Risk Management for Distributed Energy Resources

Anuj Sanghvi
Cybersecurity Research Engineer

NREL at-a-Glance

2,926

Workforce, including

219 postdoctoral researchers

60 graduate students

81 undergraduate students

World-class

facilities, renowned technology experts

More than 900

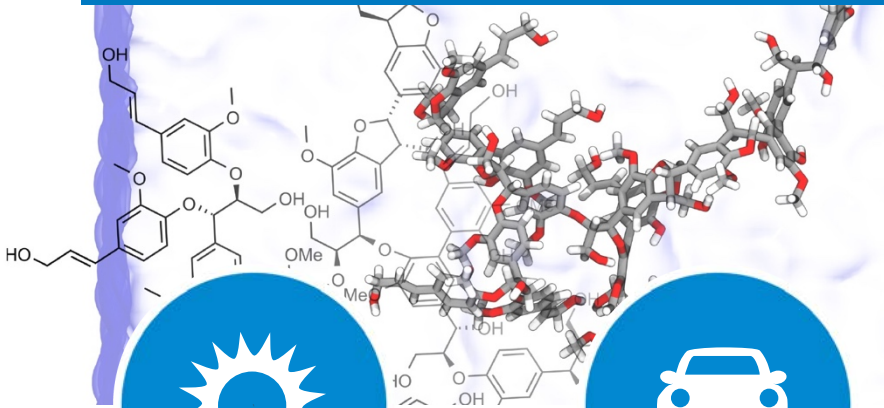
Partnerships

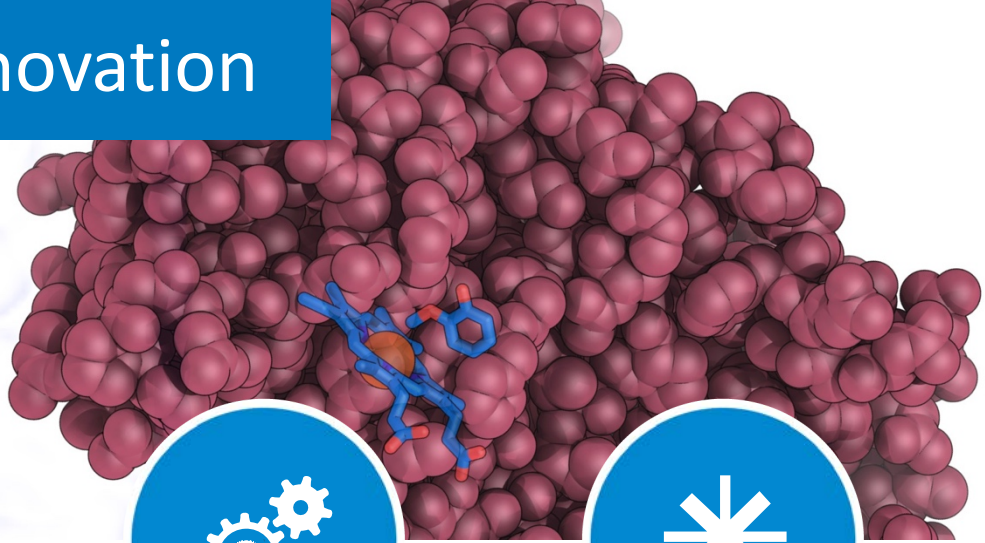
with industry, academia, and government

Campus

operates as a living laboratory

NREL Science Drives Innovation





Renewable Power

Solar

Wind

Water

Geothermal

Sustainable Transportation

Bioenergy

Vehicle Technologies

Hydrogen

Energy Efficiency

Buildings

Advanced Manufacturing

Government Energy Management

Energy Systems Integration

Grid Integration

Hybrid Systems

Security and Resilience

Trends Driving Change in Energy

Increasing Interdependencies

Energy Diversification

Vehicle Electrification

Grid-Connected Smart Buildings

Big Data, Artificial Intelligence, and Machine Learning

Cybersecurity

