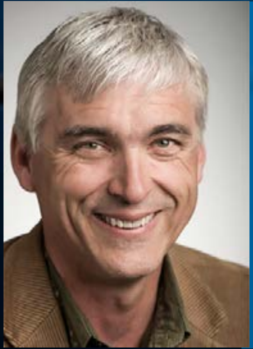
NREL
Transforming ENERGY

Cybersecurity Standards for Photovoltaic Operations

April 8, 2022



Andy Walker

Sr. Research Fellow

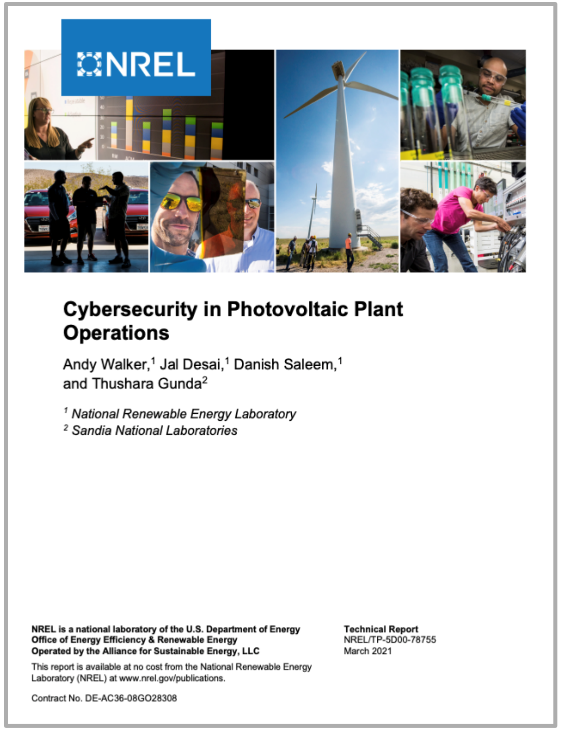
David Benton

Professional Partnership Development

Photo by Dennis Schroeder, NREL 55200

NREL/PR-5C00-82588

Cybersecurity in PV Plant Operations.



NREL

Cybersecurity in Photovoltaic Plant Operations

Andy Walker,[1] Jal Desai,[1] Danish Saleem,[1] and Thushara Gunda[2]

[1] *National Renewable Energy Laboratory*
[2] *Sandia National Laboratories*

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5D00-78755
March 2021

Cybersecurity in Photovoltaic Plant Operations
https://www.nrel.gov/docs/fy21osti/78755.pdf

PV System Control and Data Acquisition System including Radio Communications (Photo by Andy Walker, NREL)

Cybersecurity "Best Practices" for PV Plants

1. Isolate internal (controls) and external (reporting) communications.

2. Use multiple means of authentication to ensure identity of individuals and maintain integrity of the validation process.

3. Use role-based access control (RBAC) and authentication for all data interactions, and frequently revise access permissions.

4. Use Transport Layer Security (TLS) to ensure encryption, authentication, and data integrity.

5. Use a Certificate Revocation List (CRL) to revoke expired and bad certificates used to authenticate the Transmission Control Protocol (TCP) session.

6. Provide adequate physical security such as video surveillance, badge in access controls, fenced walls, door security and alarms.

7. Use antivirus software that is frequently updated, including ongoing patches.

8. Consider using application software with "rollback" capabilities if update introduces malware.

Cybersecurity “Best Practices” for PV Plants

9. Back up data frequently, run malware scan, encrypt the backup, and store in a separate server or secure cloud.

10. Periodically test your backup to make sure you can retrieve data.

11. Use effective password management to protect from brute force credential attacks and least-privilege violations.

12. Use monitoring tools such as intrusion detection and/or prevention (IDS/IPS) to ensure that due diligence to watch for cybersecurity incidents is being met regularly.

13. Consider using visualization of where security incidents are occurring and easier to interpret than textual reports.

14. Log alerts, login attempts, irregular activities, etc. for network forensics and audits.

15. Address supply chain management and insider threats to ensure that devices are secure.

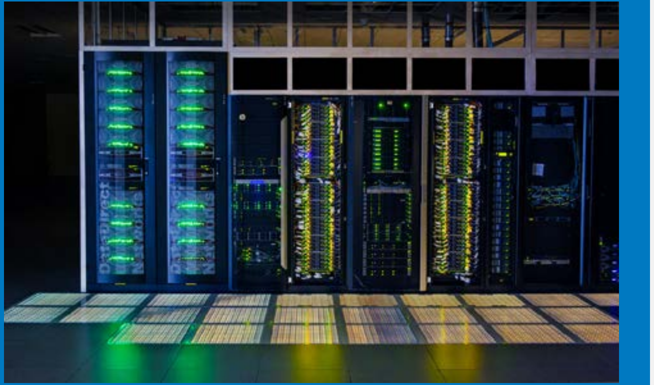
16. Document preventative and corrective actions taken to reduce and mitigate the risk of cyber vulnerabilities.

