NASEO
National Association of State Energy Officials

Standards Quick Guide

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

Standards Quick Guide

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

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

This material is based upon work supported by the U.S. Department of Energy (DOE) under award number DE-EE0009004. This report was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof.

About the Project

The Cybersecurity Advisory Team for State Solar (CATSS) is a project implemented by the National Association of State Energy Officials (NASEO) and the National Association of Regulatory Utility Commissioners (NARUC) to aid in mitigating cybersecurity risks and consequences in solar energy developments. With support from the United States Department of Energy Solar Energy Technologies Office, the project leverages state, federal and private-sector expertise on cybersecurity, grid and photovoltaic to identify and model cybersecurity programs, policies, and actions for states to take in partnership with utilities and the solar industry.

Acknowledgements

The authors of this paper are Dakota Roberson from the University of Idaho and Shoshana Cohen, Jack Graul, Jonathon Monken, and Alex Pina, from Converge Strategies, LLC (CSL). The authors would like to gratefully acknowledge the input and feedback from the project Advisory Group.

The authors also thank Sarah Trent and Kirsten Verclas from National Association of State Energy Officials (NASEO), their partners at the National Association Regulatory Utility Commissioners (NARUC), and at the Department of Energy (DOE) Solar Energy Technology Office (SETO) for their leadership and guidance.

Executive Summary

This Standards Quick Guide contains a list of relevant standards developed or in development for the cybersecurity of solar energy resources and is the first of several guidance documents. It outlines different types of standards, such as industry standards, enforceable regulations, and conceptual relevant cybersecurity studies. The role of states in the scoping, development, implementation and enforcement of the standards outlined here varies widely depending on the issuing organization and the use of state legislation. The responsibility to mandate a standard, or encourage use of any one standard, is dependent on a state's legislative authority. This resource should not be viewed as a prescriptive tool, but an educational tool.

States may use this quick guide as a tool to enhance understanding of existing standards and for brainstorming new ideas to help states improve the cybersecurity of solar energy resources in their jurisdiction through innovative policy.

The different types of standards highlighted in this guide are briefly explained below.

Industry standards are developed by subject matter experts through an iterative process in which SMEs draft, debate, test and refine the standard. The process is typically initiated by a relevant professional society or standards body such as the Institute of Electrical and Electronics Engineers (IEEE) or the International Electrotechnical Commission (IEC). Working Groups are usually globally inclusive and operate publicly by publishing meeting minutes, in addition to publishing peer-reviewed journal articles and papers highlighting emerging issues and new ideas. In the case of cybersecurity for solar energy assets, IEEE has a working group dedicated to 1547.3, the "Guide for Cybersecurity of DERs Interconnected with Electric Power Systems." Discussions are led by a chairperson who also serves as the contact for technical inquiries, and all IEEE members are invited to participate in working groups. This inclusiveness allows State Energy Offices and Public Utility Commissions (PUCs) the opportunity to participate in technical conferences, content reviews, and publishing activities. No individual has the authority to set an industry standard, they can only be set through deliberation and consensus. The standards do not carry the weight of law or financial penalty, instead they are used as a means of codifying existing best practices for the purpose of improving interoperability and simplifying specifications for manufacturers. The inclusivity and transparency of this process allows participants to better understand technical trends and engage with subject matter experts.

Regulatory standards are developed by federal regulatory bodies such as the Federal Energy Regulatory Commission (FERC). As the result of the Energy Policy Act of 2005, enforcement of FERC regulations and standards pertaining to electric grid reliability is the purview of the designated Electric Reliability Organization (ERO) - currently the North American Electric Reliability Corporation (NERC). This body is a private organization that works with FERC to ensure proper development and enforcement of reliability standards through regular auditing and review of the systems and policies of companies they regulate. States have a limited ability to impact the development of federal regulation, relying instead on participation in working groups to voice the concerns and needs of states. Additionally, the states are able to provide comments and input during hearings that follow a Notice of Proposed Rulemaking (NOPR), which indicates the intent of FERC to issue a new order. With regards to NERC standards, the opportunity for states to engage is even more limited.

