# Guide to the Distributed Energy Resource Risk Management Framework

Dana-Marie Thomas, Anuj Sanghvi, MD Touhiduzzaman, Paul Wand, 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-5R00-81715
April 2022

# Guide to the Distributed Energy Resource Risk Management Framework

Dana-Marie Thomas, Anuj Sanghvi, MD Touhiduzzaman, Paul Wand, and Tami Reynolds

*National Renewable Energy Laboratory*

**Suggested Citation**

Thomas, Dana-Marie, Anuj Sanghvi, MD Touhiduzzaman, Paul Wand, and Tami Reynolds. 2022. *Guide to the Distributed Energy Resource Risk Management Framework.* Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-81715. https://www.nrel.gov/docs/fy22osti/81715.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-5R00-81715
April 2022

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.*

NREL prints on paper that contains recycled content.

# Acknowledgments

This guide was developed with support from the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Federal Energy Management Program (FEMP). Saralyn Bunch and Hayes Jones provided invaluable support and oversight throughout the project.

Ted Etter from the U.S. Department of Agriculture, Tom Nicklaus from the National Aeronautics and Space Administration, and Andy Shetland from the U.S. Navy each generously offered their perspectives and expertise. Nika Durham, Caitlin Dorsey, and Anthony Castellano from the National Renewable Energy Laboratory communications team provided editing and design support.

# List of Acronyms

| | |
|---|---|
| AO | Authorizing Official |
| ATO | Authority to Operate |
| CNSS | Committee on National Security Systems |
| DER | distributed energy resource |
| DER-CF | Distributed Energy Resource Cybersecurity Framework |
| DER-RM | Distributed Energy Resource Risk Manager |
| DMS | distribution management system |
| DR | demand response |
| eMASS | Enterprise Mission Assurance Support Service |
| EMS | energy management system |
| EV | electric vehicle |
| FDEMS | Facilities DER Management System |
| FedRAMP | Federal Risk and Authorization Management Program |
| FEMP | Federal Energy Management Program |
| FY | Fiscal Year |
| GIS | geographic information system |
| ICS | industrial control system |
| ISO | independent system operator |
| LAN | local area network |
| NIST | National Institute of Standards and Technology |
| NREL | National Renewable Energy Laboratory |
| NVD | National Vulnerability Database |
| OMS | Outage Management System |
| OSCAL | Open Security Control Assessment language |
| PCC | point of common coupling |
| POAM | plan of action and milestone |
| PV | photovoltaic |
| RMF | Risk Management Framework |
| RTO | regional transmission organization |
| SAR | security assessment report |
| SCADA | Supervisory Control and Data Acquisition |
| SSP | system security plan |
| WAN | wide area network |

# Executive Summary

The emergence of distributed energy resources (DERs) has transformed the electric power sector and will likely have even more profound impacts on the future evolution of the United States energy sector as it modernizes and becomes more reliant upon complex informatics programming and systems to ensure that our power grid remains safe from malicious interference.

In an effort to improve the nation's cybersecurity posture, Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017) recognizes the increasing interconnectedness of federal information systems while acknowledging that critical infrastructure is at risk due to the misalignment of many policies that govern information technology at a national level. Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource" (2016) addresses responsibilities for protecting federal information resources, requiring agencies to implement the Risk Management Framework (RMF), developed by the National Institute of Standards and Technology. Executive Order 14028: Improving the Nation's Cybersecurity (2021) clarifies the responsibility of the federal government to collaborate with the private sector to maintain a safe virtual environment that is agile and may be modified in tandem with the discovery of new cybersecurity threats and proactive mitigation of unknown future cybersecurity incidents.

This report aligns with priorities outlined in the Department of Energy's Cybersecurity Strategy, highlighting a cybersecurity risk management framework for DERs to prioritize and preserve technology investments, methods to improve responses to rapidly evolving threats, and DER cybersecurity solutions. It also demonstrates how the National Renewable Energy Laboratory leverages its work with DERs to develop and deliver innovative cybersecurity capabilities and solutions to improve the cybersecurity posture of critical energy infrastructure and other federal sector assets.

To mitigate risks associated with the increased and diversified use of DERs, the Distributed Energy Resource Cybersecurity Framework (DER-CF) was developed in 2019. The National Renewable Energy Laboratory extended the scope of the DER-CF to include the RMF. To address the challenges faced by federal energy managers and energy system stakeholders in applying the RMF to DER systems, the Distributed Energy Resource Risk Manager (DER-RM) is a six-step process to proactively manage cybersecurity risk in a methodical manner. The DER-RM is independent of the DER-CF's existing assessment, allowing users to focus specifically on the RMF steps. The tools are targeted to different processes—DER-CF enables organizations to perform self-assessments to improve their cybersecurity posture, while DER-RM assists organizations in achieving compliance with specific requirements.

This document provides an overview of the DER-RM. The RMF process outlined in this report serves as a guide to diagnose information and operational system threats, gather required materials to comply with industry standards, and document plans for achieving Authority to Operate. Using the DER-RM, federal agencies and other organizations can easily and intuitively follow the RMF process, manage the risks to their grid-edge infrastructure through the integration of their on-site DERs, and comply with appropriate requirements.

# Table of Contents

# List of Figures

# 1 Introduction

To address rapidly changing threats to the nation's critical energy infrastructure, the National Renewable Energy Laboratory (NREL) works to advance cybersecurity research and develop tools to assist federal agencies with the challenges of integrating more renewable energy sources.

Two recent executive orders highlight the growing cybersecurity threats associated with our increasingly interconnected energy and information systems. Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017) recognizes the increasing interconnectedness of federal information systems. Additionally, Executive Order 14028: Improving the Nation's Cybersecurity (2021) tasks government to partner with the private sector in order to strengthen the cybersecurity posture of the United States. This directive clarifies the importance of federal and private sector collaboration in order to maintain a safe virtual environment that is agile and may be modified in tandem with the discovery of new cybersecurity threats for proactive mitigation of unknown future cybersecurity incidents.

In furtherance of federal cybersecurity objectives, Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource," addresses agency responsibilities to protect federal information resources with a requirement to implement the Risk Management Framework (RMF) established in National Institute of Standards and Technology (NIST) Special Publication 800-37, Revision 2. The RMF process provides a well-organized and thorough approach to diagnosing information system threats, gathering required materials to comply with industry standards, and documenting a plan for achieving Authority to Operate (ATO).

Distributed energy resources (DERs) are grid-edge devices designed to generate and store energy in the case of interruptions to a site's main source of energy. DERs ensure continuity of operations at a time when efficiency and cost effectiveness are increasingly essential. These technologies are generally customized according to individual on-site energy needs. As new, diverse, and customized technologies, DERs may pose a cybersecurity risk to legacy infrastructure when integrating with grid components.

To mitigate risks associated with the increased and diversifying use of DERs, NREL developed the Distributed Energy Resource Cybersecurity Framework (DER-CF) starting in 2019. The DER-CF is a web-based tool useful in identifying risks introduced by renewable energy assets, and prioritizing investments to mitigate and manage those risks. While risk cannot be entirely eliminated, it can be mitigated, managed, and accepted with proper documentation and informed decision-making.