Cybersecurity Response Plan for Photovoltaic Plant Operations

Cyber Energy Emulation Platform (CEEP) at the National Renewable Energy Laboratory. (Photo by Werner Slocum / NREL 62543)

1. Establish definitions of cybersecurity incidents, such as inability to monitor or control versus loss of information.
2. Identify roles and responsibilities of each person involved in the response team; specify who the decision makers will be.
3. Have contact information ready to call in case of an incident, including information about what each contact oversees within the company and external contacts, such as the utility company and law enforcement personnel.
4. Plan which computers will need to be isolated from the network, or locked, and how data will be backed up.

Cybersecurity Response Plan for Photovoltaic Plant Operations

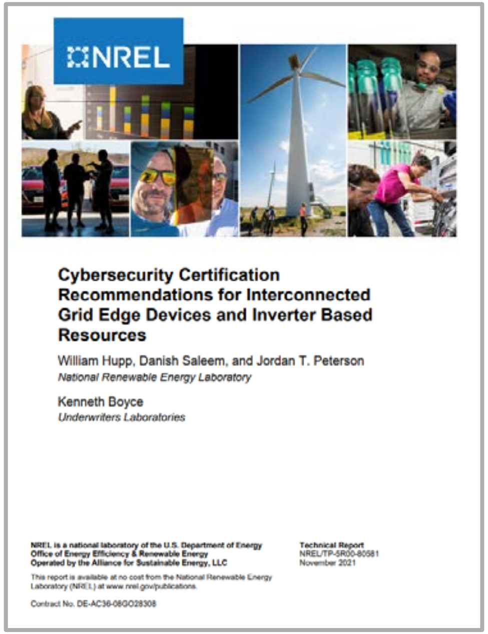


High Performance Computing Data Center at the National Renewable Energy Laboratory. (Photo by Dennis Schroeder / NREL24358)

5. Establish criteria for what needs to be reported to emergency response, senior management, cybersecurity experts, legal counsel, suppliers, or insurance providers. Some notifications might be legal requirements if confidential information was stolen or disclosed.
6. Develop instructions on when to notify appropriate authorities. Contact your local police to file a report if there is a possibility that any personal information, intellectual property, or other sensitive information was stolen.
7. Revise response plan frequently as circumstances change

Cybersecurity Test Cases Studied

- Two-Party Application Association (bidirectional communications observed only when connected)
- Transport Layer Security (protocol for authentication and encryption, associated latency)
- Transport Layer Security Recovery (recover from interruptions)
- Key Update (update encrypt/decrypt key and inform operator of update)
- Message Authentication Code (validate message not altered).
- Certificate Revocation List (revoked TLS certificates disallowed and operator informed)
- Expired Certificate (expired TLS certificates disallowed and operator informed)
- Operating System Security and Service Version (applications are running most recent secure versions or disabled)
- Authentication and Password Management (strong passwords, changes)
- Security Management (security management plan with threats and mitigations)



NREL

Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources

William Hupp, Danish Saleem, and Jordan T. Peterson
National Renewable Energy Laboratory

