the scenarios to inform exercise planning, engage stakeholders, and provide context to risk analysis. Multiple scenarios were used to inform the Risk Assessment that follows later in this tool. Detailed versions of the cyber attack scenarios can be found in Annex C.

SCENARIO ELEMENTS

Attack Type

The primary cyber attack used to compromise an aspect or component of the solar PV system. Multiple attack types were used in the scenarios.

Targeted Component

The primary or initial component targeted by the cyber attacker. Each component was selected in the scenarios to match the attack type and importance to solar PV systems.

Damage to Component

The amount or degree of damage - requiring repair or replacement - to the attacked component. This matches the likely outcome of the attack type used in the scenario.

Impacts to the Bulk Power System

The potential amount of damage that the attack could cause on the bulk power system and/or in the local area. This depends on the attack type and components targeted in the solar PV system.

Scenario Description

The prompt provides additional details on the attack, affected components, and impact on the grid. Each description leverages real world events to increase realism.

Real World Example

Each scenario includes an article about a real world example of the attack type and impact to equipment. This provides a resource to review for additional details on attacks.

Stakeholders and Consequences

The primary stakeholders that are affected by the attack in the scenario and potential impacts if the attack is successful.

State Objectives to Alleviate Risk

Potential objectives that states could pursue to alleviate risks from the attacks in the scenarios. The suggestions are starting points and other objectives may help decrease risk.

SCENARIO PROGRESSION

Easy	Challenging	Difficult	Hard	
Distributed Denial of Service Attack on Remote Terminal Units	**Insider Threat Attack on String Combiners and Microgrid Controllers**	**Man-in-the -Middle and Ransomware Attack on Data Acquisition Systems**	**Advanced Persistent Threat and Zero-day Vulnerability on Smart Inverters**	**See Annex C for Detailed Versions of the Cyber Attack Scenarios**

Risk Assessment Process

OVERVIEW

Risk-Based Prioritization | There is a significant number of solar PV components for states to consider developing and implementing cyber risk policy and governance. Risk assessments for each component can help identify which are most susceptible to cyber attacks. This information, combined with the earlier assessment of grid disruption risk, will assist state officials to prioritize their policy efforts. This section outlines a **Probabilistic Risk Assessment (PRA)** model to classify and quantify the cyber risk of solar PV components using the five elements listed below using the Mitre Corporation Adversarial Tactics Techniques and Common Knowledge (ATT&CK) planning framework.

PROBABILISTIC RISK ASSESSMENT (PRA) MODEL

Component Vulnerability

An attacker's physical or cyber access to the component through direct or indirect (supply chain) means.

Indicator Weighting

The presence or lack of specific capabilities needed by adversaries to conduct a successful attack.

Consequence Severity

A successful attack's predicted impact on a component, based on the 10 identified variables.

Risk Mitigation

The effectiveness and deployment of tools, people, and systems to protect critical assets.

Attack Likelihood

The overall ease of execution for an attacker to target and compromise a component.

PRA VARIABLES

Description | Components must be assessed for the adversary capabilities needed to successfully attack them (indicators) and the availability/presence of technical tools to address them (mitigations):

Indicators

- **Expertise/Difficulty -** Perceived technical difficulty of an attack
- **Special Knowledge -** Attacker needs knowledge of unique systems
- **Specialty Equipment -** Tailored equipment needed for successful attack
- **Window of Opportunity -** Specific time or sequence window required to attack
- **Cost -** High cost of equipment, tools, or personnel to conduct an attack
- **Vulnerabilities and Exploits -** Understanding attack vectors

Scored on a scale of 0 (low indicator) to 9 (high)
*Window of Opportunity is binary 0 (no) or 1 (yes)

Mitigations

- **Firewall Configuration -** Firewall properly configured based on asset
- **Packet Inspection Technology -** Network packets inspected
- **Timing Inspection -** Network message timing captured, recorded reviewed
- **Network Disaggregation.** No/limited connections between IT/OT networks
- **DoS Security -** Presence of Denial of Service (DoS) security software or systems
- **Disaster Recovery -** Capacity to quickly restore system operation

Each is scored as a binary answer - 0 (not applicable/present) or 1 (applicable/present)

Probabilistic Risk Assessment Variables

Component Vulnerability Weighting

Description | The vulnerability of a specific component is assessed as a function of the four criteria listed below. The criteria relate to an attacker's ability to access or compromise a component and can be used to provide an indication of components that are inherently vulnerable.

