Distributed Energy Resources Cybersecurity Framework: Applying the NIST Risk Management Process

Charisa Powell, Konrad Hauck, Tami Reynolds,
Anuj Sanghvi, MD Touhiduzzaman, and Joshua Van Natta

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-5R00-77431
October 2020

Distributed Energy Resources Cybersecurity Framework: Applying the NIST Risk Management Process

Charisa Powell, Konrad Hauck, Tami Reynolds,
Anuj Sanghvi, MD Touhiduzzaman, and Joshua Van Natta

National Renewable Energy Laboratory

Suggested Citation
Powell, Charisa, Konrad Hauck, Tami Reynolds, Anuj Sanghvi, MD Touhiduzzaman, and Joshua Van Natta. *Distributed Energy Resources Cybersecurity Framework: Applying the NIST Risk Management Process*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-77431. https://www.nrel.gov/docs/fy21osti/77431.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-5R00-77431
October 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 Office. 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

This material is based on work supported by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy (EERE) Federal Energy Management Program. The authors thank EERE Energy Technology Program Specialist Saralyn Bunch for her support and oversight throughout the project. The NREL research team is also extremely grateful for the time put in by the Missoula Field Office at the United States Department of Agriculture and the sharing of their experiences within the Risk Management Framework process.

List of Acronyms

DERs	distributed energy resources
DERCF	Distributed Energy Resources Cybersecurity Framework
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
RMF	Risk Management Framework
SC	security categorization

Executive Summary

In an effort to strengthen the cybersecurity posture of federal agencies and reduce the time and complexities of following the Risk Management Framework (RMF) six-step process, the National Renewable Energy Laboratory has dedicated research into expanding the existing Distributed Energy Resources Cybersecurity Framework to provide functionality that aids in completing the RMF steps. Users will have the opportunity to learn, interact with, and review the framework, saving time and resources. Existing functionality within the Web application will continue to be available with added features to improve usability.

Table of Contents

List of Figures

1 Introduction

The National Renewable Energy Laboratory (NREL) is actively researching new methods to address the gap in our nation's cybersecurity assessment tools. The growth of distributed energy resources (DERs) presents new attack avenues and a greater surface area for potential vulnerabilities. The Distributed Energy Resource Cybersecurity Framework (DERCF) is a holistic tool for evaluating the cybersecurity posture of federal sites with DER systems—filling an important gap that expands upon existing cybersecurity frameworks for our evolving energy networks. *The Guide to Distributed Energy Resources Cybersecurity Framework* (Powell et al. 2019) provides foundational context as well as an introduction to the inner workings of the Web application.

The goal of this research is to intertwine existing DERCF work with the Risk Management Framework (RMF) process to provide context and resources for federal facilities at each step of their cybersecurity evaluation. This document describes the implementation details of this added work and expansion of the DERCF Web application (NREL 2020).

1.1 Background

The DERCF Web application is now publicly available to create an account, assess cybersecurity posture, and take initiative on customized, actionable recommendations. The Federal Energy Management Program has funded NREL researchers to understand the specifics of the RMF, provide resources for federal facilities to meet agency requirements, and to save time and money.

In addition to pursuing research into existing National Institute of Standards and Technology (NIST) documentation, the team continues to gain hands-on experience through discovery assessments, working closely with federal sites to address cybersecurity challenges unique to DERs. This involves identifying individual DERs and conducting field visits and virtual meetings to understand components and interconnectivity of:

1. Photovoltaic systems
2. Wind turbine systems
3. Battery storage systems
4. Electric vehicle charging ports.

With the extended DERCF-RMF capabilities, users will have a guided experience with readily available resources. NREL's goal is to provide an approach to cybersecurity risk management and provide a collection of functionalities for users to continuously use the tool as they work to improve their operational technology cybersecurity posture and track their progress.