Kenneth Boyce
Underwriters Laboratories

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

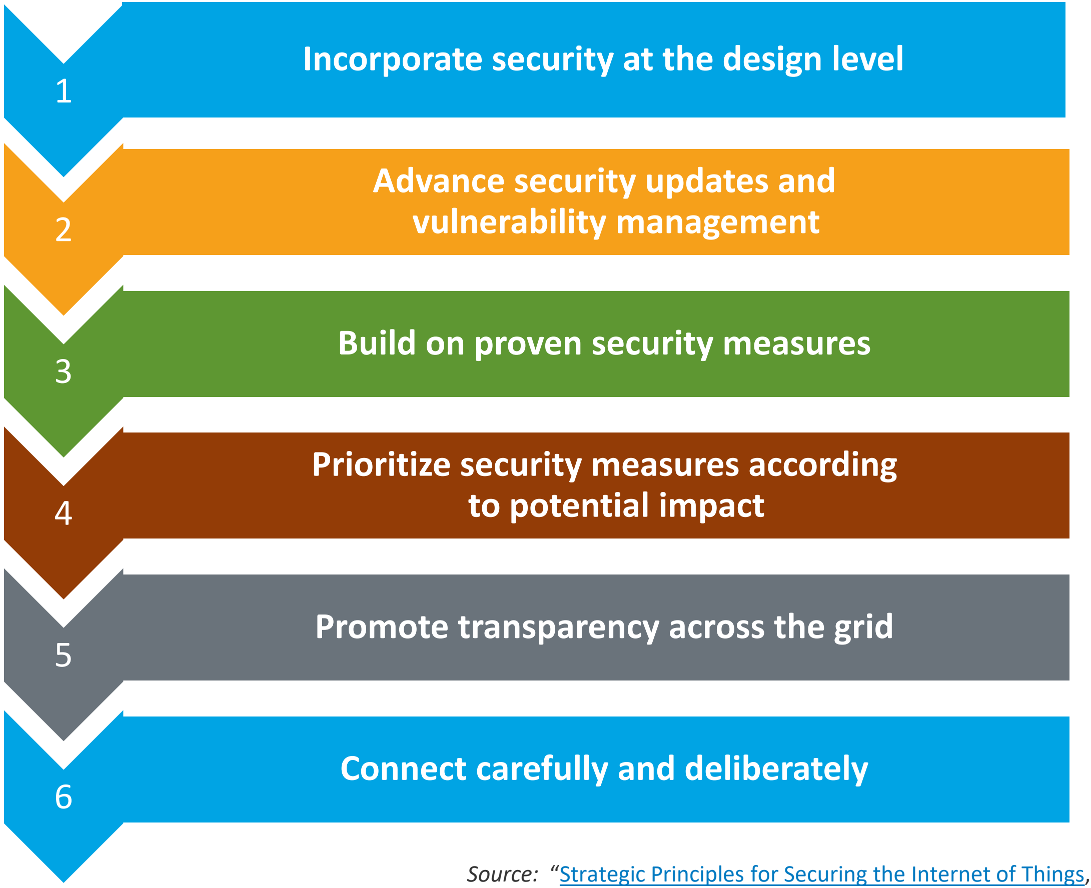
Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-80581
November 2021

Think Before You Connect

Implement **security by design** and practice basic **cyber hygiene.**

- Change default passwords.
- Use two-factor authentication.
- Install updates, i.e., authentication, TLS1.2 or higher, etc.
- Consider security of underlying infrastructure during patch management or remote connection.
- Monitor both consumer devices and vendor-managed devices.
- If possible, add code-signing and roll-back firmware.
- Use vendors with cyber hygiene.
- DO NOT connect printers or other similar devices to the operations network.



1 **Incorporate security at the design level**

2 **Advance security updates and vulnerability management**

3 **Build on proven security measures**

4 **Prioritize security measures according to potential impact**

5 **Promote transparency across the grid**

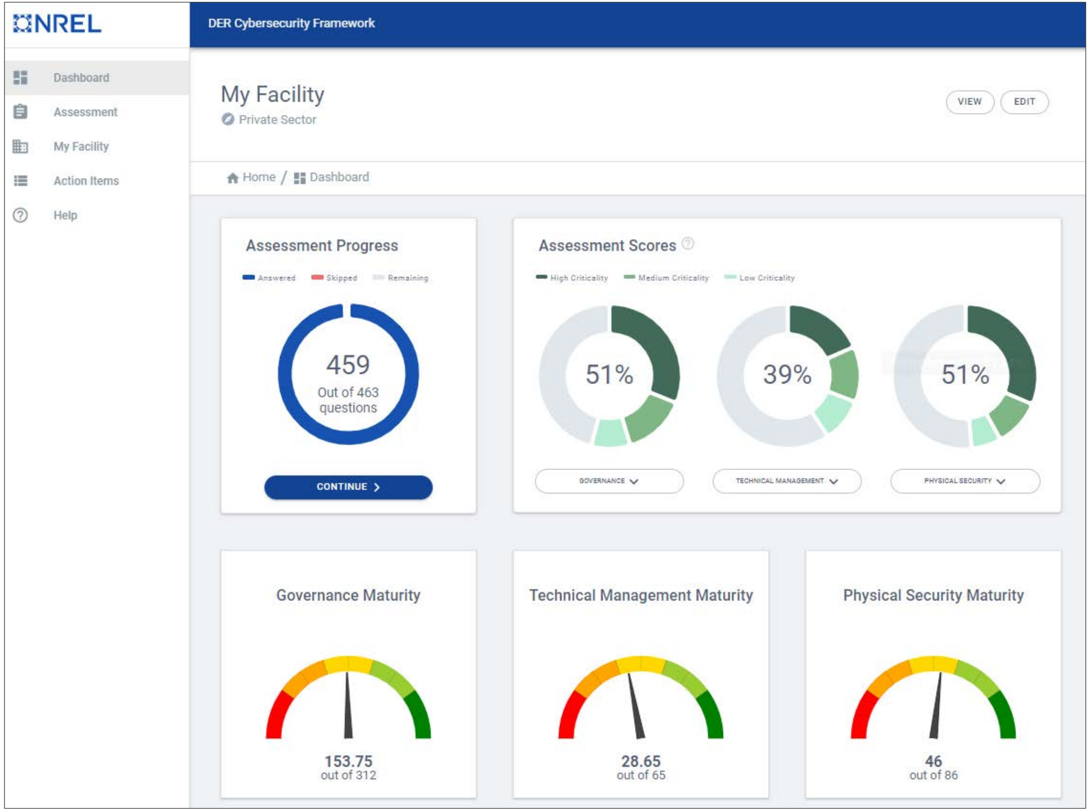
6 **Connect carefully and deliberately**