Connected to OT/ICS Network
Carries the potential for remote access

Supply Chain Transparency
Visibility into hardware/software production

Remote Updates Pushed
The relative ease of updating security

Physical Security to Deter Tampering
Ability of attackers to access components

Scoring | Each component is scored as a binary assessment of 0 (not present) or 1 (present). The exception is Supply Chain Knowledge Depth, which carries a scale of 1 (total visibility) to 3 (no visibility) and rates an owner's ability to identify risk from unknown/untrustworthy subcontractors and vendors.

CONSEQUENCES

Description | The MITRE Att&CK framework measures consequences as a function of the nine impact areas listed below. They capture the degree to which a successful cyber attack can generate social, economic, and physical damage.

Financial - Lost revenue and cost of remediation for potential disruption

Environmental - Raw product spills, fires, contamination due to asset failure

Reputational - Impact of security breach in the eyes of public/investors

Operational - Disruption in business continuity or system functionality

Safety (Staff) - Potential for employees to be injured due to misoperation

National Security - Ability to conduct critical defense missions

Safety (Public) - Possibility of customers/bystanders to be harmed

Bulk Power System Operations - Impact beyond local grid reliability

Governance- Ramifications of breach; or misoperation of or public trust in government entities

Total score reflects aggregated predicted consequences

Scoring | Each component is evaluated on a scale from 0 (not present) to 10 (severe). Scores are determined using a blend of quantitative and qualitative factors for each component, based on a user's knowledge and understanding of each component.

Probabilistic Risk Assessment Methodology

Category	Variable	Raw Score	Weighting	Risk
Indicators	Expertise/Difficulty	Minimum total score of 0 (weakest indicators) to 37 (strongest) based on the sum of 5 individual variables	Combined scores from each category are used to determine the overall likelihood weighting	Scores are combined to calculate an overall risk rating
	Special Knowledge			
	Specialty Equipment			
	Window of Opportunity			
	Cost			
Mitigations	Firewall	Minimum total score of 0 (fewest mitigations) to 6 (most mitigations) based on the sum of 6 individual variables		
	Packet			
	Timing			
	Air Gap			
	OT/IT Network Disaggregation			
	DoS Security			
Component Vulnerability Weighting	Existence of OT/ICS Network	Minimum total score of 0 (lowest vulnerability) to 6 (highest)	Combined scores from each category are used to determine the overall impact weighting	
	Remote updates pushed			
	Supply chain knowledge depth			
	Physical Access			
Consequences	Financial	Minimum total score of 0 (lowest consequence) to 90 (highest) based on the sum of 9 individual variables		
	Reputational			
	Safety (staff)			
	Safety (public)			
	Political			
	Environmental			
	Operational			
	National Security			
	Bulk Power System Operations			

Risk Assessment Worksheet

Category	Variable	Raw Score	Weighting	Risk
Component Vulnerability Weighting	Existence of OT/ICS Network		A multiplier (0.0-1.0) Determined by the user as an estimate of overall impact of an attack based the vulnerability of a component and the anticipated consequences	Total risk score based on the weighted results
	Remote updates pushed			
	Supply chain knowledge depth			
	Physical Access			
Scale: 0-1, ** *note: supply chain knowledge depth carries a 1- 3 scale*				
Consequences	Financial			
	Reputational			
	Safety (staff)			
	Safety (public)			
	Political			
	Environmental			
	Operational			
	National Security			
	Bulk Power System Operations			
Scale: 0-10				
Indicators	Expertise/Difficulty		A multiplier (0.0-1.0) determined by the user as an estimate of overall likelihood of an attack based on the presence of indicators and the use of effective mitigations.	
	Special Knowledge			
	Specialty Equipment			
	Window of Opportunity			
	Cost			
Scale: 0-9 ***note: Window of opportunity is binary 0 (no) or 1 (yes)*				
Mitigations	Firewall			
	Packet			
	Timing			
	Air Gap			
	OT/IT Network Disaggregation			
	DoS Security			
Scale: 0-1, scored as a binary- 0 (not applicable/ present) or 1 (applicable/ present)				