As required, an organization should develop a cybersecurity risk management plan for its overall site focused on preventing unauthorized access to its information technology and operational technology platforms (Foster, Lawson, and Cox 2020). In response to this critical need to address cybersecurity risk management, NREL extended the scope of the DER-CF to include the RMF, addressing the challenges faced by federal energy managers when applying the RMF to DER systems.

For energy managers who seek to focus exclusively on the RMF process, NREL's Distributed Energy Resource Risk Manager (DER-RM) is independent of the DER-CF's existing, broader self-assessment. Using the DER-RM application, federal agencies and other organizations can progress through the RMF process, manage the risks to their site from integration of DERs, and comply with appropriate requirements.

DER-RM is an open-source application, which allows access for a diversity of organizations, regardless of size. The system is created to be widely accessible, user-friendly, and reliable for organizations looking to use the DER-RM as a model for strengthening their cybersecurity infrastructure. The intention is to ensure that the concepts are transferrable and that organizations can assess their systems and create risk management strategies that are reliable and not burdensome.

## 1.1 Purpose of this Guide

The DER-RM was motivated by a desire to understand challenges associated with risk management for DERs. As partnerships with federal colleagues have expanded, the NREL team has developed an understanding of common challenges throughout the federal sector related to maintaining compliance with the requirements of the RMF process. The DER-RM was designed to alleviate the difficulties of maintaining compliance by providing a central repository to collect and organize the necessary documentation throughout the entire RMF process. NREL researchers found that this was a missing feature that would bring value to federal agencies and other organizations in the process of adding or replacing DERs within their respective energy systems.

This guide aids federal energy managers and energy system stakeholders going through the NIST RMF with a focus on DER-specific cybersecurity issues. The DER-RM is expected to continually integrate relevant NIST guidelines and frameworks with necessary cybersecurity controls to address evolving user needs. The DER-RM also provides a central repository to help organize and document DER system details to support the user as they progress through all the steps of the RMF. Within each RMF step, this tool provides functionality to help users build system security plans (SSPs), risk assessment reports (RARs), security assessment reports (SARs), and plan of action and milestone (POAM) reports by providing templates and organizational and management features to help generate the ATO package. The guide also details DER-RM capabilities for continuous monitoring of implemented controls to assist in maintaining ATO. Finally, the guide provides references regarding cybersecurity controls for DERs, including context and instructions for use of the downloadable tool in order to derive the most benefit.

The DER-RM is designed to be used by agencies required to undergo the RMF process for systems that need to be approved before they can be operational. The primary goal of the DER-RM is to provide a user-friendly interface and in-depth guidance for generating the authorization package for the Authorizing Official (AO) to review during the RMF process.

The DER-RM is a tool for users to dissect and analyze the RMF's incremental method and offers clear justifications for organizational compliance with the RMF. The recommendations provided within this guide help to translate the guidance from information systems in general to DERs and renewable energy systems in particular, with examples of DER-specific control implementations wherever applicable. This reinforces stronger adherence to agency-specific requirements and better risk management of DERs.

Organizations that employ or plan to integrate DERs can use the DER-RM application to navigate the RMF process through organization of reports and risk mitigation plans. The DER-RM provides a step-by-step approach for federal site managers to walk through the RMF, with the intent to streamline the process that the RMF requires of federal sites.

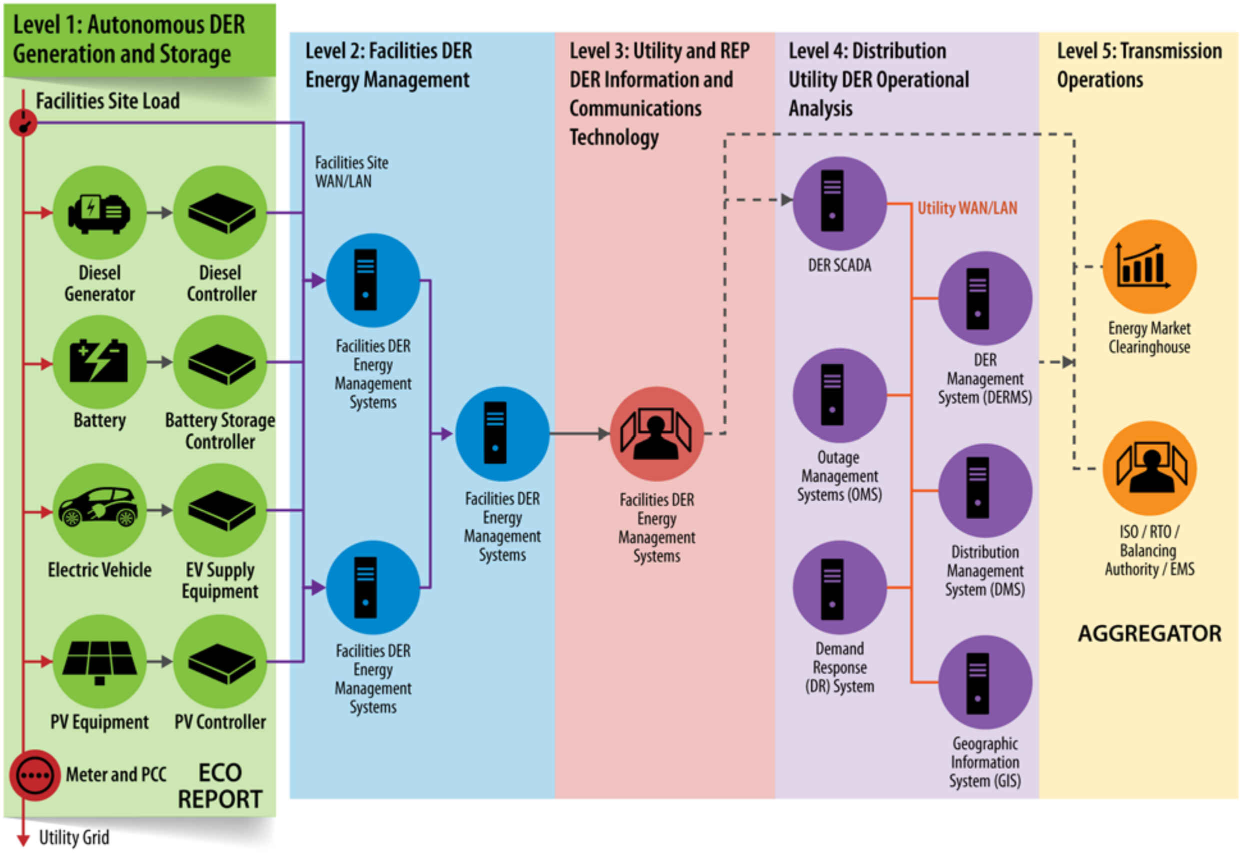
NREL's DER-RM includes specialized guidance for:

- Solar photovoltaic (PV) generation
- Wind energy generation
- Electric vehicle (EV) charging stations
- Distributed energy storage systems
- Hydropower generation.

