# CATSS Literature Review: Resources for Solar Cybersecurity[1]

| INTRODUCTORY GENERAL CYBERSECURITY RESOURCES | | |
|---|---|---|
| **TITLE** | **SUMMARY** | **KEY PROJECT LESSON** |
| Enhancing Energy Sector Cybersecurity: Pathways for State and Territory Energy Offices<br><br>**NASEO (2020)** | This guide provides background on ongoing cybersecurity efforts in both the public and private sectors and identify state-relevant communication channels and mechanisms for sharing information. Additionally, the guide identifies roles State and Territory Energy Offices might play in enhancing cybersecurity and response actions. | Foundational document on the role of State and Territory Energy Offices in cybersecurity broadly and engagement with federal agencies. |
| Cybersecurity Manual<br><br>**NARUC** | NARUC's cybersecurity manual is a comprehensive suite of cybersecurity tools to help public utility commissions (PUCs) gather and evaluate information from utilities about their cybersecurity risk management and preparedness. | Provides PUCs and other state stakeholders with a foundational overview on key cybersecurity aspects for utilities. While not focused on DERs, the tools provide many relevant questions PUCs and state stakeholder could apply to DER cybersecurity as well. |

| INTRODUCTORY INTERCONNECTION RESOURCES FOR DISTRIBUTED ENERGY RESOURCES (DER) | | |
|---|---|---|
| **TITLE** | **SUMMARY** | **KEY PROJECT LESSON** |
| A Guidebook for Distributed Energy Resource (DER) Interconnection<br><br>**NREL (April 2019)** | This report is a central document summarizing considerations, practices, and emerging solutions across a broad set of topics related to DER interconnection. The report is targeted at a high- | Includes a general outline of IEEE Standard 1547 and also outlines the NIST standards on cybersecurity as well as other utility best practices and emerging work on DER cybersecurity. |

| | | |
|---|---|---|
| | level, strategic-planning audience at utilities who are seeking an overview of DER interconnection issues and approaches and looking to understand how these may relate to their own situations. | |

| INTRODUCTORY CYBERSECURITY RESOURCES FOR DISTRIBUTED ENERGY RESOURCES (DER) | | |
|---|---|---|
| **TITLE** | **SUMMARY** | **KEY PROJECT LESSON** |
| Cybersecurity for Distributed Energy Resources and Smart Inverters<br><br>**Argonne National Laboratory (2016)** | The paper proposes a holistic attack-resilient framework to protect integrated DER and critical power grid infrastructure from malicious cyber-attacks. Specifically, the paper outlines the architecture of the cyber-physical power system with a high penetration of DER and analyze the unique cybersecurity challenges introduced by DER integration. | Outlines threat scenarios involving increased DER penetration on the electricity system. |
| Guide to the Distributed Energy Resources Cybersecurity Framework<br><br>**NREL (December 2019)** | The Distributed Energy Resources Cybersecurity Framework (DERCF) outlined in the report presents users with questions regarding their organization's security controls, practices pertaining to the use of such controls, and application to distributed energy resources (DERs) in the following categories: 1) Cyber governance 2) Cyber-physical technical management and 3) Physical security of DER devices. | This document is intended to provide an overview of cybersecurity risk as it relates directly to DERs in addition to serving as a detail-oriented reference regarding cybersecurity controls for DERs. |
| Cyber Security Primer for DER Vendors, Aggregators, and Grip Operators<br><br>**Sandia (December 2017)** | This report provides an introduction to cyber security for distributed energy resources (DER)—such as photovoltaic (PV) inverters and energy storage systems (ESS). The report outlines basic principles of cyber security, encryption, communication protocols, DER cyber security recommendations and requirements, and device-, | While the report aims at DER vendors, aggregators and grid operators, this primer of cyber security for DER provides an overview of potential cyber security attacks for DER, the basic tenets of cyber security, current U.S. requirements for DER communications and a review of cyber security recommendations, guidelines and reports that |