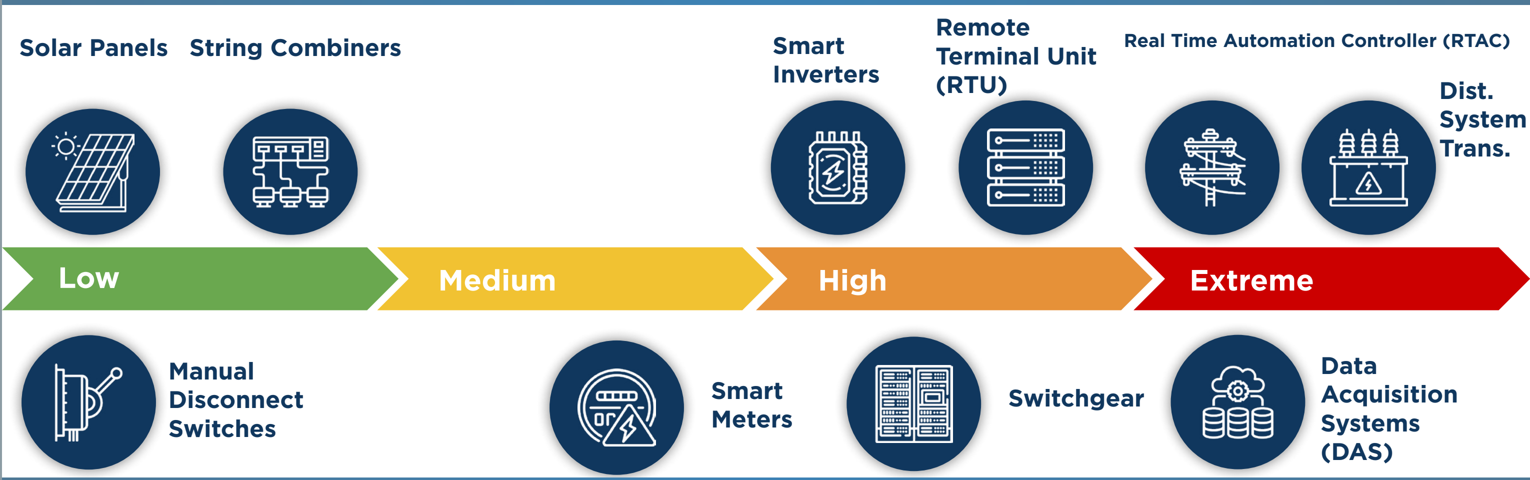
Risk Analysis Results

RESULTS OVERVIEW

Overview | This section summarizes the results of a comparative cyber attack risk analysis that was conducted for specific solar PV system components. This section also describes the Probabilistic Risk Assessment (PRA) methodology used to conduct the analysis.

PRA Results | Subject Matter Experts from Academia, National Labs, a Utility, DHS CISA and the US Army completed PRA scoring on 10 solar PV components identified in the Engineering and System Overview (grid components were not in scope of this tool). The results are listed below and reflect the input of all PRA variables and the weighted assessment of attack likelihood. State officials can use these results to identify the components with the highest priority for mitigation strategy development and implementation using state policies.

COMPONENT RISK SUMMARY



EXAMPLE: HOW TO USE PRA RESULTS

Reference Engineering and System Overview to identify PV components with grid disruption risk

Determine selected PV component individual cyber risk with PRA results or template

Use Risk Ownership Framework to determine entity with mitigation responsibility

Review Policy Quick Guide to identify the most relevant policy or governance option

Develop state policy for cyber risk mitigation

PRA Results | Detailed scoring for individual components is listed following the PRA methodology overview.

Risk Analysis Template

SELF-ASSESSMENT

Instructions | State Energy Officials can complete their own risks assessments for any grid component using this format. Technical subject matter expertise is needed to assign a score to each PRA variable based on the users' knowledge and open-source research. The scores can be totaled for each of the four PRA result columns listed below as a means to compare the "raw" risk levels of components. The user will also determine the likelihood of an attack as a function of the relative technical ease to conduct the attack. This will provide the overall risk score. The following pages contain the detailed results for each solar PV component analysis presented using the standard format shown below.