Source: "Strategic Principles for Securing the Internet of Things," U.S. Department of Homeland Security (2016)

Distributed Energy Resources Cybersecurity Framework (DER-CF)

The DER-CF provides a holistic assessment for evaluating the cybersecurity posture of DER systems. Available as a written guide or interactive web tool, the DER-CF expands upon existing cybersecurity frameworks for more modern energy systems.

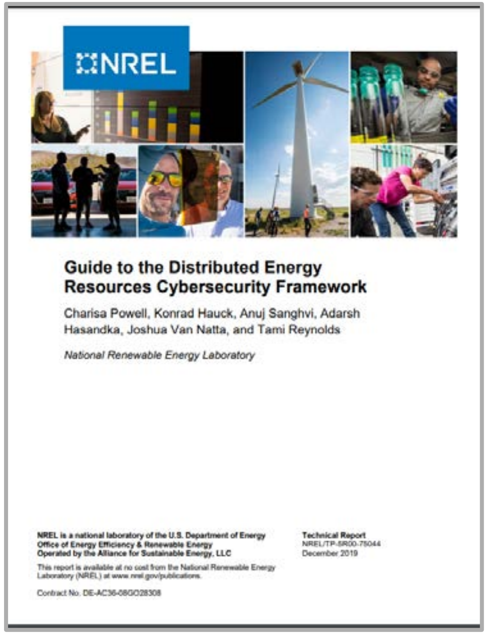
The DER-CF informs policies and controls for **cyber governance, cyber-physical technical management**, **and physical security of distributed energy technologies** at federal sites across the country.



Learn more about the tool: www.dercf.nrel.gov

Distributed Energy Resource Cybersecurity Framework (DERCF)

- Go to dercf.nrel.gov
- Register your distributed energy system
- Define roles for assessment participants
- Answer assessment questions
- Receive your assessment report



Guide to the Distributed Energy Resources Cybersecurity Framework

Charisa Powell, Konrad Hauck, Anuj Sanghvi, Adarsh Hasandka, Joshua Van Natta, and Tami Reynolds

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-75044
December 2019

Standards Related to Distributed Energy Resource Cybersecurity

- Executive Order 14028, “Improving the Nation’s Cybersecurity”
- DOE/DHS ES-C2M2: Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
- DOE/NIST/NERC Risk Management Process
- NIST Cybersecurity Framework
- NIST SP 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security
- NIST Interagency/Internal Report 7628: Guidelines for Smart Grid Cybersecurity
- NERC Reliability Guideline: Cyber Intrusion Guide for System Operators

- IEC 62351: Power Systems Management and Associated Information Exchange
- IEC 62443: Security for Industrial Automation and Control Systems
- IEEE C37.240-2014: IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems
- IEEE 1686: Standard for Intelligent Electronic Devices Cyber Security Capabilities
- IEEE 1547.3: IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems *(currently under development)*

Cybersecurity in Photovoltaic Plant Operations

- Large photovoltaic (PV) power plants or large fleets of plants that provide power to the bulk electric system must comply with North American Electric Reliability Corporation (NERC) standards enforced by the Federal Energy Regulatory Commission:
  - Operator training and certification of personnel in cybersecurity and critical infrastructure protection
  - Emergency preparedness plans
  - Services during and after disturbances
  - Communications between plant and utility.
  - Critical Infrastructure Protection (CIP) Standards

Control Room at the Energy Systems Integration Facility at the National Renewable Energy Laboratory (NREL). (Photo by Werner Slocum / NREL 62555)

Thank You

www.nrel.gov

Photo from iStock-627281636

NREL
Transforming ENERGY