Other concepts relevant to this body are produced by various federal and state agencies, national laboratories, federally funded research and development centers (FFRDCs), think tanks, universities, and other independent bodies. They help to inform the rapidly evolving cybersecurity sector on up-to-date threats, cutting edge defense concepts, and industry best practices. They also tend to influence and interact with industry standards formally and informally, as many of the concepts which begin in these documents and discussions aid in the iterative working group process. For the purpose of this Quick Guide, the following terms will be used in a non-interchangeable manner:

Code: A principle developed to establish a minimum criterion 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 an authority

General Cybersecurity Frameworks Overview

Governments, international associations, and regulatory authorities develop numerous cybersecurity frameworks that provide guidance on how to improve the security of hardware, software and human operators. These can be applied to a wide range of infrastructure sectors, including electric power. Given the breadth of technical detail and the variance in applicability to components of the solar energy value chain, it is necessary to identify the frameworks based on their relevance to aid in mitigating cyber risk for relevant systems and components. Users of this guide should consider the designations provided as a means of considering what codes, standards or regulations are most capable of addressing cybersecurity risk specifically as it applies to assets in the solar value chain. Additionally, they are also sorted based on the ability of State Energy Offices and PUCs to utilize or employ them as a policy or regulatory tool to address cyber risk within their jurisdiction.

High Relevance

Standards, consensus-based codes, and frameworks designated as *High Relevance* are those which provide foundational requirements for systems and components that are both susceptible to attack and critical to 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

Codes, standards, and frameworks designated as *Medium Relevance* provide important requirements for systems and components that are both susceptible to attack and important to 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

Codes, standards, and frameworks designated as *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.

General Cybersecurity Frameworks Summary

Relevance for codes, standards and frameworks to the solar value chain are ranked based on several criteria, including direct applicability to solar assets, industry acceptance, completeness, scope, enforceability, maturity, and influence on standards and/or other regulations.

A highly relevant standard such as the IEC 60870, for example, is wide-reaching across many solar installation components, has ongoing Technical Committee or Working Group oversight. It has substantial influence on regulation structures and is generally accepted by the power system automation industry. In contrast, the NERC Critical Infrastructure Protection (CIP) Program is of medium relevance due to its lack of direct applicability and enforceability for small-to-medium sized solar installations, regardless of the fact that it is mature, accepted by industry, enforceable, and wide-reaching in scope.

The following table provides a high-level overview of relevant cybersecurity codes, standards, and frameworks and prioritizes them by relative importance that apply to solar photovoltaic systems.

ORGANIZATION	CODE, STANDARD, FRAMEWORK TITLE	RELEVANCE
IEEE	IEEE 1547	**High**
National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework (CSF)	**High**
IEC	IEC 62443: Industrial Automation and Control Systems Security *	**High**
IEC	IEC 60870: Telecontrol Equipment and Systems*	**High**
NERC	NERC CIP	**Medium**
IEC	IEC 62351	**Medium**
IEEE	IEEE 2030.5-2018	**Medium**
IEC	IEC 61850: 2022 *	**Medium**
NIST	NIST 800	**Low**
MITRE Corporation	ATT&CK Framework	**Low**
NIST	NIST SP 800-82 Revision 2	**Low**
NIST	NIST Interagency/Internal Report 7628	**Low**
NERC	NERC Reliability Guideline	**Low**
IEC	IEC 61968 *	**Low**
Department of Energy (DOE)	DOE/DHS ES-C2M2	**Low**
DOE	DOE/NIST/NERC RMP	**Low**
Department of Homeland Security (DHS)	DHS NCCIC and ICS-CERT	**Low**
Underwriters Laboratories (UL)	Potential new UL/ISA Standard	**Low**

Table 1. Codes, Standards, and Frameworks Summary Table

Note: For the purposes of this document, primary voltage is denoted as 2,300 to 39,000 volts. Common secondary voltages include 120, 208, 240, 277 and 480 volts.

HIGH RELEVANCE Codes, Standards, Frameworks

Institute of Electrical and Electronics Engineers 1547: Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces

IEEE 1547 provides technical specifications for and testing of interconnection and interoperability between Bulk Power System (BPS) and Distributed Energy Resources (DER). IEEE 1547 is the national standard for Distributed Energy Resource interconnection in the United States. IEEE is the professional society which provides the standards. Original equipment manufacturers (OEMs) choose to adopt them or not. States can mandate that pieces of equipment be certified to meet a standard such as this. Note: This standard is neutral to Distributed Energy Resource type and covers Distributed Energy Resources at typically primary and/or secondary distribution voltages. Adoption is widely recognized by industry, original equipment manufacturers, and regulators. Importantly, it is the primary vehicle for ensuring conformance to common security standards across system types and provides a consistent framework for utilities to follow. Application Guides (below) complement and expand on and clarify the initial standard adopted in 2003 and codified through the Energy Policy Act of 2005.