EXAMPLE

Name of Component

COMPONENT SUMMARY | Brief Overview of the technical capabilities of the component and its role/location in the schematic

Notes from SMEs with information regarding the scoring for individual variables in the criteria categories is listed below.

PRA Results

X — Component Vulnerability Weighting **High**

X — Indicator Weighting **High**

X — Consequence Severity **High**

X — Risk Mitigation **Medium**

Cyber Attack Likelihood **Extreme**

Overall Risk Level — **Combined scores with weighting**

Vulnerability	Indicator	Severity	Mitigation	Likelihood
Scores ≤ 2 result in a low risk rating, reflecting few known vulnerabilities in a component, 3+ results in high rating	Low score indicates easy adversary access to attack tools or capabilities: 0-19: High 20-28: Medium 29+: Low	Rating scale for severity reflects the degree to which a cyber compromise causes damage: 0-25: Low 26-40: Medium 41-60: High 61-90: Extreme	The availability and use of more technical mitigation tools reduces overall risk: 0-1: High 2-3: Medium 4-6 Low	Assessed as a function of the relative ease of attack (tools, systems, adversaries) to weight results. High likelihood "amplifies" PRA scores

Results Summary

SOLAR SYSTEM

Solar System

COMPONENT SUMMARY | All solar systems include solar modules made up of individual solar cells that produce direct current (DC) electricity from sunlight.

- ❏ Minimal points of connection and no networking
- ❏ Lack of IT/OT points of entry does not generate targeting
- ❏ Disruptions limited to single assets/sites
- ❏ Limited policy and governance strategies and tools available
- ❏ Direct attack highly unlikely

PRA Results

2	Component Vulnerability Weighting	**Medium**
28	Indicator Weighting	**Medium**
11	Consequence Severity	**Low**
2	Risk Mitigation	**Medium**
	Cyber Attack Likelihood	**None**

Overall Risk Level Low

MANUAL DISCONNECT SWITCHES

Manual Disconnect Switches

COMPONENT SUMMARY | Most solar PV includes a manual disconnect switch for disconnecting the system from the grid during maintenance or emergencies.

- ❏ Requires physical access
- ❏ No active targeting
- ❏ Impacts would be very localized
- ❏ Mitigation tied to physical access
- ❏ Readily available risk mitigation resources

PRA Results

3	Component Vulnerability Weighting	**High**
12	Indicator Weighting	**High**
9	Consequence Severity	**Low**
2	Risk Mitigation	**Medium**
	Cyber Attack Likelihood	**Low**

Overall Risk Level Low

Results Summary

STRING COMBINERS

String Combiners

COMPONENT SUMMARY | Combiners control rows or "strings" of panels and measure the electrical current, voltage and temperature, providing protection against electrical surges and overcurrents that could cause damage.

- ❑ Limited connections and simple software + hardware
- ❑ Risk of data corruption and connectivity loss
- ❑ Impacts are likely to be localized
- ❑ Effective software/hardware mitigation available
- ❑ Low consequences decrease likelihood of targeting

PRA Results

Risk Mitigation	Indicator Weighting	Consequence Severity	Risk Mitigation	Cyber Attack Likelihood
2	29	25	3	
Medium	**Medium**	**Low**	**High**	**Low**

Overall Risk Level **Low**

SMART METERS

Smart Meters

COMPONENT SUMMARY | An electrical meter records the amount of power and energy produced by the solar PV and provides the information necessary for utilities, project developers, and customers to buy and sell the energy.

- ❑ Extensive supply chains and connectivity increase vulnerability.
- ❑ Potential means of compromise readily available.
- ❑ Impacts would be very localized.
- ❑ Readily available risk mitigation resources.
- ❑ Targeting unlikely.

PRA Results

Component Vulnerability Weighting	Indicator Weighting	Consequence Severity	Indicator Weighting	Cyber Attack Likelihood
2	19	29	19	
Medium	**High**	**Medium**	**Medium**	**Medium**

Overall Risk Level **Medium**

Results Summary

SMART INVERTERS

Smart Inverters

COMPONENT SUMMARY | Inverters convert direct current (DC) electricity generated by a solar panel to alternating current (AC) electricity which is used on the grid. More information can be found on the Solar Energy Technology Office Website.