The DER-RM approach considers each element of risk management, security, and privacy throughout the life cycle of a DER system. The application is agile in order to meet the needs of a diversity of DER sites while promoting proven RMF strategies.

# 2 Distributed Energy Resource Systems

DER systems are rapidly being adopted and integrated within the electric grid. DER systems are large and can be complex if an orderly approach is not used to control them. We propose a hierarchical approach, recognizing the distinction among all five levels of DERs, as shown in Figure 1.


Level 1: Autonomous DER Generation and Storage
Facilities Site Load
Diesel Generator
Diesel Controller
Battery
Battery Storage Controller
Electric Vehicle
EV Supply Equipment
PV Equipment
PV Controller
Meter and PCC
ECO REPORT
Utility Grid
Level 2: Facilities DER Energy Management
Facilities Site WAN/LAN
Facilities DER Energy Management Systems
Facilities DER Energy Management Systems
Facilities DER Energy Management Systems
Level 3: Utility and REP DER Information and Communications Technology
Facilities DER Energy Management Systems
Level 4: Distribution Utility DER Operational Analysis
DER SCADA
Utility WAN/LAN
DER Management System (DERMS)
Outage Management Systems (OMS)
Distribution Management System (DMS)
Demand Response (DR) System
Geographic Information System (GIS)
Level 5: Transmission Operations
Energy Market Clearinghouse
ISO / RTO / Balancing Authority / EMS
AGGREGATOR

PCC: point of common coupling. SCADA: Supervisory Control and Data Acquisition. WAN: wide area network. LAN: local area network ISO: independent system operator. RTO: regional transmission organization. EMS: energy management system.

**Figure 1. Five levels of DER. DER-RM enables facilities to assess the cybersecurity posture of Level 1, behind-the-meter assets that are owned and controlled by organizations themselves.**

Image adapted from Cleveland and Lee (2013) by Al Hicks, NREL

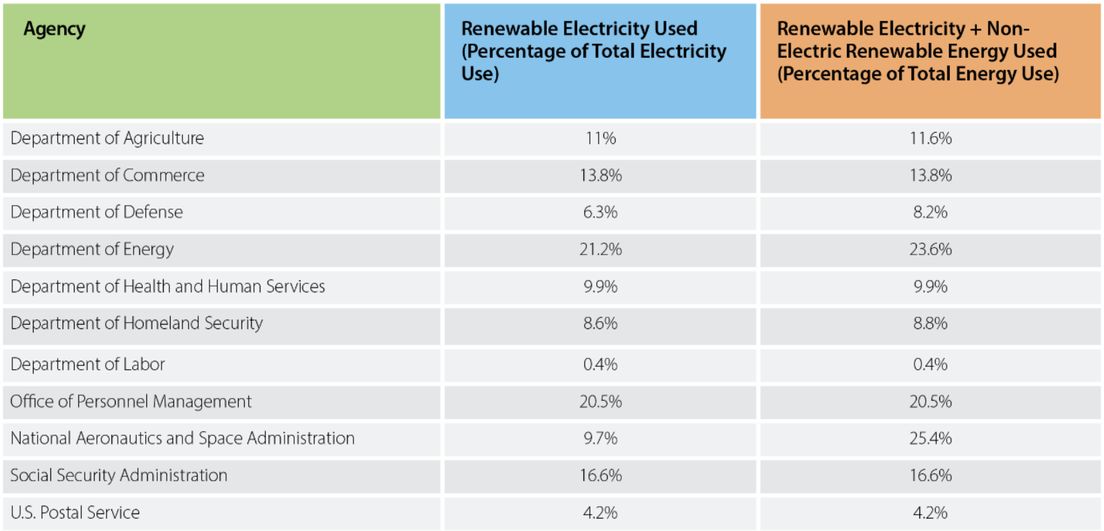
Figure 1 describes the complexity and interconnectedness of various DER systems. DER-RM focuses on assets that are owned by organizations with the aim of incorporating additional renewable energy resources at their facilities. The highlighted portion of Figure 1 emphasizes the level 1 DER assets that are usually behind the meter and generally operate under the authorization of the facilities.

## 2.1 The Growth of DERs

Worldwide investment in the renewable energy sector was $282.2 billion in 2019, with the United States investing $55.5 billion (Zhou 2021). Federal Energy Management Program (FEMP) federal government-wide performance data for Fiscal Year (FY) 2020 reveal the federal government exceeded a goal of 7.5% renewal electricity penetration, actually achieving -9% of electricity use with renewable energy. The United States has a targeted goal to reach 100% carbon-free electricity by 2035 (U.S. Office of the Press Secretary 2021).

FEMP data in Table 1 from the FY 2020 Office of Management and Budget Scorecard for Efficient Federal Operations/Management reveal renewable energy use among select federal government agencies for illustrative purposes.

**Table 1. Renewable Energy Use Among Select Federal Government Agencies, FY 2020**



| Agency | Renewable Electricity Used (Percentage of Total Electricity Use) | Renewable Electricity + Non-Electric Renewable Energy Used (Percentage of Total Energy Use) |
|---|---|---|
| Department of Agriculture | 11% | 11.6% |
| Department of Commerce | 13.8% | 13.8% |
| Department of Defense | 6.3% | 8.2% |
| Department of Energy | 21.2% | 23.6% |
| Department of Health and Human Services | 9.9% | 9.9% |
| Department of Homeland Security | 8.6% | 8.8% |
| Department of Labor | 0.4% | 0.4% |
| Office of Personnel Management | 20.5% | 20.5% |
| National Aeronautics and Space Administration | 9.7% | 25.4% |
| Social Security Administration | 16.6% | 16.6% |
| U.S. Postal Service | 4.2% | 4.2% |

Sources: Agency-submitted data from Annual Energy Data Report, EISA 432 Compliance Tracking System, Federal Real Property Profile, Federal Automotive Statistical Tool, and Federal Procurement Data System. Agency renewable electric energy consumption is submitted to FEMP through Annual Energy Data Reports. Details and background data can be found on FEMP's Comprehensive Annual Energy Data and Sustainability Performance data site (FEMP 2021).

# 3 Description of the DER-RM Application

The DER-RM was developed to help federal agencies and other organizations to strengthen their risk management processes and improve DER operational security of their on-site, behind-the-meter assets (see Figure 1). The tool is unique in that it centers around an agile, content-driven approach; serves as an internal-facing application to aid research and investigations based on user behavior; and acts as a user experience-focused application to encourage repeated use. The tool also generates an ATO package once the assessment is completed. DER-RM allows users to prepare for navigating through the steps of the RMF by structuring questions about the facility and the DER system. This information is then utilized to enhance the user experience by customizing the stepwise process for each facility. The tool also provides recommendations for DER control implementation.

Designed to be a standalone application, the DER-RM is functional without external connections for the purpose of securely navigating through DER system-level questions. The DER-RM is a framework that generates documentation for AO review, and includes an easy to interpret and customized report that identifies common vulnerabilities and prioritizes mitigation strategies. The DER-RM addresses a critical consideration—the vulnerability of DERs to a range of operational risks—which does not exist in other well-known frameworks today.

