

International Cybersecurity: Capabilities and Overview

Tami Reynolds
Group Manager
Cyber Risk Optimization

Energy Systems Across the Globe Are Changing



Photo from iStock 902601546

The National Renewable Energy Laboratory (NREL) is advancing the safety, reliability, security, and resilience of future energy systems.


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.



Photo from iStock 1181551812

- 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 cyberattacks.



Rapid increase in the quantity and diversity of connected devices.

Loss of exclusive **ownership** of utility operational technology and information technology systems necessary for grid monitoring and control.

Less tractable **supply chains** impact trust in edge devices and services.

Legacy and current solutions not prepared for technology and threat revolutions.

Photo from iStock 1181551837

Energy Transformation: Grand Challenges

With deep expertise in the design, integration, and operation of clean, highly distributed energy systems, NREL is equipped to address these challenges as the grid continues to evolve and become increasingly modern, autonomous, and complex.



Photo by Dennis Schroeder NREL 51927

NREL Technical Capabilities

To support the secure and resilient deployment of renewable energy assets and to address grid interconnection challenges, NREL’s Energy Security Team has developed a technical assistance plan to help partners achieve a rapid transition to energy decarbonization.

Risk Assessment Tools





DER-CF



Graphic by NREL

The Distributed Energy Resource Cybersecurity Framework (DER-CF) helps organizations mitigate gaps in their cybersecurity posture for distributed energy systems.

Assessing Three Key Areas for Cybersecurity



Governance



Technical Management



Physical Security

The DER Risk Manager

- NREL extended the scope of its existing risk management tools to include the National Institute of Standards and Technology (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** is independent of the DER-CF's existing self-assessment and allows users to focus on the RMF process.