IEEE 1547 Standards (Application Guides)	
1547.1-2020	Test Procedures for DERs and Interfaces
1547.2-2008	Application Guide for Std 1547
1547.3-2007	Cybersecurity and Information**
1547.4-2011	Island Systems
1547.6-2011	Recommended Practices for DER Connections on Secondary Networks
1547.7-2013	Guide for Conducting Distribution Impact Studies for DER Interconnection

Table 2. IEEE 1547-2018 Standards (i.e., Application Guides)

National Institute of Standards and Technology Cybersecurity Framework

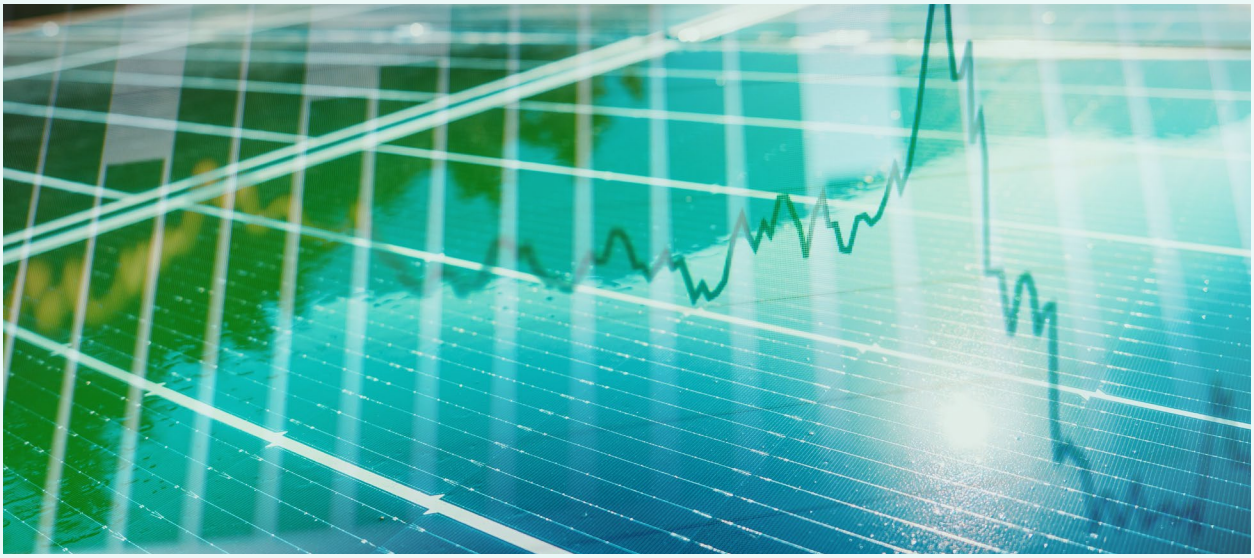
The Cybersecurity Framework (CSF) directs NIST to develop a voluntary framework – based on existing standards, guidelines, and practices – with industry and government stakeholders to reduce critical infrastructure cyber-risks. It was the result of the February 2013 Presidential Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*. It was further enhanced by the Cybersecurity Enhancement Act of 2014. The CSF is a generally adopted resource upon which most cybersecurity applications are built, making it highly relevant to regulators and practitioners alike. Additionally, the CSF is the primary framework used by the U.S. Department of Homeland Security, and it informs the development of state cyber security strategies implemented by emergency management personnel. As such, it represents an important tool of coordination between state agencies to reconcile policy with legislation, regulation, and industry best practice. It can be adapted to address cyber risk to solar assets.

International Electrotechnical Commission 62443: Industrial Automation and Control Systems Security

IEC 62443 is a set of international standards which addresses cybersecurity for operational technology (OT) in automated industrial control systems (ICS). The standards outline technical and human aspects of automation and associated cybersecurity topics categorized by stakeholder (operators, service providers, and manufacturers) using standard risk management approaches. It is one of the broadest international standards with applicability to a range of components which interact with the solar energy value chain at numerous operational levels.

