Distributed Energy Resource Cybersecurity Framework Best Practices

Charisa Powell, Konrad Hauck, Anuj Sanghvi, 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-5R00-75921
January 2020

Distributed Energy Resource Cybersecurity Framework Best Practices

Charisa Powell, Konrad Hauck, Anuj Sanghvi, and Tami Reynolds

National Renewable Energy Laboratory

Suggested Citation
Powell, Charisa, Konrad Hauck, Anuj Sanghvi, and Tami Reynolds. 2020. *Distributed Energy Resource Cybersecurity Framework Best Practices*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-75921. https://www.nrel.gov/docs/fy20osti/75921.pdf.

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-5R00-75921
January 2020

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Federal Energy Management Program. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

Acknowledgments

The research team for the Distributed Energy Resources Cybersecurity Framework is extremely grateful to the sites and organizations that provided their time, resources, and feedback for our site visits.

List of Acronyms

DER	distributed energy resources
DERCF	Distributed Energy Resource Cybersecurity Framework
ES-C2M2	Electric Sector Cybersecurity Capability Maturity Model
IT	information technology
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
OT	operational technology
RBAC	role-based access control

Table of Contents

1 Introduction

Current cybersecurity challenges for distributed energy resources (DERs) stem from the integration of various systems and the cyber-physical security concerns they bring. Although frameworks exist for industrial control systems and other energy systems, a simple guided tool that can prioritize recommended actions for controls specific to DERs is lacking. Additionally, the novelty of the field has made it difficult to create a standardized procedure for DERs with cybersecurity in mind. In response to this critical need to address cybersecurity risk management, the National Renewable Energy Laboratory (NREL) has developed a framework and accompanying web application known as the Distributed Energy Resources Cybersecurity Framework (DERCF)[1] (Powell, 2019). A brief overview of the DERCF can be found in Section 1.2.

This document provides a guide to cybersecurity best practices identified by technical research and site visits where the framework was used to assess the cybersecurity posture of DER systems.

1.1 Background

In 2019, NREL developed the Distributed Energy Resources Cybersecurity Framework (DERCF) and web application. The web-based tool assists the facility's management team by bringing guidance and structure to the extensive array of cybersecurity controls applicable to DERs and walking the user through a three-pillar assessment framework. Upon completion of an assessment, users are provided with a set of results that identify and assess the forte of their cyber and physical assets.

1.2 Framework Details

The DERCF is based on the U.S. Department of Energy's Electric Sector Cybersecurity Capability Maturity Model (ES-C2M2) (U.S. Department of Energy 2014) and the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework (2018) with an extension that targets technical and physical aspects of DER system security. To organize the controls associated with these new areas of focus, the DERCF is organized into three main pillars:

- Cybersecurity governance
- Technical management
- Physical security.

Each of these pillars contains multiple layers that address key cybersecurity topics and together create a robust and flexible framework specifically designed for DERs. Table 1 presents the domains and subdomains of the three pillars that comprise the DERCF. As previously mentioned, the DERCF's flexible design allows for new domains and subdomains to be created, modified, and removed as necessary.

[1] The DERCF document and accompanying web application are available at no cost from www.dercf.nrel.gov.

Table 1. DERCF's Three Domains and Their Respective Subdomains Address a Comprehensive Set of Controls for Securing DER Technologies

Cyber Governance Security Assessment	Cyber-Physical Technical Management Security Assessment	Physical Security Assessment
Domains:	Domains:	Domains:
• Risk Management • Asset, Change, and Configuration • Identity and Access Management • Threat and Vulnerability Management • Situational Awareness • Information Sharing and Communication Management • Incident Response • External Dependency Management • Cybersecurity Program Management	• Account Management - Role-Based Access Control - Anomalous behavior in system logs • Configuration Management - Access Restrictions - Configuration Settings - Configuration Change Control - Internal/External User Management • Systems/Device Management - Fail-Safe Procedures - Ports and Input/output Device Access - Cryptographic Protection - Software Integrity/Patch Management	• Administration Controls - Audits - Holistic Security/Contingency Planning - Personnel Security Planning • Asset Controls - Equipment - Maintenance • Structure Controls - Distancing Practices for Sensitive Assets - Intrusion Detection/Prevention Assets - Response Teams/Force Protection

2 Research

Considerable time was put into understanding the challenges faced by DER site personnel. The framework and DERCF web tool are designed to be living, dynamic resources that adapt to new obstacles in the field as those challenges arise. In conjunction with preliminary technical research to identify and fully understand the function and interaction of DER systems components, the team conducted a series of site visits to learn more about operations and the application of DERs.

To better appreciate the operational challenges faced by on-site personnel, field visits (called discovery assessments) provided a hands-on experience and allowed researchers to talk face to face with DER owners. These results helped shape the content provided as "best practices," detailed in Section 3.