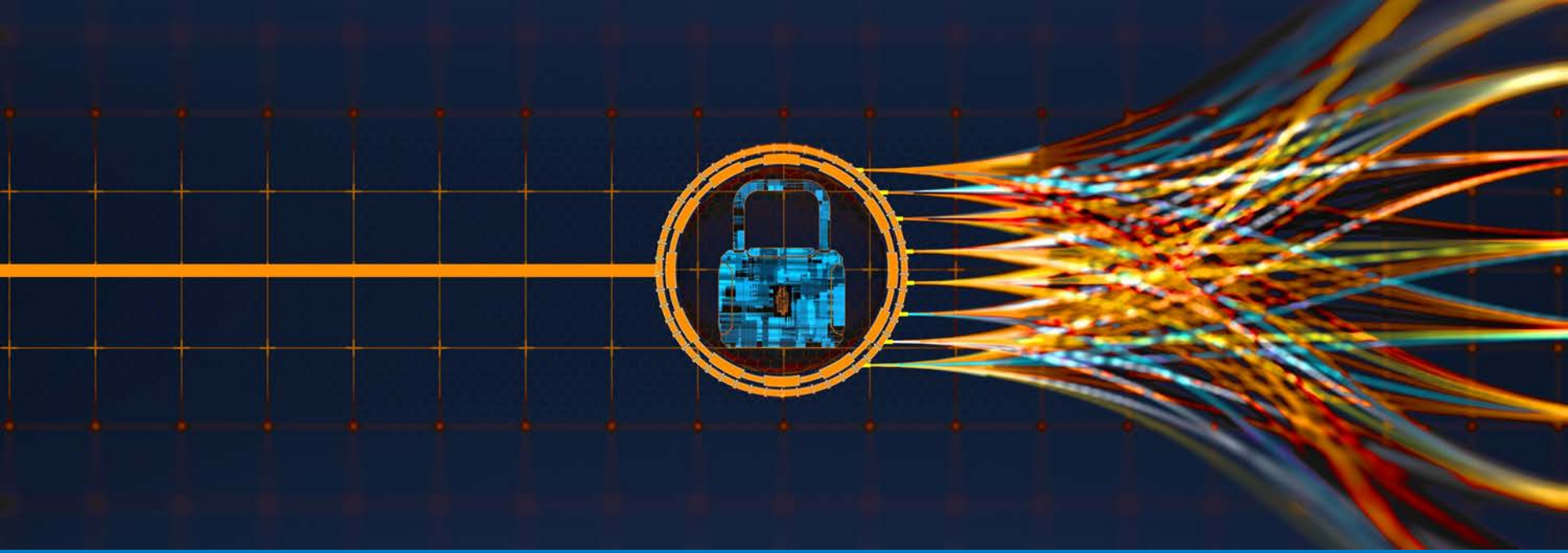
Resilience

Millions of Devices at the Grid Edge

Cybersecurity for Distributed Energy Resources

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

- DERs use multiple separate communications networks to connect with the energy grid.
- This 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 cyber vulnerabilities and limit utility visibility over the entire system.



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

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

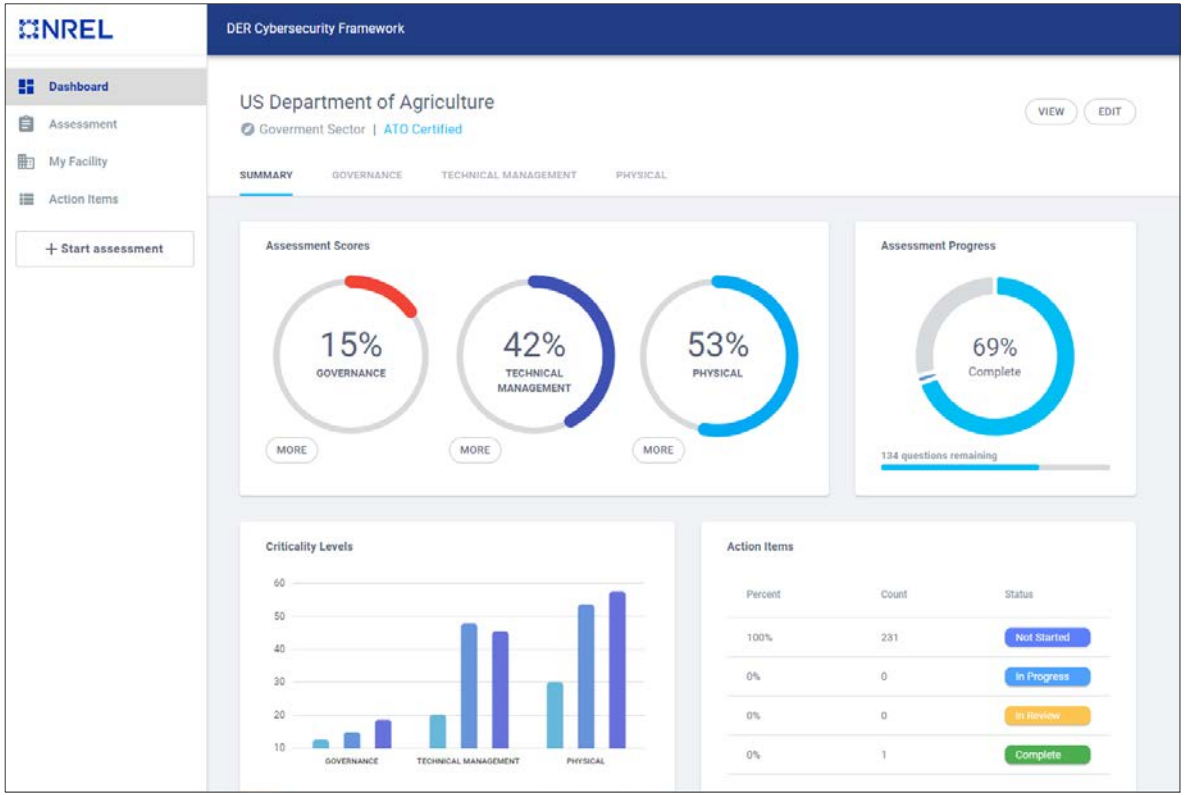
Physical Security Assessment

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

DERCF Tool: 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



The Distributed Energy Resources Risk Manager

- NREL extended the scope of the DERCF 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 **Distributed Energy Resources Risk Manager (DER-RM)** is independent of the DERCF's existing self-assessment and allows users to focus on the RMF process.