- Extensive supply chains and connectivity increase vulnerability
- Active target for vulnerabilities from adversarial countries (based on country of manufacture)
- Compromise can impact local grid stability quickly
- Readily available risk mitigation resources
- Ubiquity increases risk

PRA Results

Component Vulnerability Weighting	Indicator Weighting	Consequence Severity	Risk Mitigation	Cyber Attack Likelihood
3	19	48	3	
High	**High**	**High**	**High**	**High**

Overall Risk Level **High**

SWITCHGEAR

Switchgear

COMPONENT SUMMARY | The switchgear monitors and controls the voltage and frequency of the electricity being sent to the local distribution system.

- Integration with local control system assets presents risk.
- International supply chain with poor controls.
- High potential for safety risk.
- Relatively accessible

PRA Results

Component Vulnerability Weighting	Indicator Weighting	Consequence Severity	Risk Mitigation	Cyber Attack Likelihood
2	22	57	0	
Medium	**Medium**	**High**	**High**	**Low**

Overall Risk Level **High**

Results Summary

REMOTE TERMINAL UNITS

Remote Terminal Units

COMPONENT SUMMARY | A small computer located near the solar PV that collects data, such as how much electricity it is generating, and aggregates that data for delivery over a wired or wireless data link.

- IT/OT data linkage creates potential for remote access
- Tools and capabilities to target are readily available
- Disruptions will impact local grid asset visibility
- Readily available risk mitigation resources
- A common target for adversaires to gain visibility

PRA Results

Component Vulnerability Weighting	Indicator Weighting	Consequence Severity	Risk Mitigation	Cyber Attack Likelihood
3	19	30	2	
High	**High**	**Medium**	**Medium**	**High**

Overall Risk Level **High**

REPROGRAMMABLE RECLOSERS & RTACs

Repro-grammable Reclosers and RTACs

COMPONENT SUMMARY | A circuit, like a light switch, that is both automated and remotely controlled by the utility using a wireless or wired data signal. If the recloser senses a "fault" on the local electric lines, the recloser opens the circuit, cutting the flow of power (equivalent to turning a light switch off).

- Multiple points of connection and network access
- Malware is easily/cheaply accessible and does not require sophisticated actors
- Can impact multiple assets simultaneously
- Mitigation is largely effective but requires vigilance
- Common target for attack

PRA Results

Component Vulnerability Weighting	Indicator Weighting	Consequence Severity	Risk Mitigation	Cyber Attack Likelihood
3	16	48	2	
High	**High**	**High**	**Medium**	**Extreme**

Overall Risk Level **Extreme**

Results Summary

DATA ACQUISITION SYSTEMS

Data Acquisition Systems (DAS)

COMPONENT SUMMARY | Sensors and controls are installed in the equipment listed below, and collect data that is aggregated by the DAS system and delivered wirelessly to a remote server.

- ❑ Highly interconnected (IT/OT) device with persistent access
- ❑ Malware is easily/cheaply accessible and does not require sophisticated actors
- ❑ Can impact multiple assets simultaneously
- ❑ Mitigation is largely effective but requires vigilance
- ❑ Common target for attack

PRA Results

Component Vulnerability Weighting	Indicator Weighting	Consequence Severity	Risk Mitigation	Cyber Attack Likelihood
2	16	48	3	
Medium	**High**	**High**	**Medium**	**Extreme**

Overall Risk Level **Extreme**

DISTRIBUTION SYSTEM TRANSFORMERS

Distribution System Transformers

COMPONENT SUMMARY | The first piece of equipment between the local electric distribution system and the solar PV system, transformers convert high-voltage current delivered by regional transmission lines to lover voltage for customer usage.