## 3.1 Key Features of DER-RM

The DER-RM combines specifications from NIST 800-37, 800-53, and 800-82 into an application that guides users through the RMF process with respect to controls tailored for DER-powered facilities. DER operators are responsible for ensuring uninterrupted energy and continuity of operations during an outage. Often, DER security is taken for granted, which makes it an easy target for intentional, malicious acts like ransomware. Implementing the RMF serves as a specific preventive measure for DER systems and is advised to achieve and maintain resilience.

The DER-RM is used not only for navigating the RMF process, but also for tailoring recommended DER-based controls to save user time. The tool can develop comprehensive SSPs, SARs, risk assessment reports, SSAs, and POAM reports that form the basis of the ATO package. The DER-RM has a user-friendly interface with options to maintain history, and the application is operated offline.

The DER-RM expands upon the MITRE ATT&CK industrial control system (ICS) framework to populate generic control system threats and techniques and define mitigation strategies for the user's DER system assets (MITRE 2021). MITRE ATT&CK for ICS is a trusted resource built upon actual examples of cybersecurity breaches. The information from these attack patterns is mapped to controls from NIST 800-53 to provide actionable plans of action and risk reports.

The DER-RM supports the import and export of Open Security Control Assessment Language (OSCAL) formatted data, which allows it to act as an element of an automated pipeline for security control implementation. Support for Enterprise Mission Assurance Support Service (eMASS) and Federal Risk and Authorization Management Program (FedRAMP) SSP template import/export is a feature currently under consideration to widen DER-RM support for authorization package integrations.

The DER-RM contains embedded data from the National Vulnerability Database (NVD), the government's key resource for cataloging and sharing cybersecurity vulnerabilities as they are verified and known. Users can enable live updates to automatically connect to the NVD, ensuring the most up-to-date information on vulnerabilities. Common Vulnerabilities and Exposures are mapped to MITRE attack patterns using a Natural Language Processing classifier so that tools for prevention and mitigation of vulnerabilities can be provided with respect to the system architecture.

## 3.2 Methodology

Risks related to the integration of newer renewable energy assets were identified based on experience conducting cyber governance, technical management, and physical security assessments for utilities and federal sites. Feedback from federal energy managers also indicated a major related challenge in fulfilling requirements for executive approval of these projects. To manage, reduce, and mitigate cyber risks and impacts to site operations, personnel, equipment, and the nation's safety, it is crucial to address these challenges and advance the agencies' missions. We initiated discovery discussions and then conducted preliminary assessments to identify areas of concern. The DER-RM was developed to meet identified agency needs by simplifying and expediting the RMF processes.

### 3.2.1 Technical Approach to the Tool

Throughout the RMF process, immense quantities of information must be stored, serialized, versioned, and encrypted. Historically, this has been an exhaustive process entailing the creation of zip files with folders of Microsoft Excel spreadsheets and Word documents, as well as manual verification of control implementation details. The DER-RM is built using Ionic React (Ionic 2021) and Electron (2021) and the data model is validated using JSON schema technology.

#### 3.2.1.1 OSCAL

NIST recently published the first official version of the Open Security Control Assessment language, known as OSCAL. The intent behind the language is to provide a machine-readable format with which all types of software can store and manage authorization package data. Historically, authorization packages have been challenging to work with and have taken the form of large collections of Word and Excel documents or proprietary program-specific formats. OSCAL was created to standardize SSPs and POAMs, as well as provide a machine-readable format for continuous monitoring of security control implementation.

##### 3.2.1.1.1 Importing and Exporting OSCAL

NIST provides JSON and XML schemas which are generated by their custom ‘meta-schema’ technology. These schemas can be leveraged to validate incoming data and guarantee that the information being imported or exported will be readable by the next OSCAL-compatible application in the pipeline. The schemas are designed such that the shape of the data is extremely predictable and is simultaneously flexible enough to store any type of additional property. Organizations can publish metadata property vocabularies to standardize the sort of additional metadata their OSCAL-compatible organizations will provide. FedRAMP has been working closely with NIST to provide name spaced metadata expectations for attaining ATO for cloud software-as-a-service providers.

##### 3.2.1.1.2 OSCAL in the DER-RM

OSCAL document fields closely correlate with the steps in the RMF. Nearly every step of the RMF process can be documented and stored in an OSCAL format. In the DER-RM implementation, an OSCAL workspace is created, and using several easy-to-use widgets, an SSP is created and validated. Data is stored locally in an indexed database and the application runs utilizing Electron, the same technology that powers Microsoft Teams.

## 3.3 DER-RM Steps

The DER-RM’s primary purpose is to assist federal agencies in navigating compliance with government requirements by helping to proactively manage DER cybersecurity risk using the methodical manner presented in the RMF, as described in NIST Special Publication 800-37. Undergoing the RMF process positions federal agencies to better achieve compliance. DER-RM enhances the RMF process by automating system categorization requirements to adapt to specific organizational needs and presents appropriate and aligned templates with recommendations. It achieves this purpose by providing knowledge and guidance on the application of NIST controls and DER-RM specific approaches, so the users understand the required steps and manage risk effectively. DER-RM extends the user-friendly interaction that will not only prepare the agency to reduce and mitigate operational risk, but also calculate risk scores and provide system-specific requirements through real-world examples specifically focused on DER systems.

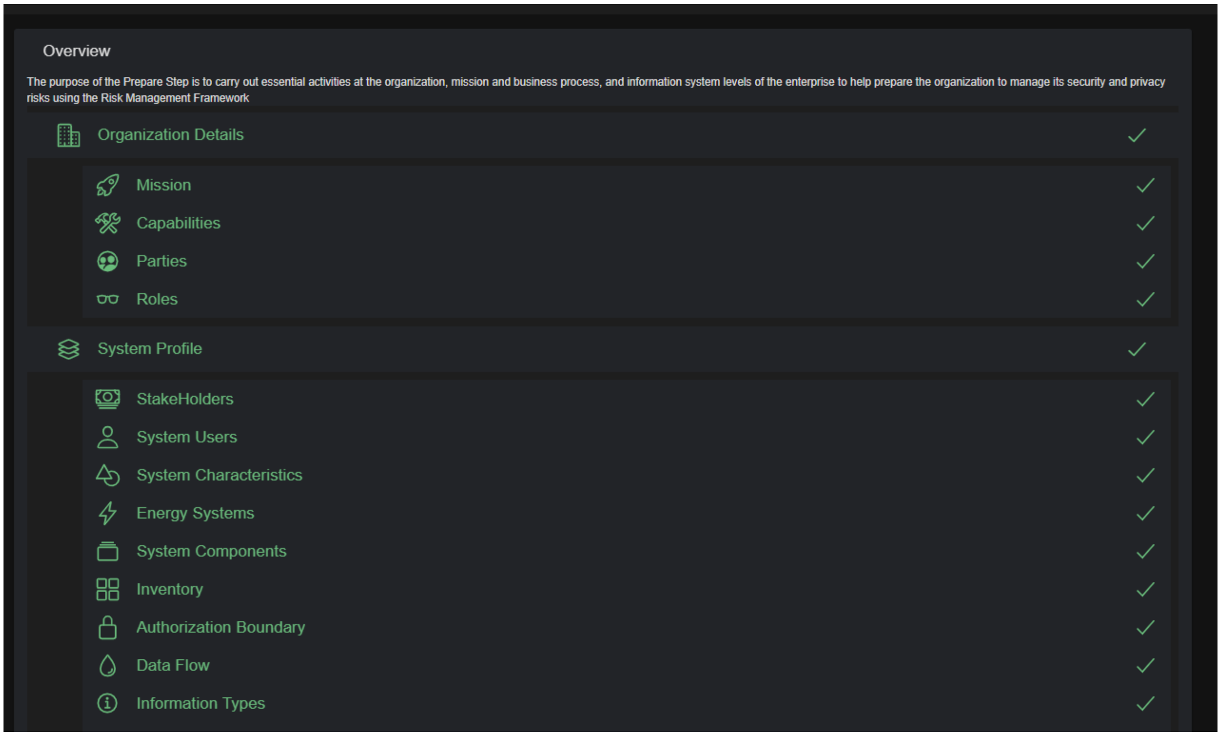
The DER-RM addresses each step in the RMF, ensuring that the application is neutral and may be used across operating systems.