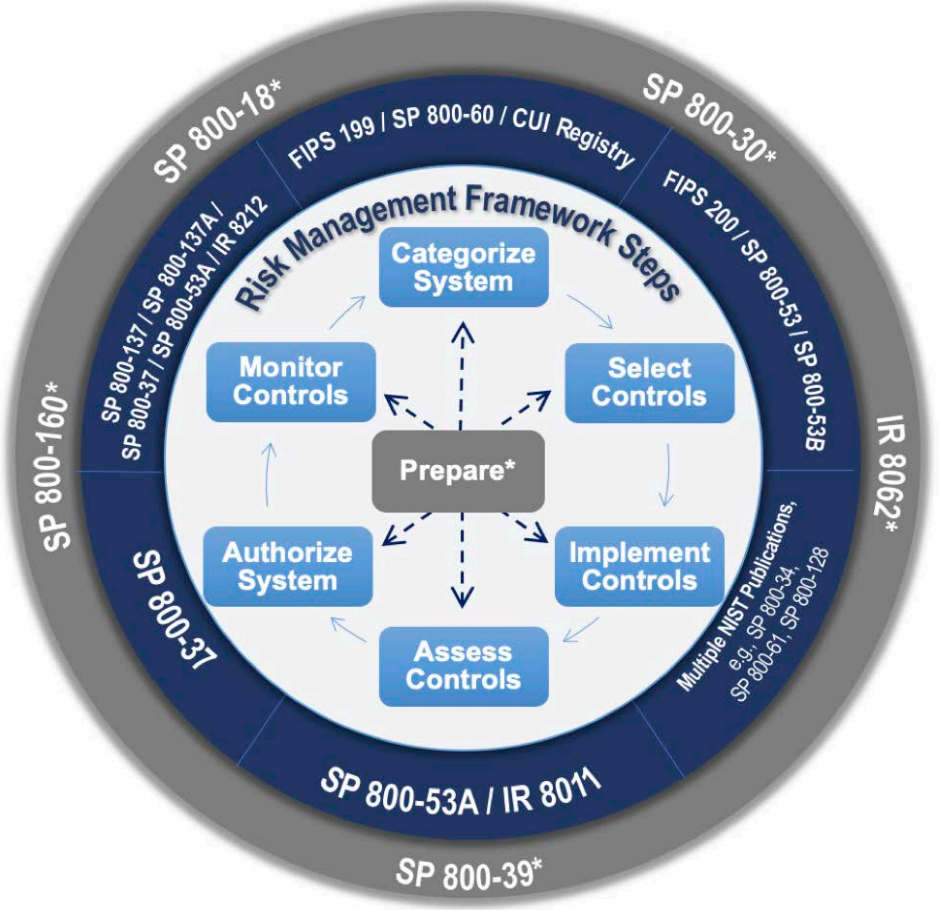


Illustration from NIST

DER-RM Goals

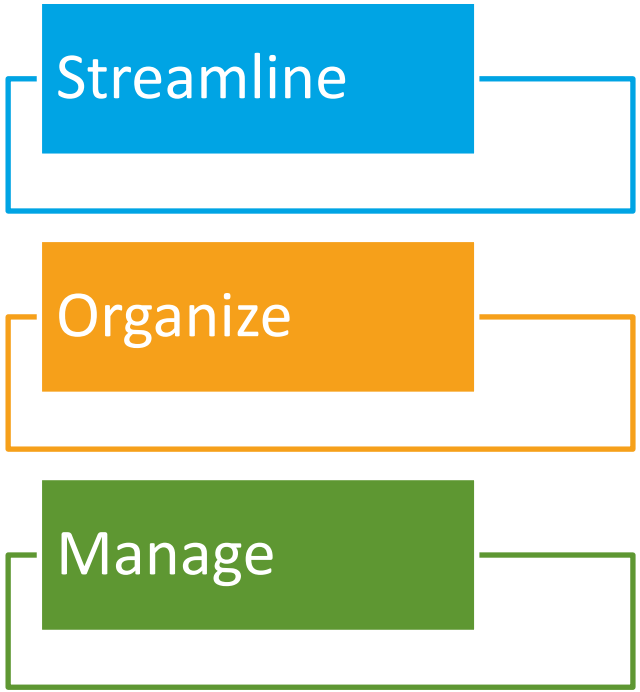
- **Navigate compliance**

  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 (DERCF)

- 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)

- Under development, extends the DERCF 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.

Q&A

www.nrel.gov

Contact:
Tami Reynolds – Tami.Reynolds@nrel.gov
Anuj Sanghvi – Anuj.Sanghvi@nrel.gov