1.2 Preliminary Research

In addition to research into DER types and their communications, the NREL research team studied controls from NIST's Industrial Control Systems (ICS) overlay, a refined collection of controls from the baseline Special Publication (SP) 800-53 document (NISTg 2020). These controls, which provide a more refined approach to ICS security, have served as a foundation for the DERCF as controls are

continuously added and modified as appropriate. The NREL research team references additional NIST documents including, but not limited to, 800-37 (NISTf 2018), 800-160 (NISTc 2019), 800-16 (NISTa 2014), and 800-60 (NISTh,i 2008).

2 RMF Expansion Methodology

Currently, DERCF is divided into three pillars—Governance, Technical Management, and Physical Security—which make up a robust self-guided cybersecurity posture assessment. The collection of features for the RMF expansion are independent of the existing self-assessment, allowing the user to focus on the RMF process, cybersecurity posture assessments, or both.

The approach to the RMF expansion follows closely the individual RMF steps, wherein each step has several requirements. The DERCF tool addresses and assists the user with one or more of the following approaches:

- **Language**: Helper text or links to external sites to provide more context. This does not require any structural changes to the tool.
- **Guidance and documentation**: New tool functionality that allows for a user to input information for the purposes of documentation but does not provide an output (e.g., entering assets into a simple database to maintain a record).
- **Algorithm integration:** A collection of tool functionalities that use underlying mechanics and algorithms to provide dynamic and meaningful output based on input from the user.

This document is organized by the requirements for each of the seven RMF steps. The functionality of the DERCF tool may automate some of these steps or perform operations behind the scenes to enhance usability.

2.1 Prepare

As part of new content presented in Revision 2 of the Risk Management Framework (NIST 2018), the *Prepare* step is unique in that it applies to the other six steps simultaneously to add clarity and establish a solid foundation before moving on to the next steps. Preparation through the RMF's guidance assists the organization in executing RMF steps by viewing its DER systems from two perspectives:

1. **Organization level**: This perspective includes all assets that are operated by an organization.
2. **System level**: This perspective is limited to the scope of DER systems and their components.

These two perspectives are essential for understanding risk management, as an unclear definition of scope can make tasks for the future a near-impossible endeavor. The DERCF-RMF overlay focuses specifically on the system-level perspective to provide more clarity to DER cybersecurity and to narrow the scope.

Tasks for an organization during the *Prepare* step include but are not limited to:

- Assigning roles and responsibilities

- Identifying missions and business functions (for IT and OT) that relevant systems support at an organization and system level

- Identifying and prioritizing DER assets, stakeholders, and information.

An authorizing official is an individual designated to provide the official acceptance of risk during the RMF process. The preparation and subsequent steps should involve the authorizing official in reviewing and approving all efforts.

2.2 Categorize

The purpose of this step is to understand, organize, and document system-level data that are being processed, stored, and transmitted. It begins with the preliminary task of creating a system description.

2.2.1 System Description

Defining a clear system description is a critical step in cybersecurity management. One subtask of the *Categorize* step is to develop a system description documenting the characteristics of the system. This includes understanding relevant assets, scope, and connectivity. The process starts by an initial asset categorization followed by more detailed tiers of characteristics. At the most descriptive level, it includes identifying a list of specific assets organized by operating system, communication protocol, storage media, ownership characteristics, and procurement information.

To categorize assets in a complex DER system, the process starts by splitting the overall assets into several groups based on their type. For example, "*Windows*" installed on an engineering workstation is a characteristic that falls in the "*Operating System*" asset group. In any DER system, these asset groups can be organized into three different layers:

- **Logical layer**: This layer consists of different types of software components and characteristics such as operating system, firmware, application, standard software, etc.

- **Operational layer**: This layer supports the operations of the DER system and consists of different types of servers, media, clients, network components, etc.

- **Physical layer**: This layer consists of facilities, electrical assets, etc.

These asset groups send data and information to one another through the layers described above. The data and information are also categorized as assets, as they help keep the DER system operational.