- ❑ Remote-accessible, some physical security measures
- ❑ Most manufacturing occurs internationally including in adversarial countries
- ❑ Outages can cause distribution disruption and possible BPS instability
- ❑ Limited spares available to replaced damaged assets
- ❑ Actively targeted by adversaries

PRA Results

Component Vulnerability Weighting	Indicator Weighting	Consequence Severity	Risk Mitigation	Cyber Attack Likelihood
2	19	64	0	
Medium	**High**	**Extreme**	**High**	**High**

Overall Risk Level **Extreme**

Risk Ownership Framework

OVERVIEW

Roles and Responsibilities | The Probabilistic Risk Analysis (PRA) identifies the solar PV components with the highest risk of cyber disruption as a function of likelihood and impact. This analysis also highlights the presence or effectiveness of mitigation strategies. Not all solar components fall under the purview of a single owner (or even owner type). As a result, ownership of these risks - and the responsibility to mitigate them - must be identified in order to determine the most effective mix of policy, regulation, codes, and standards to address them. Risk ownership is a combination of where solar PV systems or components physically "reside" in the grid, and the involvement of different categories of owners, as described below.

OWNER CATEGORIES

Operators

Utilities at the transmission and distribution level, Reliability Coordinators (RC), Independent System Operators (ISO), utility scale solar operators

Users

End-use customers, Distributed Energy Resource (DER) owners (e.g., rooftop solar), market participants, and entities dependent on operator systems.

Vendors

Component manufacturers in the solar asset supply chain, contract hardware/software, technical solution providers, consultants/ integrators

Note: Each owner category is subject to varying degrees of regulatory, legal, contractual or compliance oversight depending on their scale of operation, corporate status, or jurisdictional disposition.

GOVERNANCE AND POLICY STRATEGIES

Applicability | Not all regulations, codes, and standards will apply to all categories of ownership. When selecting a governance or policy strategy, users will need to assess whether the owner responsible for risk is subject to compliance in a mandatory or voluntary manner. The Standards Quick Guide in Annex A identifies how specific policies and strategies are relevant to individual solar PV components.

High Relevance

Provide foundational requirements for systems and components that are both susceptible to an attack and critical for preventing operational disruptions to electricity systems. They also have direct application to solar energy assets for both hardware and software. Content with this designation should be considered as a high priority for incorporation in state policy or regulation.

Medium Relevance

Provide important requirements for systems and components that are both susceptible to attack and important for preventing operational disruptions to electricity systems. Not all have direct applications to solar energy assets for both hardware and software but are still useful to building out a comprehensive cybersecurity strategy.

Low Relevance

Provide informational requirements for systems and components that are less likely to be attacked or result in operational disruptions to electricity systems. Not all have direct applications to solar energy assets for hardware or software but are still useful to building out a comprehensive cybersecurity strategy.

Governance and Policy Strategies

Compatibility and Effectiveness | The Standards Quick Guide in Annex A provides a detailed breakdown of some relevant codes, standards, and regulation to support risk mitigation. Below is a reference table for five categories of options for state officials to consider for integration into state policy: 1) Industry Standards, 2) Voluntary Frameworks, 3) Consensus-based codes, 4) Mandatory Standards, and 5) Market Tariffs. Each is color-coded using the format introduced in the Risk Ownership Framework on page 18 based on their relevance to solar PV components. Users can identify strategies that align with jurisdictional and legislative authority for adoption or implementation.

MITIGATION APPLICATIONS

Industry Standards	**IEEE 1547.1-2020** Test Procedures for DERs and Interfaces	**IEEE 1547.2-2008** Application Guide for Std 1547
	IEEE 1547.3-2007 Cybersecurity and Information	**IEEE 1547.4-2011** Island Systems
	IEEE 1547.6-2011 Recommended practices for DER connections	**IEEE 1547.7-2013** Guide for Impact Studies for DER Interconnection
	IEEE P-2800 Interconnection and interoperability of Inverter-Based Resources	
Voluntary Frameworks	**NIST** Cybersecurity Framework (CSF)	**NIST** SP 800-82 Revision 2
	MITRE ATT&CK Framework	**DOE** ES-C2M2
Consensus-Based Codes	**IEC 62443** Industrial Automation and Control System Security	**IEC 60870** Telecontrol Equipment and Systems
	IEC 62351 Info Security for Power System Control Operations	**IEC 61850: 2022** CommNetworks for Power Utility Automation
Mandatory Standards	**NERC** CIP-002-5.1a BES Cyber System Categorization	**NERC** CIP-006-6 Physical Security of BES Cyber Systems
	NERC CIP-003-8 Security Management Controls	**NERC** CIP-007-6 System Security Management
Market Tariffs	**Procurement Language** Hardware/software supply chain integrity	**California Public Utility Commission** Rule 21 Interconnection Requirements