| | | |
|---|---|---|
| | aggregator-, and utility-level security best practices to ensure data confidentiality, integrity, and availability. | would be also very helpful for state energy offices and public utility commissions. |
| Summary of Sandia DER Cybersecurity Research<br><br>**Sandia (September 2020)** | The report provided a high-level synopsis of Sandia National Labs' DER cybersecurity work. SNL has authored numerous technical reports, stood up a DER cybersecurity working group with more than 500 experts, and performed various simulated and real cybersecurity tests on DER equipment. | Provides overview of SNL's DER cybersecurity activity with links for opportunities to access further technical reports. |

| STATE EXAMPLES | | |
|---|---|---|
| **TITLE** | **SUMMARY** | **KEY PROJECT LESSON** |
| California Rule 21 Smart Inverter Working Group<br><br>**California Public Utilities Commission** | The Smart Inverter Working Group (SIWG) grew out of a collaboration between the CPUC and California Energy Commission (CEC) in early 2013 that identified the development of advanced inverter functionality as an important strategy to mitigate the impact of high penetrations of distributed energy resources (DERs). The SIWG is currently drafting a *Utility Cybersecurity Requirements Guide for Communication to DER Facilities* to reflect a risk-based approach to ensure an enhanced cybersecurity posture is maintained to the utility for any interconnection requirement to a DER. | California is one of the leading states in developing guidelines on cybersecurity for DERs. The Smart Inverter Working Group could be considered a potential model for other states in engaging stakeholders and advancing the DER cybersecurity discussions |

| | | |
|---|---|---|
| Electricity Grid Cybersecurity – DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems.<br><br>**GAO (March 2021)** | Provides a high-level assessment of U.S. Department of Energy distribution cybersecurity system priorities. The paper also includes select state commission actions taken to address distribution grid cybersecurity generally. These actions included incorporating cybersecurity into routine oversight processes and hiring dedicated cybersecurity personnel. Federal agencies have supported these actions by, for example, providing cybersecurity training and guidance. | In addition to background on the national cybersecurity framework and relevant policies, the report includes examples of activities commissions have performed regarding distribution system cybersecurity that could be relevant to other states and DER cybersecurity more specifically. |

| ROADMAPS | | |
|---|---|---|
| **TITLE** | **SUMMARY** | **KEY PROJECT LESSON** |
| Roadmap for Photovoltaic Cyber Security<br><br>**Sandia (December 2017)** | This document is a five-year roadmap intended to chart a path for improving cyber security for communication-enabled PV systems with clear roles and responsibilities for government, standards development organizations, PV vendors, and grid operators. | Provides not only an introductory overview of solar cybersecurity, but also outlines potential state policy and regulatory approaches to address the issue. |
| Roadmap for Wind Cybersecurity<br><br>**U.S. Department of Energy (July 2020)** | The Wind Energy Cybersecurity Roadmap is a summary of critical infrastructure cybersecurity best practices and, looking to the future, a list of possible next steps to serve as a model for the wind industry and the strengthening of its cyber resiliency. It also includes a framework, or time-phased roadmap, for addressing such wind cybersecurity challenges, building strategies, and meeting milestones for improving wind energy cybersecurity in the near-, mid-, and long-term. | The components of this roadmap are specific to wind energy, but many may be applicable, as well, to other DERs and their control systems. |

| TECHNICAL RESOURCES – VULNERABILITY AND THREAT ASSESSMENT | | |
|---|---|---|
| **TITLE** | **SUMMARY** | **KEY PROJECT LESSON** |
| Power System Effects and Mitigation Recommendations for DER Cyber Attacks<br><br>**SNL (January 2019)** | National and jurisdictional interconnection standards require DER to include a range of autonomous and commanded grid-support functions which can drastically influence power quality, voltage, and bulk system frequency. This paper investigates the impact to the cyber-physical power system in scenarios where communications and operations of DER are controlled by an adversary. The findings show that each grid-support function exposes the power system to distinct types and magnitudes of risk. | This is a very technical paper but could be helpful for a deeper dive into understanding physical impacts from cyber-attacks. |
| Certification Procedures for Data and Communications Security of Distributed Energy Resources<br><br>**NREL (July 2019)** | The document provides cases that can be used to test the cybersecurity posture of the data and communications of DERs. As the electric power system infrastructure has evolved, the industry has increasingly relied on the availability of modern DER information systems to operate power system controls. This document provides a draft certification procedure for DER cybersecurity, and it is intended to be used as input to national and international certification test standards for DER equipment. | The report outlines a variety of potential vulnerabilities and test cases, which could possibly be used for exercise scenario development. |
| Cyber Security Assessment of Distributed Energy Resources<br><br>**Sandia (June 2017)** | To advise the solar industry, grid operators, and government of the current risks and provide evidence-based recommendations to the community, Sandia performed cyber security assessments of a communications enabled PV inverter and remote grid monitoring gateway. The team found several well-designed security features but also some weaknesses. Based on these findings, recommendations are provided to improve the security features of DER devices. | Technical report on potential vulnerabilities and cyber threats. |

