Cybersecurity Assessment Tools for Distributed Energy Resources

Tami Reynolds

Project Manager & Lead

Energy Exchange 2021

Tami Reynolds

Project Manager & Lead, Secure Cyber-Energy Systems

National Renewable Energy Laboratory

Cybersecurity for Distributed Energy Resources

Modern energy systems are increasingly reliant on smaller decentralized generation sources or **distributed energy resources (DERs)** such as solar PV, wind, and energy storage.

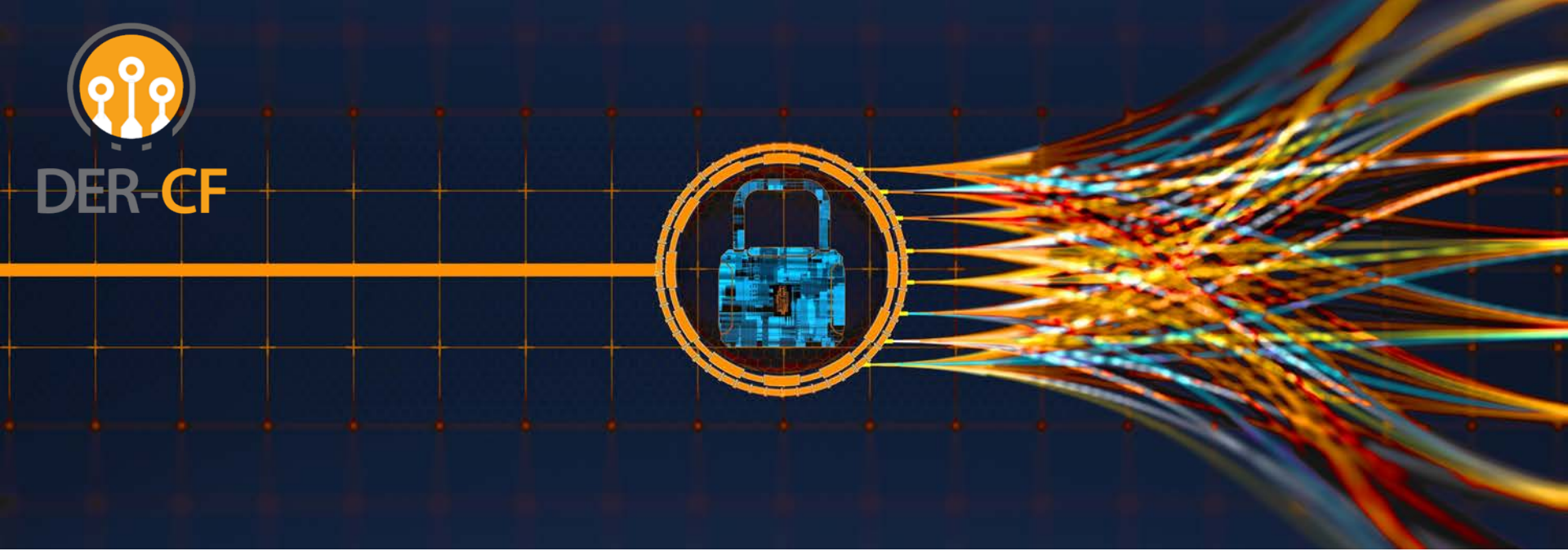
- DERs are equipped with complex, data-driven communications networks to connect with the energy grid.
- The growing number of smart devices that support DERs can increase the number of access points outside a utility's administrative domain, which can increase the potential for cyberattack.

With the integration of DERs at federal sites, the cybersecurity vulnerabilities of DER systems must be understood and addressed.

The Distributed Energy Resource Cybersecurity Framework (DER-CF)

Cybersecurity Assessment for Distributed Energy Resources

- NREL conducted over 30 assessments for utilities across the United States with a cybersecurity assessment tool based on the DOE Cyber Security Capability Maturity Model (C2M2) and the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and focused on business process.
- With funding from the U.S. Department of Energy (DOE) Office of Renewable Energy and Energy Efficiency Federal Energy Management Program (FEMP), NREL modified the current cyber governance assessment tool to include an assessment process specifically for DERs.



The Distributed Energy Resource Cybersecurity Framework (DER-CF) was developed to help federal agencies mitigate gaps in their cybersecurity posture for distributed energy systems.