- **Data**: Data are the content that are taken as input and output by a DER system. All data in a DER system are grouped based on their type, such as subscriber data, network data, security data, application data, etc.

- **Information**: In a DER system, information enables the operational technologies, communications, and controller hardware. This information is grouped based on its characteristics. For example, network configuration information manages the DER system's network and supporting processes. Operational information such as status, alerts, and logs help maintain smooth DER operation.

Figure 1 depicts a high-level view of asset categorization where assets are dispersed across all three layers.

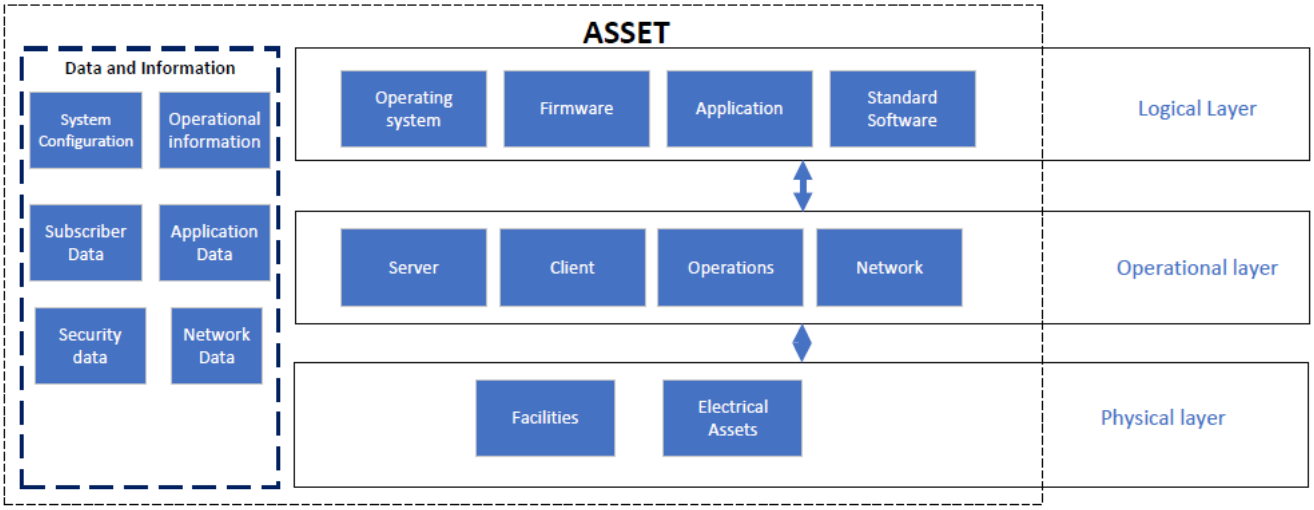

Figure 1. System description

2.2.2 System Categorization

Upon finalizing the system description, the process of system categorization begins. System categorization involves analyzing risk of loss and potential consequences utilizing documentation from Federal Information Processing Standards 199 (NISTd 2004). Not only does this categorization assist the site in identifying and documenting potential cybersecurity vulnerabilities, but it also provides a cohesive idea of security areas that need to be prioritized. The security categorization (SC) can be determined by the following expression, where each "impact" is to be assigned a value of low, medium, or high:[1]

$$SC_{\text{DER system}} = \{(\textbf{confidentiality}, \text{impact}), (\textbf{integrity}, \text{impact}), (\textbf{availability}, \text{impact})\}$$

Developing a system description is also part of the *Categorize* step. This provides clear context to avoid ambiguity for assets and the systems they comprise. The DERCF tool's expansion will walk users through identifying components of interest and assign an SC (low, medium, high) to their entire DER system. This value will be used later throughout the tool (such as when taking an assessment), as content will be oriented according to the determined SC. Agencies also have a space in the tool to describe their systems for extended documentation purposes. Once this is complete, the authorizing official reviews and approves the determined SC. NIST SP 800-18 provides more information on how to categorize systems appropriately (NISTe 2006).