International Electrotechnical Commission 60870: Telecontrol Equipment and Systems

IEC 60870 defines systems used for telecontrol (i.e., supervisory control and data acquisition (SCADA)) (60870-5). Pertinent subsections of IEC 60870 include: 1, 2, 3, 101, 103, 104. Because distributed assets such as solar photovoltaic can and will continue to adopt telecontrol/SCADA systems for monitoring and control, this standard will continue to be highly relevant into the future



MEDIUM RELEVANCE Codes, Standards, Frameworks

North American Electric Reliability Corporation Critical Infrastructure Protection

NERC Critical Infrastructure Protection (CIP) is a set of regulations adopted in 2008 to secure assets required for operating North America's BPS. NERC Regional Entities are responsible for *auditing* and *enforcement* of the CIP standards. NERC CIP is marked as medium relevance because most solar installations are smaller than 75MW. NERC CIP only applies to installations larger than 75MW. While CIP *does not currently apply to rooftop solar*, it could potentially apply to aggregated DERs through future adoption of FERC Order No. 2222 - "Participation of Distributed Energy Resource Aggregations in Markets Operated by Regional Transmission Organizations and Independent System Operators". FERC released a Notice of Proposed Rulemaking January 20, 2022, regarding internal network security for high- and medium-impact bulk electric system cyber-systems – with it, FERC wishes to "address concerns that the existing standards do not address potential vulnerabilities of the internal network to cyber threats", so a new CIP control family can be expected soon. While CIP is foundational to the overall cybersecurity of the Bulk Electric System, the designation as "Medium" relevance for the purpose of this guide is a reflection of its interstate-scale scope which limits the ability of states to influence it, and the lack of standards directly addressing the solar value chain.

Control Families Enforced by CIP***	
CIP-002-5.1a	BES Cyber System Categorization
CIP-003-8	Security Management Controls
CIP-004-6	Personnel and Training
CIP-005-6	Electronic Security Perimeter(s)
CIP-006-6	Physical Security of the BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-6	Incident Reporting and Response Planning
CIP-009-6	Recovery Plans for BES Cyber Systems
CIP-010-3	Configuration Change Management and Vulnerability Assessments
CIP-011-2	Information Protection
CIP-013-1	Supply Chain Risk Management
CIP-014-2	Physical Security

Table 3. Control Families Enforced by CIP

International Electrotechnical Commission 62351: Information Security for Power System Control Operations

IEC 62351 provides cybersecurity guidelines for power system communications. The standard includes recommendations for a number of emerging communications protocols, including Generic Object-Oriented Substation Event (GOOSE), sampled value, routable-GOOSE, etc. It provides guidance for managing the transition between the large number of available communication protocols to those which are presently emerging as popular and robust.

Institute of Electrical and Electronics Engineers 2030.5-2018: "Smart Energy Profile" Application Protocol

IEEE 2030.5 defines application protocols which enable the end-user energy environment to be managed by the utility. These include demand response and other types of load modulation, real-time pricing, distributed generation management, etc. It is built upon information and recommendations emanating from a number of existing standards such as IEC 61850.

International Electrotechnical Commission 61850: Communication Networks and Systems for Power Utility Automation

IEC 61850 defines communications protocols to provide secure communications between substation components for automation. Note that many small- and medium- PV installations are connected at or near the substation whose operations are automated using standardized substation hardware and networking protocol. However, the protocols defined therein are not widely adopted by industry yet, although equipment manufacturers have begun adopting and deploying 61850-compliant hardware across a broad range of devices. Thus, IEC 61850 is of medium relevance currently but will continue to increase in relevance over time.

LOW RELEVANCE Codes, Standards, Frameworks

Federal-Level Codes, Standards, and Frameworks (Low-Relevance)

Name	Description
NIST 800	A series of documents which address Federal Government specific assets. Comprised of publications which guide, recommend, report on, and provide technical specifications on NIST's cybersecurity activity
NIST SP 800-82 Revision 2	Guide to Industrial Control Systems (ICS) Security
NIST Report 7628	Guidelines for Smart Grid Cybersecurity
MITRE ATT&CK Framework	A matrix which outlines the techniques adversaries used to accomplish a given objective.
NERC Reliability Guideline	Cyber Intrusion Guide for System Operators
IEC 61968	Defines standards for information exchange between distribution systems. Note: Most sections are under development.
DOE/DHS ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
DOE/NIST/NERC RMP	Electricity Subsector Cybersecurity Risk Management Process Guideline
DHS NCCIC and ICS-CERT	Defense strategy recommendations (i.e., layering multiple security features for deterrence
Potential new UL/ISA Standard	Cybersecurity Certification Standard for DERs

Table 4. Low-Relevance Federal-Level Codes, Standards, and Frameworks