Energy Exchange

Assessing Three Key Areas for Cybersecurity

Governance

Technical Management

Physical Security

Cyber Governance Security Assessment

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

Cyber-Physical Technical Management Security Assessment

Domains

- Account Management
  - Authentication, authorization, and accounting
  - Role-based access control
  - Remote access
  - Monitoring and logging
- Configuration Management
  - Change management
  - Access control
  - System settings
  - Cloud security
- Systems/Device Management
  - Software integrity
  - Cryptography
  - System protections

Physical Security Assessment

Domains

- Administration Controls
  - Audits
  - Awareness training
  - System security testing
  - Operational management
  - Security plan
  - Secure data
- Physical Access Controls
  - Perimeter security
  - Building security
  - Lighting
  - Signage
  - Intrusion alarm/motion detector
- Technical Controls
  - Intrusion Detection/prevention assets
  - Smart card/keying/badges
  - Sensor system/proximity reader/radio-frequency identification
  - Communication system
  - Closed-circuit television

DER-CF Tool: Overview

- Publicly available interactive version of the DER-CF framework
- User-focused assessment
- Detailed results and action items
- Userbase: site operations, energy managers, executive managers
- Tailored assessment to individual site

Unique from Any Other Assessment Tool

The DER-CF tool expands to DERs, specifically:

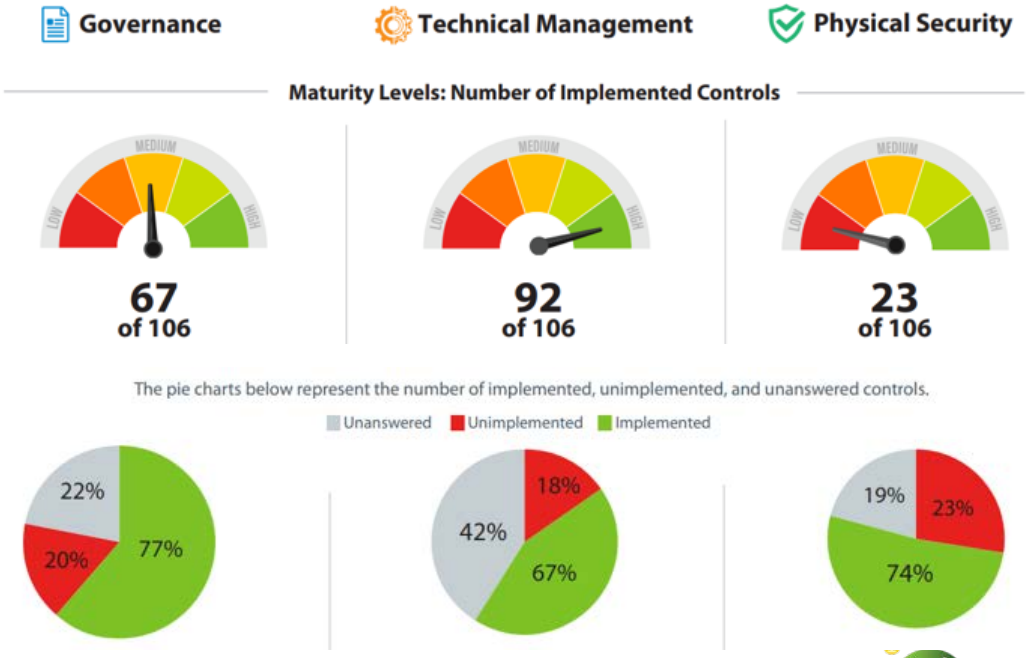
- Solar PV
- Wind
- Electric vehicles (charging stations)
- Buildings
- Energy Storage

The DER-CF uses the following standards and/or frameworks:

- DOE Cyber Security Capability Maturity Model (C2M2)
- NIST 800-53, 800-30,800-82, CSF
- DHS Cyber Assessments of ICS
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- International Electrotechnical Commission (IEC) 62351
- Executive Order 13800

Other Unique Features

- Dynamic content-driven approach
- Internal-facing application to aid researchers based on user behavior
- User experience focused application, encourages re-use
- Data secured to meet FIPS-199 medium standards