Furthermore, the team conducted a separate set of federal site visits to identify strengths and weaknesses in the web tool, which allowed the team to make adjustments before release. These site visits are characterized as "validation" assessments.

2.1 Discovery Assessments

Discovery assessments revealed a prevalence of third-party involvement with DER systems. Third parties can include vendors, manufacturers, cloud providers, and contractors. Often, sites do not have full access or management over all systems components, despite being the owner. It is common for DER systems to be installed and maintained by a contractor, leaving the system owners with limited to no access. This creates a layer of abstraction between the relevant systems and federal site personnel, resulting in limited system knowledge and understanding.

2.2 Validation Assessments

Validation assessments were designed to identify the completeness of content, ability to satisfy user needs, as well as regulatory and agency requirements. This also includes the appearance and aesthetic of the web tool and the way the tool asks questions and provides feedback. The DERCF's web tool is significantly advanced compared to existing tools, in that it avoids the standard "yes or no" answer type for every question; responses to cybersecurity assessment questions are rarely as simple as a binary answer. This allows the user to a receive a score that reflects their cybersecurity risk posture more accurately.

The tone of the web tool has been adjusted such that it does not mimic the legalistic language often found in compliance and standards documents, but instead provides an immersive and human-friendly experience.

A key component to a successful cybersecurity assessment is ensuring that the appropriate individuals are present and available to respond to questions in their subject area topics. The following roles have been identified and defined in the web tool to assist with identifying a site team:

- **Energy systems manager:** management-level individual
  responsible for overseeing a team of technical personnel in the field of energy systems informational technology (IT) and operational technology (OT) system administrators

- **Force protection personnel:** Individual(s) responsible for on-site physical security needs, including physical enforcement of rules, incident response, and patrolling operations

- **Access control personnel:** Individual(s) responsible for badges, visitor controls, site visits from external personnel, locks, and keys

- **DER/OT/IT systems administrator:** A network/system administrator for the DER system (and beyond), responsible for managing accounts and system configuration

- **Emergency planning and management personnel:** Individual(s) responsible for planning, administrating, and disseminating important information around site-wide security matters

- **Physical security training personnel:** Individual(s) who work closely with emergency planning and management personnel to ensure policies, procedures, and drills are performed and all personnel on-site are aware of how to respond to site incidents

- **Compliance officer:** Individual(s) responsible for enforcing up-to-date standards relevant to DERs

- **Human resources personnel:** Sitewide team specifically assigned to administrative tasks related to employees

- **Systems/controls engineer:** Technical individual primarily working directly with control systems for research and/or operational purposes

- **Contracting personnel:** Individual(s) familiar with existing third-party agreements associated with the installation and operation of DERs.

Note that these roles do not constitute an exhaustive list of personnel a site might have. Additionally, some roles and responsibilities may be combined into a single position.

3 Best Practices

This section highlights noteworthy findings in select domains from each DERCF pillar. Sites should follow their agency policies and guidance to prioritize strengthening site-specific findings. Research and discovery assessments have consistently indicated a lack of strong cybersecurity practices in certain areas.

3.1 Cybersecurity Governance Pillar

Cybersecurity governance is the practice of identifying cybersecurity principles in an organization and creating polices that ensure all principles are followed. Although decisions and documentation of procedures are primarily the responsibility of energy systems managers and system administrators, effective implementation of strong cybersecurity policies requires participation from all team members, including day-to-day users.

Risk Management

Discovery assessments revealed an informal, undocumented understanding of potential and present risks to DER systems. In addition to clear communication between federal managers, contracting personnel, and system engineers, maintaining healthy documentation practices is essential during normal operation, and especially important during transitions in employment.

According to the ES-C2M2, risk management in the context of cybersecurity is defined as "*risk to organizational operations (including mission, functions, image, and reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information for both IT and OT systems.*" While risk cannot be entirely eliminated, it can be mitigated, managed, and accepted with proper documentation and informed decisions. The ES-C2M2, in conjunction with other cybersecurity risk management frameworks, should be used as a reference to develop an overall site risk management plan and ensure that the risks associated with DER are included and addressed appropriately. The inclusion of DER into the sitewide cybersecurity plan encourages communication and documentation.

Asset Management and Network Topography

For small and large organizations, maintaining an effective and consistent asset management policy facilitates visibility into the environment and helps ensure that devices can be accounted for. Sites should have a regularly updated inventory of devices that includes both IT and OT components. This inventory will serve as a useful reference during normal operation as well as during a potential cybersecurity incident.

Interconnectivity between IT and OT environments can prove to be challenging in terms of managing, documenting, updating, and maintaining systems. The Purdue Enterprise Reference Architecture (Williams 1994) provides a foundational layered approach using demilitarized zones to separate an organization's enterprise and operational networks, and can be used as a reference to categorize assets into layers. This reduces the likelihood of a potential cybersecurity attack on the enterprise network affecting the availability of DER systems, and vice versa.