Risk Ownership Crosswalk

OVERVIEW

Determine Ownership | Solar PV components from the Engineering Overview in Annex B are listed below based on their Grid Disruption Risk Level and their overall risk identified by Probabilistic Risk Assessments. Additionally, the risk owner is identified to aid in the selection of policy strategies that are applicable and impactful based on the component and the entity who owns responsibility. The state role lists options that will allow policymakers the ability to utilize existing pathways for engagement with organizations responsible for the development of codes, standards, and regulation.

OWNERSHIP CHART

Risk Level	Components	Owner	Governance/ Policy	State Role
Class IV - Catastrophic: Attack destabilizes local grid depending on asset size	❏ Programmable Reclosers ❏ Transformers ❏ Data Acquisition Systems	❏ Operator ❏ Vendor	❏ Industry Standards ❏ Consensus based codes ❏ Mandatory Standards	❏ Task Force participation ❏ NOPR Comments ❏ Stakeholder engagement ❏ Legislation and policy development
Class III - Critical: Attack takes system offline, destabilizes local distribution system	❏ Smart Meter ❏ Smart Inverters	❏ Operator ❏ User ❏ Vendor	❏ Market Tariffs ❏ Consensus based codes ❏ Voluntary frameworks ❏ Procurement Language	❏ Tariffs and interconnection requirements ❏ Framework development
Class II - Marginal: Attack takes system offline, disrupts solar asset performance	❏ Remote Terminal Unit ❏ String Combiners ❏ Manual Disconnect ❏ Switches ❏ Switchgear	❏ Operator ❏ Vendor	❏ Industry standards ❏ Procurement Language ❏ Consensus based codes	❏ State policy ❏ Framework development
Class I - Negligible: Attack only disrupts solar asset performance	❏ Point of Interconnection (POI) ❏ Solar Panels	❏ Vendor ❏ User	❏ Procurement Language ❏ Voluntary frameworks	❏ Tariffs and interconnection requirements

Decision Support Example

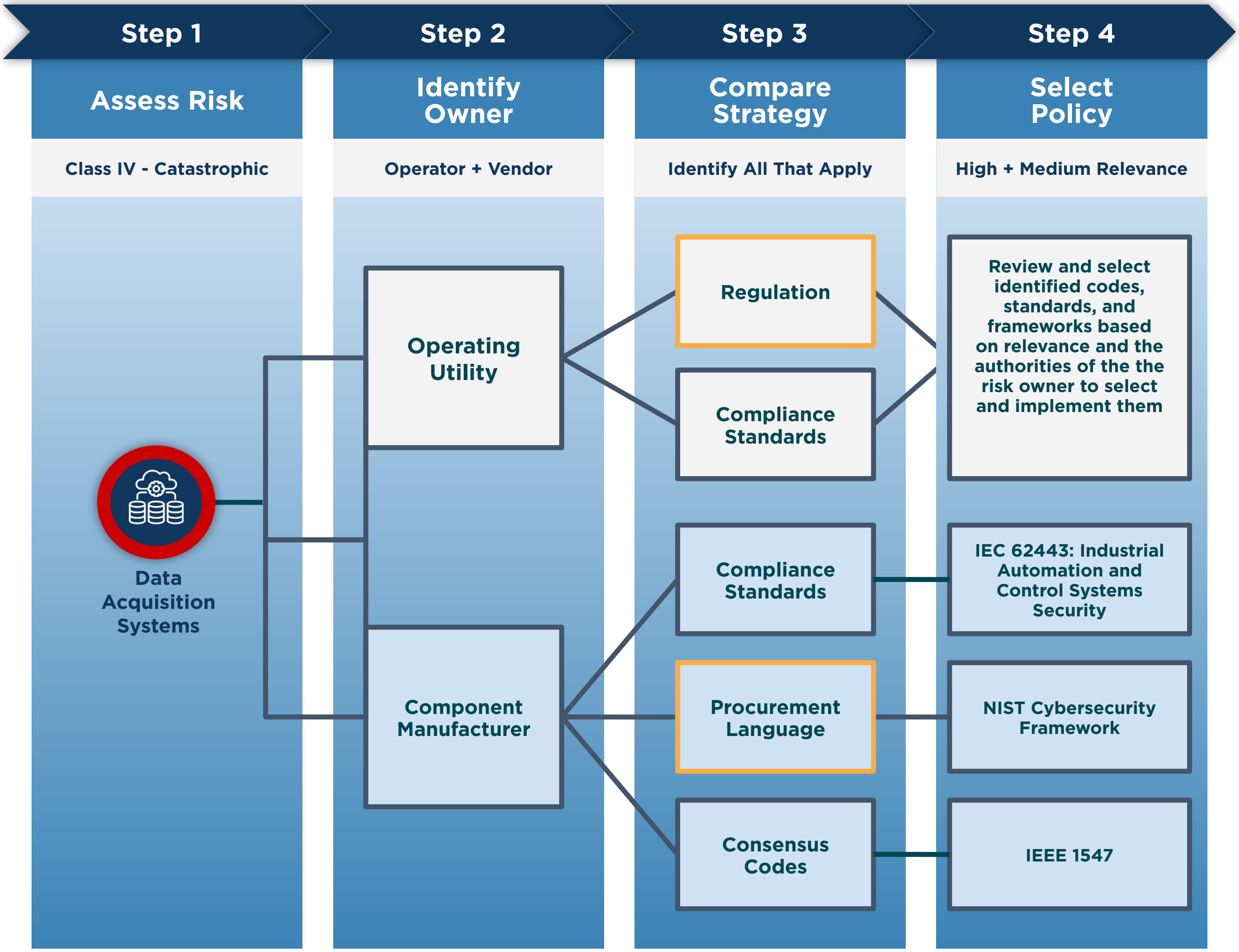
Resource Integration | The Decision Support process helps the user in evaluating the highest priority actions based on component risk, ownership, and policy effectiveness.