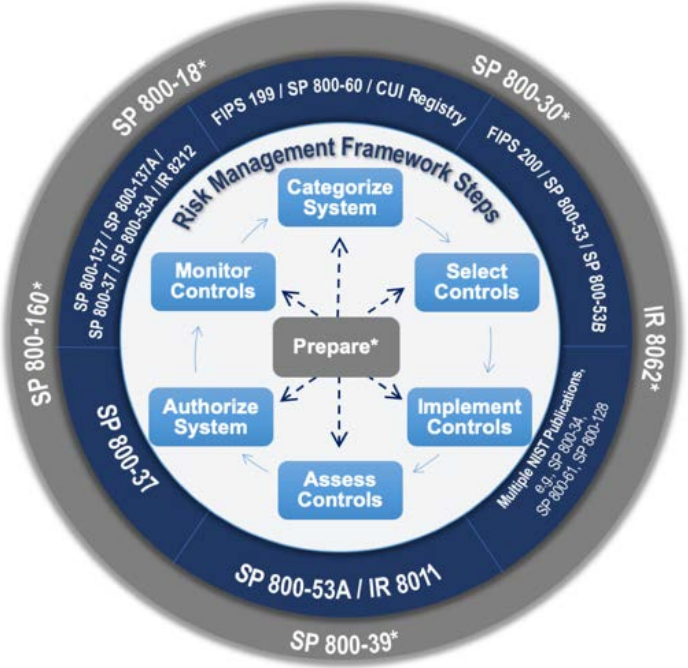
Integration with NREL's Cyber-Energy Emulation Platform (CEEP)

The CEEP is a new, innovative way to research and analyze energy systems and can replicate a federal site through data visualization. Combined with the integration of data from the DER-CF, CEEP can help merge the two complex cybersecurity topics of policy and technology by providing an integrated way to interact with cybersecurity logs and alerts.

The Distributed Energy Resource Risk Manager (DER-RM)

The DER Risk Manager

- NREL extended the scope of the DER-CF to include the NIST Risk Management Framework (RMF), addressing the challenges faced by federal energy managers when complying with the NIST RMF for DER systems.
- The NIST RMF is a cyclical process designed to incorporate principles of security and risk management into an organization's system policies and procedures.
- As an additional tool, NREL's **DER Risk Manager (DER-RM)** is independent of the DER-CF's self-assessment and allows users to focus on the RMF process.

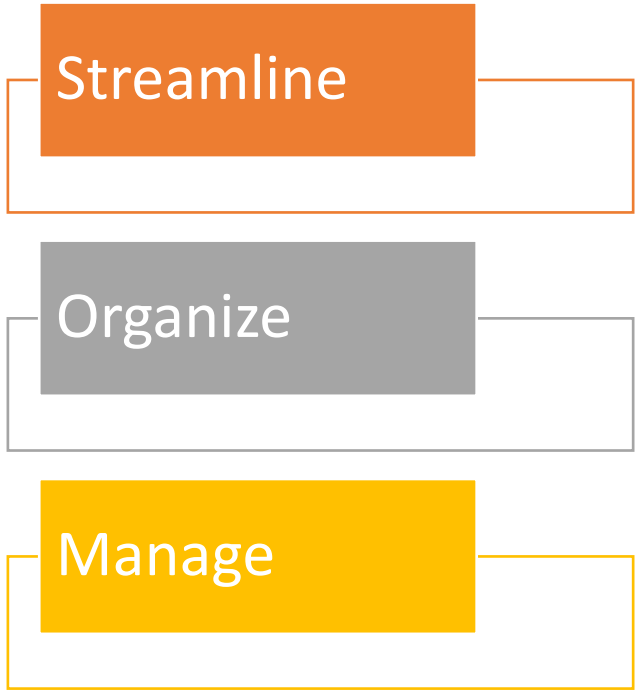


DER-RM

Energy Exchange

DER-RM Goals

- **Navigate compliance**
  Manage cybersecurity risk with government requirements in an organized manner
- **Automate requirements**
  Adapt to specific organization specific needs and present the most aligned templates and recommendations
- **Provide knowledge**
  Apply NIST guidance and DER-RM specific approaches
- **User-friendly interaction**
  Calculate risk score and generate system-specific requirements through real-world examples



Summary

Distributed Energy Resource Cybersecurity Framework (DER-CF)

- A holistic tool for evaluating cybersecurity posture of sites with DER systems.
- Offers a sharper focus on distributed energy technologies—and greater emphasis on physical security and technical management.
- The web-based tool converts simple user inputs to generate customized security control and practice recommendations that relate to their use of DERs. Results downloadable in a PDF report.

Distributed Energy Resource Risk Manager (DER-RM)

- Extends the DER-CF by applying it to the NIST RMF process.
- Will be downloadable application that runs locally and documents all the major requirements for achieving Authority to Operate the DER.

NREL/PR-5R00-80524

Thank You!

Tami.Reynolds@nrel.gov

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 in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.