Managing Supply Chain Risks

Supply chain and external software dependencies are critical to the cybersecurity of DERs. Validation assessments showed that the management of these external dependencies on vendors and manufacturers often are not understood, documented, or controlled. This vulnerability needs to be addressed immediately. Consequences of ineffective supply chain management can introduce privacy concerns and potential software vulnerabilities via backdoors.

Moving forward, the DERCF will continue to incorporate key concepts associated with risk management frameworks. Specifically, the NIST (2013) supply chain risk management process provides approaches that include organization-wide security controls that identify risks associated with a lack of visibility and/or control. It is important to know that these vulnerabilities can be both adversarial and accidental in nature. From an external, adversarial perspective, risk can occur from tampering or altering devices in the manufacturing process before it is installed. From an internal, accidental perspective, this risk can arise from simply having devices with poor quality or existing internal procedural flaws. Numerous publications by NIST on the topic of supply chain risk management can be found at https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications.

3.2 Cyber-Physical Technical Management Pillar

Cybersecurity best practices in the technical management pillar relate to system- and device-level configurations and likely involve system engineers, administrators, and any other personnel who have direct access to DER systems.

Access Control

Restricting who has access to a system serves as a first line of defense. It is important to note that access control includes both remote and local interactions.

Access control encompasses many principles, including but not limited to:

- Least privilege
- Role-based access control (RBAC)
- Two-factor authentication.

The principle of least privilege ensures that users only have the privileges necessary to accomplish their tasks, minimizing the opportunity for unauthorized access to files and software. This concept can be applied site-wide and in conjunction with other access control policies.

RBACs are particularly useful in environments where users may have different duties on the same system. For instance, providing the DER system administrator and a third-party contractor with the same access poses a major cybersecurity risk. RBACs restrict privileges based on the duties for each user account.

Lastly, two-factor authentication requires a second credential to be provided for authentication. For example, this can include electronic identification (e.g., smart card/certificate, rotating numeric PIN provided by RSA SecurID) or even biometric identification (e.g., fingerprints or

irises). These additional credentials can prevent password attacks and unauthorized access. Although these technologies exist, more research is needed on the best way to integrate them with OT systems.

Implementing these three principles, in addition to other healthy cybersecurity practices, can greatly increase security.

Third-Party Interactions

Although interactions with third parties are often unavoidable, measures can be taken to help ensure cybersecurity is a priority. Cloud platforms and web-based software solutions are often used to manage resources and view data. Documentation of the current software and any subsequent software updates should be readily available to the federal manager.

Software managed by a third party can provide useful log data that should be included in the documentation process. Examples include auditing log data to track users who have logged in, notating changes to system configuration, and more. Organizations should identify needed information and documentation in third-party agreements and are highly encouraged to maintain a healthy relationship with third parties that provide software solutions.

The DERCF's dynamic scoring capabilities present a unique set of questions to avoid penalizing sites for utilizing services provided by a third party. Furthermore, the tool automatically provides actionable intelligence that suggests contractual language with cybersecurity in mind.

Logging and Alerts

Lack of visibility is a critical issue that can be remediated by enabling logging at an appropriate level. Too much logging can cause an inundation of data, preventing federal managers and technical team members from finding the necessary information. However, logs also play a critical role in response and recovery when an incident or emergency occurs, providing valuable context.

Enhancing technical management cybersecurity posture includes using logs to create alerts based on behaviors. These alerts can be specific to the status of device components as well as provide notification of data values exceeding a certain threshold. The user can go a step further to create severity-based alerts that only notify certain individuals upon being triggered.

3.3 Physical Security Pillar

As critical as it is to have cybersecurity controls for federal facilities, these sophisticated and often expensive technical controls can be undermined simply by a lack of strong physical security controls. Physical controls should serve as a first line-of-defense deterrent, forcing adversaries to use more elaborate and technical attacks. For an organization to have this foundational layer of physical security, the following areas should be prioritized.

Holistic Security and Contingency Planning

A robust physical security plan will provide structure and organization in the event of an incident or emergency. Defense in-depth is a principle that employs a layered-security approach that incorporates various countermeasures to improve the security posture of an organization, should

the first line of defense fail. If an organization prioritizes the time and resources to develop a solid physical security plan tailored to their site, they can help ensure to cover all of the site's physical security aspects (e.g., management, minimal structural deterrents, policies and procedures), practice defense in-depth, and have a higher level of coordinated efforts in securing organizational assets. This physical security plan should include the following:

- Clearly defined roles and responsibilities
- Physical security controls that cover the entirety of the site
- Redundant checks and balances for the security controls implemented and periodic maintenance.