### 3.3.1 Prepare

**Requirements:** The *prepare* step is intended to leverage the activities already being conducted by any federal site and is divided into organization- and system-level tasks.

**Implementation Challenges:** An agency usually has defined organization-wide procedures concerning security and privacy, which cover tasks such as establishing risk management roles, formulating the risk management strategy, conducting risk assessments, deployment of organization-wide common controls, and other strategies. These may need to be documented multiple times at different stages of the RMF process.

**DER-RM Approach:** DER-RM's process guides users to collect relevant information beyond those policies and procedures, including business functions, assets, information types, and other system-dependent information. Each of the substeps of the system-level *prepare* tasks are structured as interactive features that help users provide the necessary information. The application enumerates each information-gathering task needed to populate and generate later reports. Without the *prepare* step, users would be required to repeatedly enter system information at various stages of the RMF process, vastly increasing required time. By making collected information more broadly applicable, DER-RM simplifies completion of subsequent steps.



Overview

The purpose of the Prepare Step is to carry out essential activities at the organization, mission and business process, and information system levels of the enterprise to help prepare the organization to manage its security and privacy risks using the Risk Management Framework

Organization Details ✓

- Mission ✓
- Capabilities ✓
- Parties ✓
- Roles ✓

System Profile ✓

- StakeHolders ✓
- System Users ✓
- System Characteristics ✓
- Energy Systems ✓
- System Components ✓
- Inventory ✓
- Authorization Boundary ✓
- Data Flow ✓
- Information Types ✓

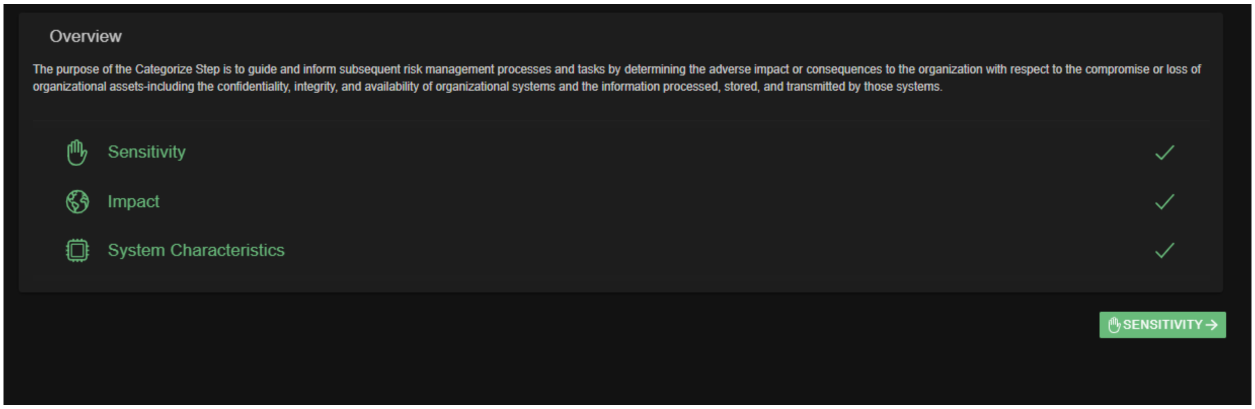
**Figure 2. System-level preparatory tasks assist with identifying the business function, assets, information types, and other system-dependent information.**

### 3.3.2 Categorize

**Requirements:** Categorization of the identified DER system is one of the more important steps of the RMF process. The purpose of this step is to understand, organize, and document a DER system description and the types of information being processed, stored, and transmitted. The overall system is categorized by first describing the various components involved within a DER system including the information types as mentioned in NIST Special Publication 800-60.

**Implementation Challenges:** It is critical to ensure that proper emphasis is given to data confidentiality, integrity, and availability and the impacts of respective losses based on the information types. It is also important to have all the required dependencies identified and applied to the DER system.

**DER-RM Approach:** In the DER-RM, emphasis is given to the information types associated with energy production and communication. DER-RM makes describing DER characteristics easier by supporting descriptive names for the system and subsystem, identifiers, version, responsibilities, purpose and function of the system, and so forth. Once the DER system is described and documented, the DER-RM provides flexibility in conducting a security categorization using either FIPS 200 (NIST 2006) to establish a single impact level for a system based on high-water mark, or Committee on National Security Systems (CNSS) Instruction 1253 (CNSS 2014) to establish three impact values that may vary based on confidentiality, integrity, and availability required for national security systems. DER-RM automates this selection based on the agency type but also provides flexibility to select it manually.



Overview

The purpose of the Categorize Step is to guide and inform subsequent risk management processes and tasks by determining the adverse impact or consequences to the organization with respect to the compromise or loss of organizational assets-including the confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