INITIAL QUESTIONS

Risk Assessment | Which components and associated risks are the most important to mitigate?

Owner | Who has the responsibility and the authority to identify, create, and implement governance or policies?

EVALUATION STEPS



= State Role

Implementation Process

Final Step | After navigating the decision support tool, state users should be able to identify the solar components that pose the greatest risk, identify the primary owner(s) of that risk, compare the available mitigation strategies, and identify the most effective codes, standards and regulations available. States can use this information to develop policies or new regulations, or to engage stakeholders with the ability to create or enforce policy if the state does not have the required authority. States should evaluate their options as a function of three means to implement risk mitigation strategies: **1) Policy Guidance, 2) Stakeholder Input, or 3) Direct Authority.**

IMPLEMENTATION PATHWAYS

Policy Development

States can develop and implement policies and plans that impact cybersecurity for public and private entities:

- State Energy Security Plans (SESP) are required in every state and outline the cybersecurity conditions of the state's energy sector. They can include overviews of state policy and activities pertaining to cybersecurity, and utility and energy provider cybersecurity plans, policies, and procedures
- State Energy Offices, Public Utility Commissions (PUC), Emergency Management Agencies (EMA), and state IT can coordinate on joint planning for cybersecurity preparedness, response, recovery and mitigation by developing public-private coordination guidance, energy emergency exercises, risk and consequence assessments, and state policies, among others

Stakeholder Input

States have access to several means of providing input on codes, standards, and regulation development forums:

- Organizations such as IEEE maintain a recurring process of developing and approving consensus-based codes that impact cybersecurity. Participation in working groups is voluntary and open to all members
- Mandatory and voluntary standards developed by FERC and NERC include working groups and open comment periods for states to contribute feedback and recommendations for new and updated federal or industry standards

Direct Authority

States have several resources at their disposal in the form of policies and plans that impact cybersecurity:

- State regulatory processes includes the ability to develop and enforce cyber standards for utilities under their purview. They can be adapted from Federal regulation or created to address specific risks
- Procurement language can adopted by states to guide in-state utilities in the purchase of equipment and services. This is also relevant through state-eligible programs such as IIJA Section 40107 and 40103(b), which require cybersecurity plans

List of Annexes