Embedded in this plan should be the opportunity for flexibility in all aspects of physical security, as it is impossible to predict how an event will transpire; this is otherwise known as contingency planning. Certainly, there is no "one size fits all" plan that works for all organizations. Actions to begin thinking about include:

1. Identify critical assets and prioritize the physical security plan around those items.
2. Enforce security procedures consistently.
3. Create a policy that updates the plan frequently.

Intrusion Detection and Prevention

The second part of the foundational layer of the physical security pillar are controls that bolster intrusion detection and intrusion prevention capabilities. Beyond baseline physical security planning, the first priority is to put in place security controls to keep out unauthorized or unwanted personnel. This layer has layers of its own, creating a hardened defense-in-depth security posture, which includes:

- The perimeter of the property (e.g., fencing, barricades, guarded gates)
- Buildings and access points to critical assets within the facility property
- Any further access point past the buildings or access points that would lead to command and control points tied to critical assets.

These security controls for mitigating and preventing physical access to sensitive areas would greatly benefit any organization, especially if controls provided visibility and redundant validity. For example, if an organization had two or more sources that could corroborate an intrusion to any area with restricted access and be able to visibly verify a disturbance remotely, response capabilities to threats would be greatly improved. These security controls would come in the form of:

- **Sensory monitoring**: implementing motion detectors, infrared perimeter sensors, motion-activated flood lighting, and so on

- **Visual monitoring**: aggregated at a central monitoring station, utilizing security cameras such as closed-circuit television cameras and motion-activated and tracking cameras, equipped with infrared capabilities for nighttime security

- **Personnel monitoring**: with patrolling guards as well as guards stationed at strategic checkpoints throughout the site.

The ability to service these controls remotely and in an automated fashion could reduce expenses and required security personnel.

Site-Supportive Equipment

These assets bolster the resilience and defense in-depth for physical security assets in places that are needed to secure the critical assets should they fail. Site-supportive equipment can range from higher quality cabling to on-site generators that provide backup generation to allow assets to have continuous operation, should a disturbance occur.

Summary

This document provides a variety of suggestions on which to focus, but it does not represent a comprehensive list of controls to create a completely robust security posture. From a cybersecurity governance standpoint, risk management, asset management, and supply chain regulation were found to be critical areas because all three have a direct impact on cybersecurity policy decisions and documentation. Risk management requires making informed decisions based on the priority of assets with a strong emphasis on documentation. Asset management not only includes maintaining an inventory of systems but also an accurate representation of how devices and systems are connected via the internal network. To mitigate potential privacy concerns, supply chain interactions should be a high priority as well. Framework guidelines and documentation from NIST and other resources provide helpful language to understand supply chain risk, though it is important to assess the risks unique to each organization.

Furthermore, access control is a pertinent step in the technical management of DER systems. Implementing a combination of RBAC and strong authentication methods that enforce the usage of multiple credentials reduces the opportunity for unauthorized access to a privileged account. In addition, logging and prioritizing alerts can provide visibility into a system both during an incident and during normal operation. While DER systems may rely on third-party tools and software, it is important to maintain visibility and documentation for these interactions and require contractual language with cybersecurity in mind, making this a process closely aligned with the cybersecurity governance pillar.

Finally, physical security is a tangible, and spatially representative, pillar in developing a robust security posture. Lapses in physical security can undermine the hard work and effort put into cybersecurity governance and technical management controls. Having a robust, systematic, defense-in-depth plan for physical security controls can assist in providing a strong foundation for an organization's security posture. Holistic security and contingency planning for physical security can help protect areas that would otherwise be vulnerable to easily bypassed checkpoints. In addition, intrusion detection and prevention controls give security operators the visibility and validation of any remote security assets deployed on site to have better response capability. While site-supportive equipment is a smaller component of the overall security architecture of a site, these assets ensure the reliability of the complex devices responsible for safeguarding valuable assets.

In conjunction with the DERCF web application, these elements can serve as a starting point for achieving a more secure system.

References

National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1. Gaithersburg, MD, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

National Institute of Standards and Technology (NIST). *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST SP 800-53 Revision 4. Gaithersburg, MD, 2013. https://doi.org/10.6028/NIST.SP.800-53r4.

Powell, Charisa, Konrad Hauck, Anuj Sanghvi, Adarsh Hasandka, Joshua Van Natta, and Tami Reynolds. 2019. "Guide to the Distributed Energy Resources Cybersecurity Framework." Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-75044.

U.S. Department of Energy. *Electric Sector Cybersecurity Capability Maturity Model (ES-C2M2)*. Version 1.1. Washington, D.C., 2014. https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

Williams, Theodore J. 1994. "The Purdue Enterprise Reference Architecture." *Computers in Industry* 24, no. 2-3: 141-158. https://www.sciencedirect.com/science/article/abs/pii/0166361594900175.