[1] Official definitions for these terms can be found at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

2.3 Select

The *Select* step is the process of officially assigning a low, moderate, or high baseline for an entire site. Most of this process is taken care of behind the scenes after the SC of an asset has been established as low, medium, or high from the *Categorize* step.

The next component of the *Select* step is tailoring controls such that they are more appropriate for the site's system or risk. This can include changing controls or adding supplemental language, making controls more applicable to DER systems and their complexities. The DERCF-RMF tool begins by providing guidance from NIST on how to properly tailor controls, then allows the user to add supplemental text to provide justification or a supporting rationale for tailoring decisions within the framework to better suit their needs.

After the selection of the security controls through the derived baseline, the site can tailor these controls based on factors such as:

1. **Mission or business function**: The risk considerations for the DER system viewed from a site-wide perspective regarding strategic goals and objectives to carry out the operation.

2. **Risk tolerance**: The acceptable level of risk or degree of uncertainty based on unique avenues of privacy risks to the site's operation and assets, individuals, and other organizations.

3. **Type of DER system**: The risks associated to individual DER system components along with their interdependencies to other systems, networks, or devices.

2.4 Implement

The *Implement* step is a simpler, shorter step. Per subdomain, the DERCF application provides functionality for a user to add an electronic signature to verify that a set of controls, as identified by the *Select* step, has been implemented. This simple documentation step is critical in ensuring roles and responsibilities are being upheld and enforced. The DERCF-RMF application also ensures that mandatory configuration settings are established and implemented on system components in accordance with guidance and security plans.

Along with documenting control implementation, the security plan also needs to be updated with implementation details. For example, changes to planned inputs, expected behavior, and expected outputs with sufficient detail should be recorded to support the *Assess* step, discussed further in Section 2.5. The changes made to the baseline, including additions and revisions to controls, will be provided as an output of this step for documentation purposes. This provides organization representatives with the ability to track changes to controls, whether those changes were authorized, and the impact of the changes on the posture of the system and the site.

2.5 Assess

The *Assess* step is a critical point in which users determine whether controls have been implemented properly by identifying confidence levels. This task is performed by a member of the team or a team with extensive knowledge in the relevant systems, in conjunction with a supervisory role such as an energy systems manager. The organization is responsible for selecting the control assessor(s) for their organization, whose skills and technical expertise match the respective DER system(s).

The DERCF-RMF tool provides users an opportunity to respond to maturity-based questions regarding the implementations of their controls. Upon completion of this self-assessment, the user will have a clear perspective on the status of control implementations through the assessment report. This process will help determine the extent to which the selected controls are implemented correctly, operating as intended, and producing the desired outcome with respect to achieving security requirements for the system and site. This process will also provide documentation of implementation and serve as a metric for continuous monitoring plans in the future. The report developed by the control assessor is a key item in the authorization package that is developed for the authorizing official.

Guidance on developing an assessment plan and an assessment report will be provided in the tool by following NIST SP 800-53A (NISTb 2013). These plans are developed by the assessor from the implementation information.

2.6 Monitor and Authorize

The remaining two steps of the RMF, *Monitor* and *Authorize*, respectively, are the key components in finalizing the RMF process. Authorization is the official acceptance of a certain level of risk. Once the risks to assets and the site have been accepted, the *Monitor* step encourages agencies to check the effectiveness of system controls and document any changes that may have occurred. For these steps, the expanded version of the DERCF will include reminders such as customized alerts to encourage effective monitoring practices. By re-verifying the implementation of controls and updating any associated documentation regularly, cybersecurity becomes more routine.

While preliminary research for these steps is ongoing, the development of tool functionality for the *Monitor* and *Authorize* steps will begin in FY 2021.

3 Future DERCF Work

In addition to the added RMF functionality, the research team continues to add components to further enhance the DERCF and web tool experience.