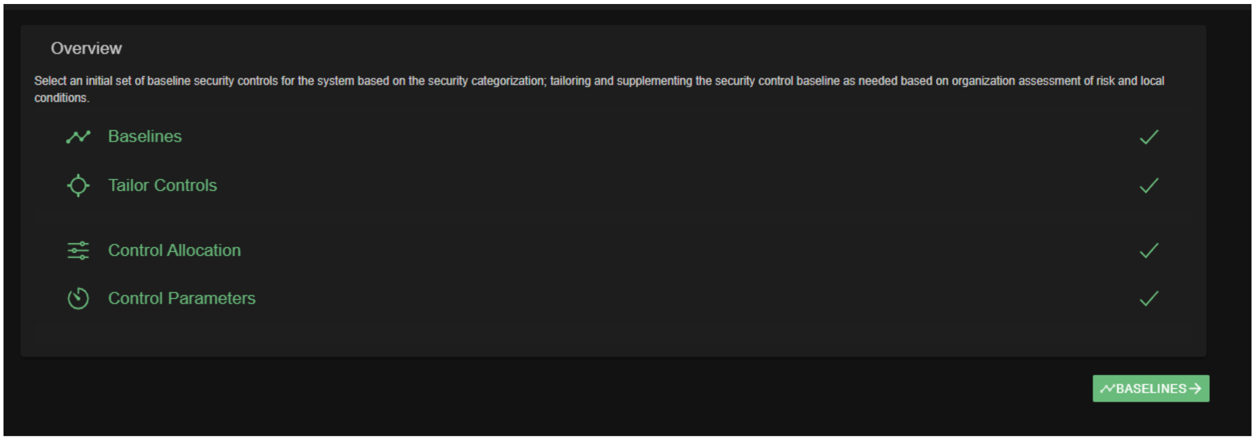
**Figure 3. During the *categorize* step, users determine potential adverse impacts or consequences to the organization in order to inform subsequent risk management processes and tasks.**

### 3.3.3 Select

**Requirements:** NIST Special Publication 800-37 proposes control baselines to protect the system based on the results of system categorization. Once tailored, controls are designated as system-specific, hybrid, or common based on their application. Allocation of controls can also be documented as a part of this step.

**Implementation Challenges:** Selection of security controls is typically a tedious task, and finalizing these selections is the most time-consuming component of the RMF process for many agencies. Once controls are selected from the NIST catalog, users must tailor the controls to meet individual agency requirements. This is an important step that provides a place for system owners to work with agency managers and even AOs to come to a common understanding in selecting appropriate controls for their system.

**DER-RM Approach:** The DER-RM enables each of these requirements for the *select* step and also acts as a repository of NIST control catalog specifications. Additionally, to enhance the user experience, the DER-RM gives the user the flexibility to either tailor the controls or leverage DER-specific controls and recommendations.



Overview

Select an initial set of baseline security controls for the system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions.

- Baselines ✓
- Tailor Controls ✓
- Control Allocation ✓
- Control Parameters ✓

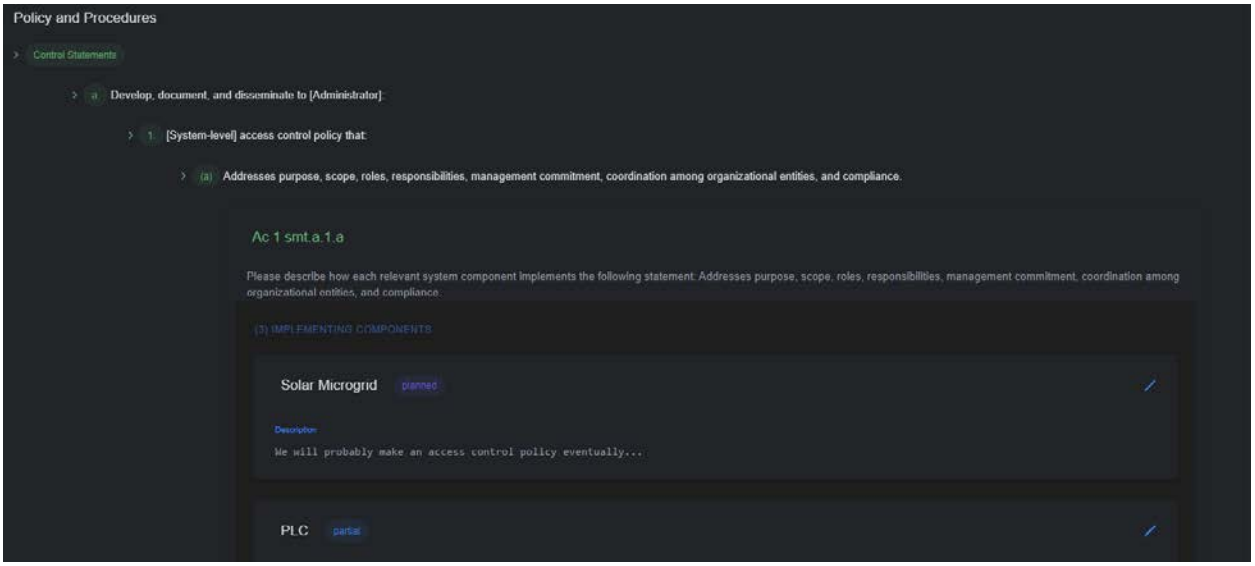
**Figure 4. The DER-RM enables the requirements for the *select* step and also acts as a repository of the NIST control catalog.**

### *3.3.4 Implement*

**Requirements:** The *implement* step recognizes the controls selected previously and allows the organization to implement the measures needed and then document further details. Variations are often required when executing the selected controls, and these variations or alterations must be documented.

**Implementation Challenges:** Organizations need to carefully plan the control implementation step as it forms the basis for the entire RMF process. In light of the potentially extensive tailoring that took place in the *select* step, it is important to document all the details of control implementation.

**DER-RM Approach:** The functionality provided by the DER-RM allows the user to elaborate on the configuration detail that accounts for their site-specific needs. The application also enables users to document the details and the status of their implemented controls. As part of the *monitoring* step, future DER-RM development plans include a control expiration and notification feature to enhance the process of maintaining the ATO. These added functions within the *implement* step enable continued system operations over time.



Policy and Procedures

a. Develop, document, and disseminate to [Administrator]:

1. [System-level] access control policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

Ac 1 smt.a.1.a

Please describe how each relevant system component implements the following statement: Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

(3) IMPLEMENTING COMPONENTS

Solar Microgrid planned

Description

```
We will probably make an access control policy eventually...
```