| TECHNICAL RESOURCES – POTENTIAL SOLUTIONS AND FRAMEWORKS | | |
|---|---|---|
| **TITLE** | **SUMMARY** | **KEY PROJECT LESSON** |
| **ModuleOT: A Hardware Security Module for Operational Technology**<br><br>**NREL (February 2020)** | In order to reduce vulnerabilities in power distribution systems, this paper presents a novel open-source hardware security module that improves both information and operational security to better protect data and communications on the distribution grid. The security hardware is called "module for operational technology," or simply Module-OT, and it has been validated and tested in an emulated distribution system application. The purpose of Module-OT is to provide a single device that provides features of end-to-end encryption, authentication, and authorization to secure communications to a DER site. | ModuleOT may address some cybersecurity issues not addressed by current DER communications standards. |
| **A Multidimensional Holistic Framework for the Security of Distributed Energy and Control Systems**<br><br>**NREL (July 2019)** | The digitization of smart grid distributed generation and industrial control systems has prompted utilities to deploy tools with ubiquitous communications that potentially widen the attack surface. This paper proposes a multidimensional holistic framework that addresses this gap through advanced technologies, intelligent algorithms, and continued assessments. To show proof, the layered defense model, a solution dimension of the framework, is integrated into the National Renewable Energy Laboratory's Security and Resilience Testbed to replicate a utility's enterprise and substation networks. | Potential model framework and best practices for utility analysts to ensure a strong cybersecurity business process before integrating third-party products. |
| **EPRI Security Architecture for the Distributed Energy Resources Integration Network** | This paper provides a practical set of cybersecurity requirements pertaining to the network components supporting distributed energy resources (DER) communications. It aims to provide a holistic view of | This resource includes a compliance checklist which may be useable for CATSS members. |

| | | |
|---|---|---|
| **EPRI (October 2019)** | the interconnected systems, including DER, and it suggests how they can be protected from cyberattacks. | |
| **Recommendations for Trust and Encryption in DER Interoperability Standards**<br><br>**Sandia (February 2019)** | Recently developed Distributed Energy Resource (DER) interoperability standards include communication and cybersecurity requirements. In 2018, the US national interconnection standard, IEEE 1547, was revised to require DER to include a SunSpec Modbus, IEEE 2030.5 (Smart Energy Profile, SEP 2.0), or IEEE 1815 (DNP3) communication interface but does not include any normative overarching cybersecurity requirements. IEEE 2030.5 and associated implementation requirements for California, known as the California Smart Inverter Profile (CSIP), prescribe the greatest security features—including encryption, authentication, and key management requirements. In this paper, (a) the elements of IEEE 2030.5 encryption, authentication, and key management guidelines are analyzed, (b) potential scalability gaps are identified, and (c) alternative technologies are explored for possible inclusion in DER interoperability or cybersecurity standards. | The report focuses on the benefits and challenges derived from IEEE 2030.5 implementation. Based on this analysis, recommendations for improvements to trust and encryption in DER communication networks are provided. |

[1] The *CATSS Literature Review: Resources for Solar Cybersecurity* provides an overview of relevant reports and research on solar cybersecurity issues by category. The list is not exhaustive, and inclusion of resources does not indicate an endorsement of the National Association of State Energy Officials (NASEO), the National Association of Regulatory Utility Commissioners (NARUC), or any of the CATSS Advisory or Control Group members. This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office Award Number DE-EE0009004. This report was prepared as an account of work sponsored by an agency of the United States Government. 