Resource Library

The resource library is a collection of documents by NIST and other organizations to guide users, as well as references the NREL team used while creating the DERCF Framework. This searchable database will provide information on other frameworks, should the user need additional context.

Enhanced Analysis Features

This effort is primarily focused on providing additional insight and metrics by allowing the user to compare assessments and perform studies over time on their cybersecurity posture. An “assessment list” will be introduced to the interface, allowing a user to take as many assessments as they would like over a period of time and see their score comparisons, plus insight into posture improvements, all at a glance.

Furthermore, the existing dashboard functionality will be rebuilt to incorporate ongoing and past assessments and provide context for comparative analysis on assessment scores.

Video Training Database

For controls that might be complex to implement, the DERCF Web application will house several video trainings that provide a solid foundation from which to start, using guidance from NIST and other

references. Video content is designed to be a starting place for site managers who may be unfamiliar with certain aspects of cybersecurity.

Reporting

The method in which data are presented to a user can significantly impact how easily they are able to interpret and utilize the data. Future work on the DERCF application will enhance users' experience while they interact with the dashboard and action items.

4 Impact

Federal sites will have a go-to resource to ease RMF challenges with this expanded version of the DERCF. Additionally, the DERCF tool serves to document and track progress of cybersecurity maturity. The relationship established between NREL and federal sites during continued validation assessments, during which NREL walks through functionality with users, will help solidify cybersecurity practices for organizations and inform further DERCF improvements.

This research also supports future work in laying the foundation for additional functionality to assist organizations in achieving and maintaining their Authority to Operate, which is a subsequent, essential step in the RMF process.

5 References

National Institute of Standards and Technology (NISTa). *A Role-Based Model for Federal Information Technology/Cybersecurity Training*, by Patricia Toth and Penny Klein. NIST SP 800-16, Revision 1 (3rd draft). Gaithersburg, MD, 2014. https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/archive/2014-03-14.

National Institute of Standards and Technology (NISTb). *Assessing Security and Privacy Controls for Federal Information Systems and Organizations: Building Effective Assessment Plans*. NIST SP 800-53A, Revision 4. Gaithersburg, MD, 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

National Institute of Standards and Technology (NISTc). *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, by Ron Ross, Victoria Pillitteri, Richard Graubert, Deborah Bodeau, and Rosalie McQuaid. NIST SP 800-160, Volume 2. Gaithersburg, MD, 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf.

National Institute of Standards and Technology (NISTd). Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems. FIPS PUB 199. Gaithersburg, MD, 2004. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

National Institute of Standards and Technology (NISTe). *Guide for Developing Security Plans for Federal Information Systems*, by Marianne Swanson, Joan Hash, and Pauline Bowen. NIST SP 800-18, Revision 1. Gaithersburg, MD, 2006. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf.

National Institute of Standards and Technology (NISTf). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. NIST SP 800-37, Revision 2. Gaithersburg, MD, 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

National Institute of Standards and Technology (NISTg). *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST SP 800-53, Revision 4. Gaithersburg, MD, 2020. https://doi.org/10.6028/NIST.SP.800-53r4.

National Institute of Standards and Technology (NISTh). *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, Kevin Stine, Rich Kissel, William C. Barker, Jim Fahlsing, and Jessica Gulick. NIST SP 800-60, Volume I, Revision 1. Gaithersburg, MD, 2008. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf.

National Institute of Standards and Technology (NISTi). *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, Kevin Stine, Rich Kissel, William C. Barker, Jim Fahlsing, and Jessica Gulick. NIST SP 800-60, Volume II, Revision 1. Gaithersburg, MD, 2008 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf.

National Renewable Energy Laboratory (NREL). "Distributed Energy Resources Cybersecurity Framework." Last modified October 1, 2020. https://dercf.nrel.gov/.

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. https://www.nrel.gov/docs/fy20osti/75044.pdf.