PLC partial

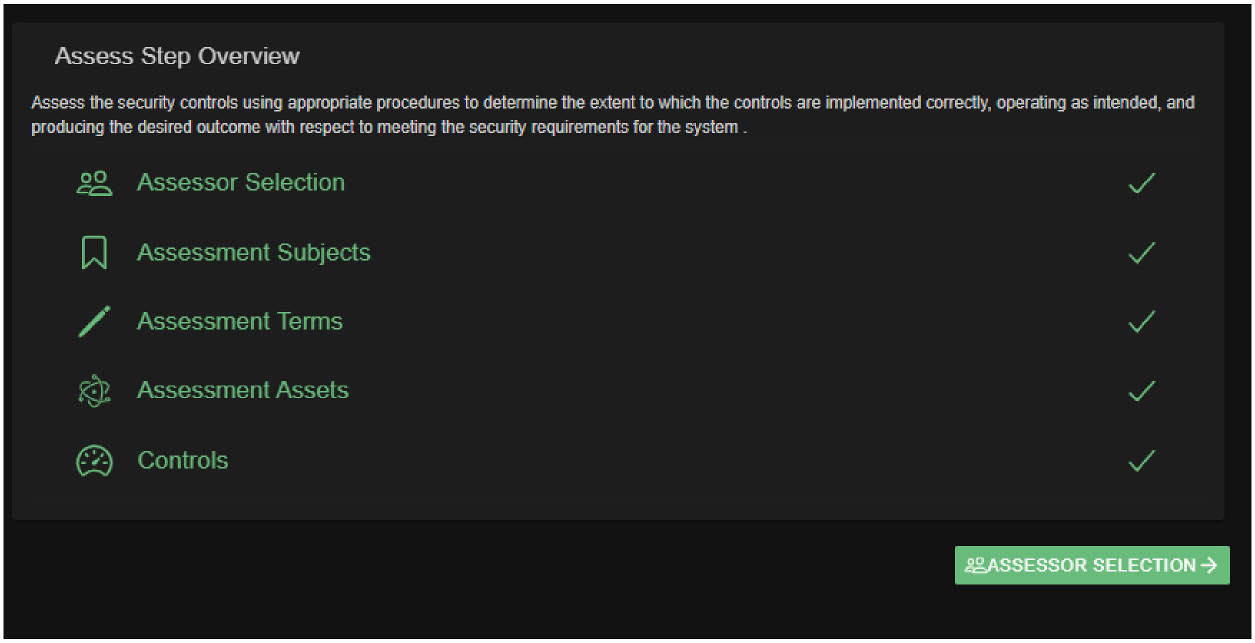
Figure 5. The DER-RM allows the user to elaborate on the configuration detail that accounts for site-specific needs.

### 3.3.5 Assess

**Requirements:** The purpose of the *assess* step is to validate that the implemented controls and measure outcomes have reduced or mitigated risk, thereby achieving a level of residual risk that is satisfactory to the organization.

**Implementation Challenges:** This step requires selection of an appropriate assessor or team of assessors, followed by formation of an assessment plan that involves documentation of the assessment process. Assessing the implementation of controls also helps with remediation actions for the residual risk. This is the risk that needs to be addressed after the controls are in place based on the controls' performance.

**DER-RM Approach:** The DER-RM application streamlines development of an assessment plan through standardized templates that potential assessors can leverage. Along with generating the SAR, the tool assists with generating the POAM for the risks that remain to be mitigated or managed. This documentation is critical for achieving ATO.



Assess Step Overview

Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system .

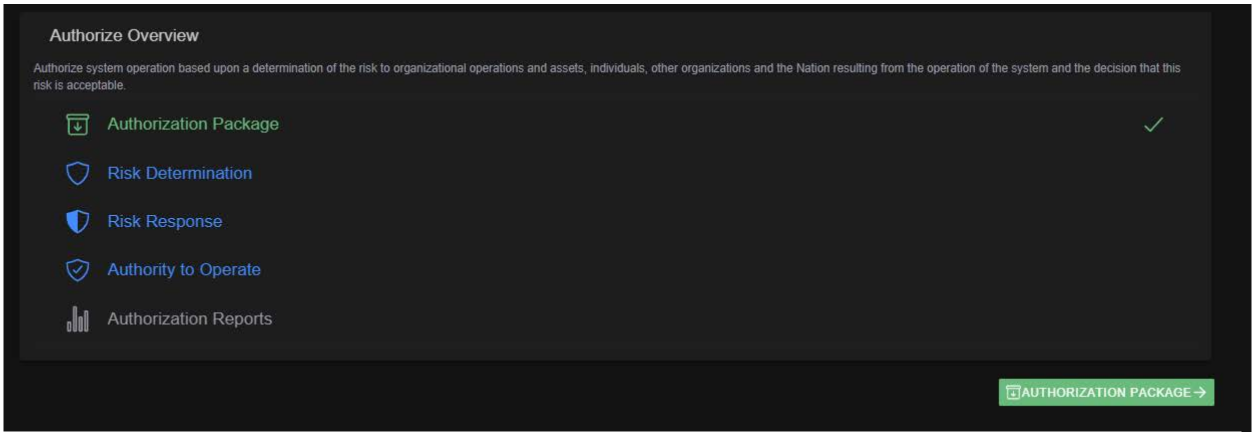
**Figure 6. The DER-RM application streamlines development of an assessment plan through generic templates that potential assessors can leverage.**

### *3.3.6 Authorization*

**Requirements:** Authorization consists of small, intentional steps that enable organizations to develop and implement complete and reliable documentation and confirmation of risks, system dynamics, mitigation plans, and control assessments. The DER system owner and senior agency officials are required to develop the authorization package for the AO. The DER system owner's ability to operate and conduct experiments on the system depends on the acceptance or acknowledgment of associated risks by the AO. The AO reviews the necessary and supporting documents—such as risk analyses and determinations, risk response, and plans of action for implementing future controls—before approving the package.

**Implementation Challenges:** Within the *authorization* step, the user must essentially accumulate and analyze system and organizational risks along with appropriate responses for the AO to consider and review. Depending on the AO's response, the user may need to repeat some steps of the assessment, thus creating updated versions of the reports in real time.

**DER-RM Approach:** The DER-RM helps users navigate through specific questionnaires based on agency requirements, and it assembles the necessary reports as a result of the assessment. This automated feature of the DER-RM makes accountability and document verification much easier, along with the added function of version control for the system owners and AO to track changes.


Authorize Overview

Authorize system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the system and the decision that this risk is acceptable.

**Figure 7. The DER-RM helps users navigate through specific questionnaires based on agency requirements, and it assembles the necessary reports as a result of the assessment.**

### *3.3.7 Monitoring*

**Requirements:** The purpose of monitoring is to maintain a desired level of risk tolerance by continuously verifying the status of implemented controls, confirming the need for or completion of change management, and performing ongoing assessments through sustained situational awareness of the DER system. Developing continuous monitoring strategies to assist with ongoing risk assessments enables ongoing authorization of the system and continuity of operations.

**Implementation Challenges:** It is of utmost importance to effectively manage continuous monitoring strategies for NIST's security control implementation, which enable ongoing authorizations through updated reports within the ATO package as additional devices are integrated and monitored.

**DER-RM Approach:** The DER-RM can notify users of any interactions through a number of methods, according to user preferences. The point at which the user must decide whether the system will require a new ATO package depends on the system's assessment of user inputs and the reported operational environment. The DER-RM will also feature version control of previous authorization reports enabling smoother maintenance of ATO.

# 4 Conclusion

DERs are becoming increasingly important as their worldwide cumulative capacity grows each year. DERs are equipped with complex, data-driven communications networks to connect with the energy grid. The growing number of smart devices that support DERs also increases the number of access points outside a utility's administrative domain, which can increase the potential for cyberattack. Maintaining ATO compliance requires that the cybersecurity risks associated with integrating DER systems at federal sites must be understood and managed to an acceptably low level. NIST created standards detailing the RMF used to assess and manage these risks.

NREL’s DER-RM allows users to focus on the six-step RMF process. The DER-RM allows users to dissect and analyze the RMF’s incremental method and offers clear justifications for organizational compliance with the RMF. It is a downloadable application that runs locally and documents all the major requirements for achieving ATO for DERs.

