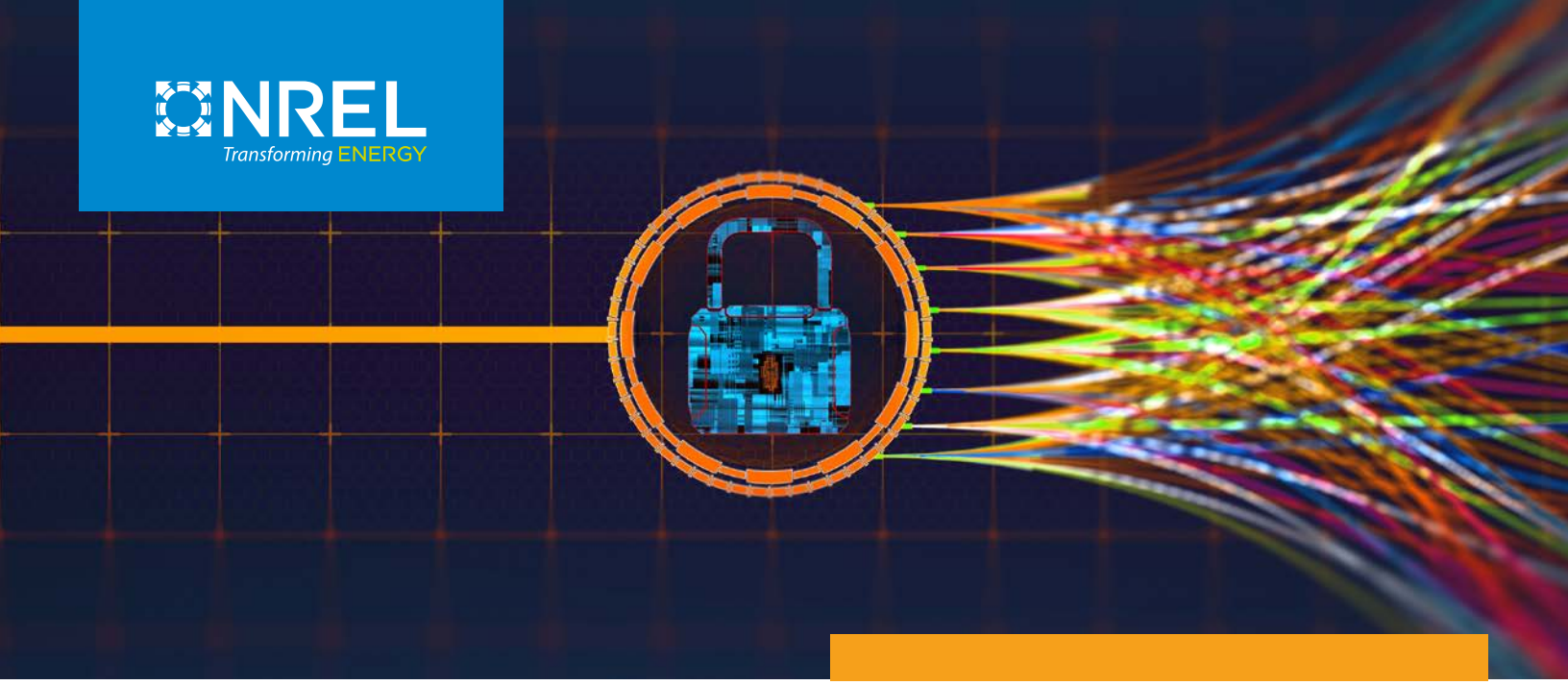
NREL
Transforming ENERGY



The Distributed Energy Resource Cybersecurity Framework

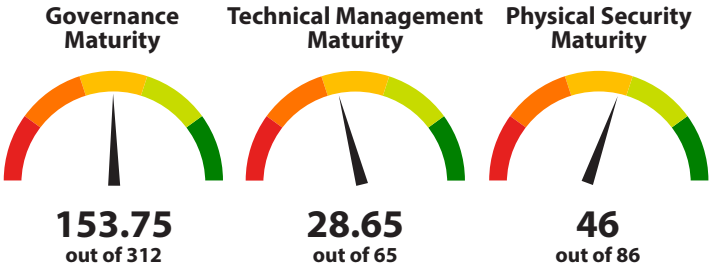
DER-CF

For facilities with distributed energy resources (DERs), cybersecurity must be considered holistically, across system architectures and down to individual components. It's hard to know where to start.

That's why the National Renewable Energy Laboratory (NREL) has developed an assessment tool for organizations with DERs to understand and improve their cybersecurity. With support from the U.S. Department of Energy's Federal Energy Management Program, the **Distributed Energy Resource Cybersecurity Framework (DER-CF)** provides a holistic evaluation of a facility's DER cybersecurity and makes customized recommendations that follow widely recognized best practices for cybersecurity. The DER-CF is available at no cost as an interactive web tool (dercf.nrel.gov).

Why We Need DER Cybersecurity

Compared to the traditional electric grid, which is powered by relatively few, centralized generation facilities, the modern grid is increasingly reliant on many decentralized generation sources. Such DER-heavy systems involve complex, data-driven communications, which can increase the number of access points outside a utility's administrative domain. Further, networked grid devices are now being controlled by consumers or third parties who might not be fully aware of the need for cybersecurity.



The DER-CF assesses a site's DER cybersecurity posture across three main pillars. This information is available to the user in an automated report that comprehensively evaluates facility risks.

How the DER-CF Works

The DER-CF guides users through a tailored questionnaire to get a complete picture of a site's cybersecurity. The questionnaire breaks cybersecurity into three pillars—governance, technical management, and physical security—ensuring that questions and action items are directed at the correct personnel. These pillars and their subdomains have unique cybersecurity importance that the DER-CF can help users work through. To track progress, users can return to their DER-CF profile and perform automated printouts of their cybersecurity report anytime.

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 – 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	• 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

Integration with the Cyber Range

The DER-CF is being integrated with NREL's cyber range, an advanced cyber-physical emulation environment that facilitates the real-time validation of cybersecurity strategies on replica energy system networks. Using information from a DER-CF assessment, the cyber range can emulate a site's connections, communications, and overall energy system. On the modeled system, NREL can simulate cyberattacks and validate organizational actions to improve site cybersecurity. Learn more about the cyber range: www.nrel.gov/security-resilience/cyber-range.html.

Guiding Frameworks

The DER-CF was founded on and expands the U.S. Department of Energy's existing Cybersecurity Capability Maturity Model (C2M2) and the National Institute of Standards Technology (NIST) Cybersecurity Framework (CSF), but it has a sharper focus on distributed energy technologies and increased emphasis on physical security and technical management. The DER-CF is the basis for another complementary tool, the DER Risk Manager (DER-RM), which closely adheres to the NIST Risk Management Framework 800-37 and allows users to focus on NIST compliance.

Learn More

Check out the tool and see how it could benefit your energy system: dercf.nrel.gov

Learn more about NREL's research in cybersecurity: www.nrel.gov/security-resilience/cybersecurity.html

Contact:

Tami.Reynolds@nrel.gov
Project Manager and Lead

NREL Transforming ENERGY

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

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

NREL/FS-5R00-82577 • May 2022