Future research on this project will include (1) modeling and visualization of services that DERs can provide; (2) expanding the foundation for renewable energy infrastructure development; (3) implementing additional DER-RM tool functionality to assist organizations in achieving and maintaining ATO—a subsequent, essential step in the RMF process; and (4) developing interoperable automation frameworks and tools for government and industry.

# References

Cleveland, Frances and Annabelle Lee. 2013. *Cybersecurity for DER Systems*. Washington, DC: Electric Power Research Institute. http://smartgrid.epri.com/doc/der%20rpt%2007-30-13.pdf.

Committee on National Security Systems. 2014. "Instruction No. 1253: Security Categorization and Control Selection for National Security Systems." https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf.

Electron. 2021. "Build cross-platform desktop apps with JavaScript, HTML, and CSS." Accessed September 15, 2021. https://www.electronjs.org/.

Executive Order No. 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 82 CFR 32172 (2017).

Executive Order No. 14028: Improving the Nation's Cybersecurity, 86 CFR 26633 (2021).

Federal Energy Management Program. 2021. "Federal Comprehensive Annual Energy Performance Data." Accessed October 26, 2021. https://www.energy.gov/eere/femp/federal-comprehensive-annual-energy-performance-data.

Foster, J., S. Lawson, and S. Cox. 2020. *Cybersecurity and Distributed Energy Resources.* Golden, CO: National Renewable Energy Laboratory. https://www.nrel.gov/docs/fy20osti/76307.pdf.

Ionic. 2021. "One Codebase. Any Platform. Just React." Accessed September 15, 2021. https://ionicframework.com/docs/react.

MITRE. 2021. "ATT&CK for Industrial Control Systems." Accessed September 13, 2021. https://collaborate.mitre.org/attackics/index.php/Main_Page.

National Institute of Standards and Technology. 2006. *FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

National Institute of Standards and Technology. 2018. *NIST Special Publication 800-37, Revision 2: Risk Management Framework for Information Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

National Institute of Standards and Technology. 2020. *NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

United States. 2016. *OMB circular A-130, Managing Information as a Strategic Resource*. Washington, DC: Executive Office of the President, Office of Management and Budget. https://www.cio.gov/policies-and-priorities/circular-a-130/

U.S. Office of the Press Secretary. 2021. "President Biden Sets 2030 Greenhouse Gas Pollution Reduction Target Aimed at Creating Good-Paying Union Jobs and Securing U.S. Leadership on Clean Energy Technologies." *The White House*, April 22, 2021. Accessed September 23, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/22/fact-sheet-president-biden-sets-2030-greenhouse-gas-pollution-reduction-target-aimed-at-creating-good-paying-union-jobs-and-securing-u-s-leadership-on-clean-energy-technologies/.

# Bibliography

Cichonski, P., T. Millar, T. Grance, and K. Scarfone. 2012. *NIST Special Publication 800-6, Revision 2: Computer Security Incident Handling Guide*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Dempsey, K., N. Chawla, A. Johnson, R. Johnston, A. Jones, and A. Orebaug et al. 2011. *NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

Dempsey, K., V. Yan Pillitteri, C. Baer, R. Niemeyer, R. Rudman, and S. Susan. 2020. *NIST Special Publication 800-137A: Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-137A.pdf.

Federal Energy Management Program. 2020. "Federal Comprehensive Annual Energy Performance Data." Accessed August 20, 2021. https://ctsedwweb.ee.doe.gov/Annual/Report/Report.aspx.

Federal Energy Management Program. 2021. "EISA Federal Covered Facility Management and Benchmarking Data." Accessed August 20, 2021. https://www.energy.gov/eere/femp/eisa-federal-covered-facility-management-and-benchmarking-data.

Johnson, A., K. Dempsey, R. Ross, S. Gupta, and D. Bailey. 2011. *NIST Special Publication 800-128: Guide for Security-Focused Configuration Management of Information Systems*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf.

Durham, Nika. 2020. "New Directions Sharpen NREL's Cybersecurity Research, Protecting Energy Systems Beyond the Grid Edge." *National Renewable Energy Laboratory.* October 29, 2020. https://www.nrel.gov/news/features/2020/new-directions-sharpen-nrels-cybersecurity-research.html.

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

National Institute of Standards and Technology. 2011. *NIST Risk Management Framework Quick Start Guide Roles and Responsibilities Crosswalk.* Gaithersburg, MD: National Institute of Standards and Technology. https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/Additional%20Resources/NIST%20RMF%20Roles%20and%20Responsibilities%20Crosswalk.pdf.

National Institute of Standards and Technology. 2014. *NIST Special Publication 800-53A, Revision 4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

National Institute of Standards and Technology. 2020. *NIST Special Publication 800-53B: Control Baselines for Information Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

Office of the Federal Chief Sustainability Officer. 2021. "Federal Sustainability Progress, Plans, and Performance." Accessed August 20, 2021. https://www.sustainability.gov/performance.html

Powell, C., K. Hauck, A. Sanghvi, T. Reynolds. 2020. *Distributed Energy Resource Cybersecurity Framework Best Practices*. Golden, CO: National Renewable Energy Laboratory. https://www.nrel.gov/docs/fy20osti/75921.pdf.

Sanghvi, A. 2021. "Risk Management for Distributed Energy Resources." Golden, CO: National Renewable Energy Laboratory. https://www.nist.gov/system/files/documents/2021/02/22/Day1.7-Anuj%20-%20DER-RM_NIST%20presentation.pdf.

Stine, K., R. Kissel, W. Barker, J. Fahlsing, and J. Gulick. 2008. *NIST Special Publication 800-60, Volume I, Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf.

Swanson, M., P. Bowen, A. Phillips, D. Gallup, and D. Lynes. 2010. *NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

The White House. 2013. "Presidential Policy Directive -- Critical Infrastructure Security and Resilience." Office of the Press Secretary. February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Touro College Illinois. 2021. "The 10 Biggest Ransomware Attacks of 2021." Accessed August 20, 2021. https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php.

U.S. Department of Energy. 2021. "U.S. Installed and Potential Wind Power Capacity and Generation." Accessed August 20, 2021. https://windexchange.energy.gov/maps-data/321.

U.S. Department of Energy. 2021. *EERE Cybersecurity Multiyear Program Plan.* Washington, DC: U.S. Department of Energy. https://www.energy.gov/sites/default/files/2021-06/EERE-Cybersecurity-Multiyear-Program-Plan-opt.pdf.

U.S. Department of Energy Alternative Fuels Data Center. 2021. "Electric Vehicle Charging Station Locations." Accessed August 20, 2021. https://afdc.energy.gov/fuels/electricity_locations.html#/find/nearest?fuel=ELEC.

U.S. Department of Homeland Security. 2013. *National Infrastructure Protection Plan*. Washington, DC: U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

Zhou, E., G. Brinkman, V. Gevorgian, E. Hale, D. Hurlbut, J. Logan, B. Mather, and Y. Zhang. 2021. *Clean Grid Vision: A U.S. Perspective – Executive Summary*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5C00-80268. https://www.nrel.gov/docs/fy21osti/80268.pdf.