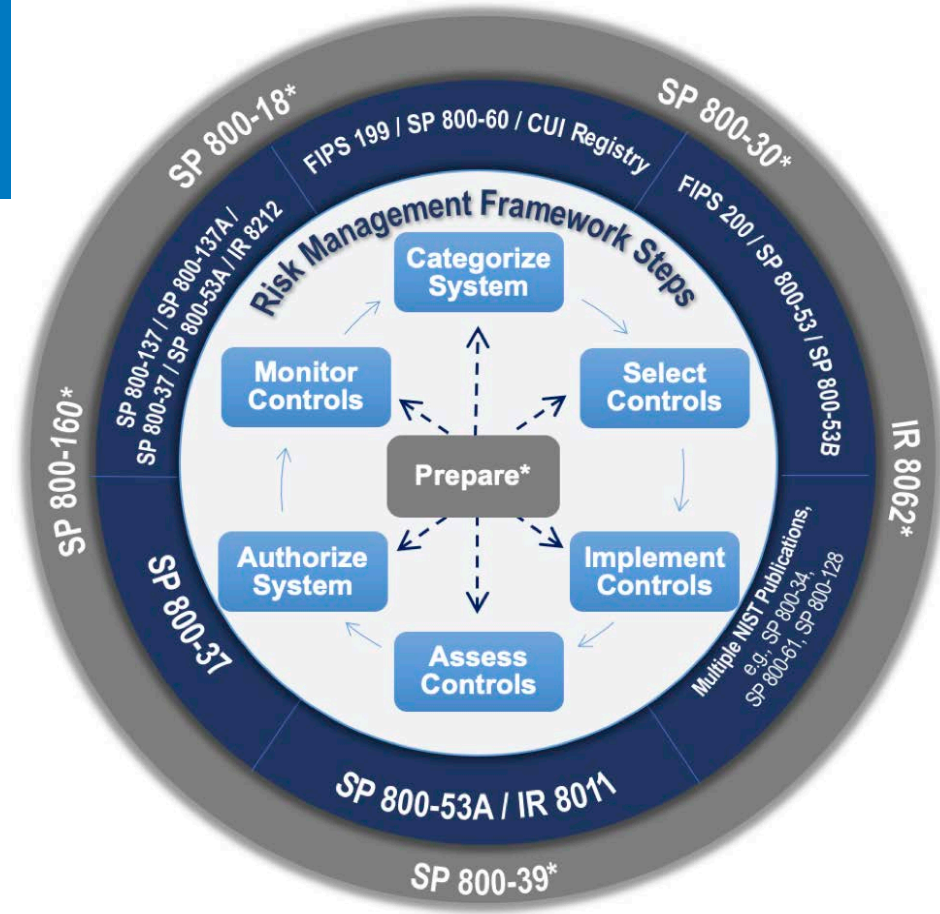


Illustration from NIST

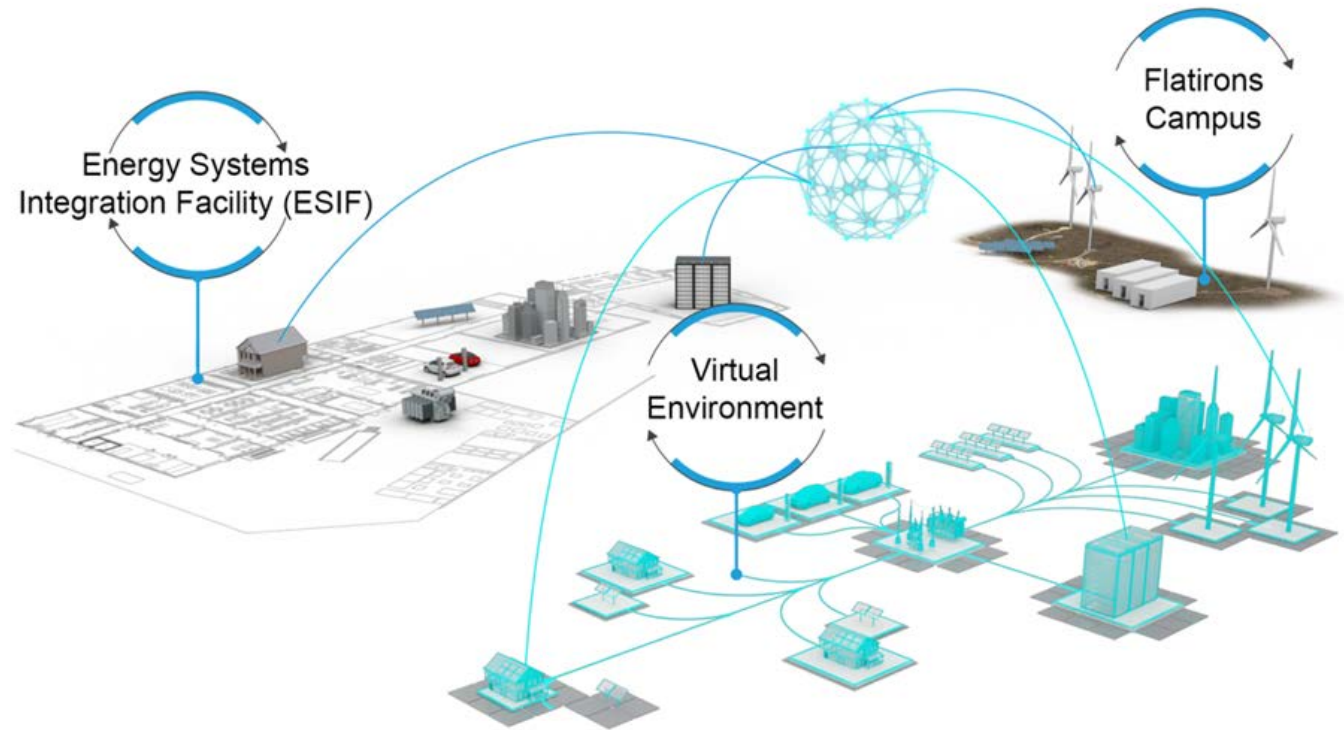


Photo by Dennis Schroeder NREL 55315

Integration With NREL's ARIES Cyber Range

NREL's Advanced Research on Integrated Energy Systems (ARIES) Cyber Range provides an innovative way to research and analyze energy systems and can replicate an energy site through data visualization. Combined with the integration of data from the DER-CF, the cyber range can help merge the two complex cybersecurity topics of policy and technology by providing an integrated method to interact with cybersecurity logs and alerts.

The ARIES Cyber Range is a broadly capable hybrid private cloud resource that integrates telecommunication networks and physical energy systems.



Graphic by NREL

With hardware-, controller-, and human-in-the-loop integration, the ARIES Cyber Range creates a realistic, interactive dynamic environment and provides visualizations of the **digital and physical systems for real-time awareness, historical analysis, and future planning and operation.**

NREL ARIES Cyber Range Testing and Validation

NREL's ARIES Cyber Range offers testing and validation of energy systems used to educate users on a broad range of cybersecurity threats.

With the help of NREL researchers, organizations can:

- Use NREL's ARIES Cyber Range to test and validate their security controls
- Enable technical implementation changes that improve the security, efficiency, and reliability of an organization's core mission
- Improve organizational decision-making on procurement and third-party risk.



Photo from iStock 1312253155

Cyber Range Use Case

NREL is currently working with a U.S. federal agency to test and validate the security and resilience of its advanced metering infrastructure. These efforts will:

- Evaluate the advanced metering infrastructure systems against attack scenarios like denial-of-service, adversary-in-the-middle, etc.
- Identify security risks that need immediate mitigation and illuminate gaps within their security architecture
- Boost the overall cybersecurity posture of the organization's operational technology network.



Photo from iStock 1157131951

The Cyber Range

Helps Us by...



**Hosting
Cosimulations**



**Orchestrating
and Automating**



**Emulating
Communication**



**Facilitating
Hardware-in-the-
Loop Studies**



**Visualizing
Results**

Cybersecurity Technical Assistance



Our Comprehensive Technical Assistance Addresses the Full Spectrum of Cybersecurity Risk Planning and Management

Expertise



Photo by Werner Slocum NREL 67843

- ✓ Modeling and data visualization
- ✓ Renewable energy technologies, including buildings and mobility
- ✓ Distributed energy systems and microgrids
- ✓ Cybersecurity and supply chain disruptions
- ✓ Stakeholder convening.

Partners



Photo by Werner Slocum NREL 78586

- ✓ Federal agencies
- ✓ Federal, state, local governments, and tribes
- ✓ Private industry
- ✓ Emergency managers
- ✓ International governments
- ✓ Community leaders and nongovernmental organizations.

Services and Solutions



Image from iStock 926497376

- ✓ Cybersecurity strategy assistance and support
- ✓ Cyber risk assessment tools
- ✓ Identification and mitigation of cybersecurity risks
- ✓ Incident preparation and response
- ✓ Capacity building and technical trainings.

International Energy Security Highlights



NREL Works With Over 80 Countries

Around the World on Advanced Energy Solutions



Research and
Development



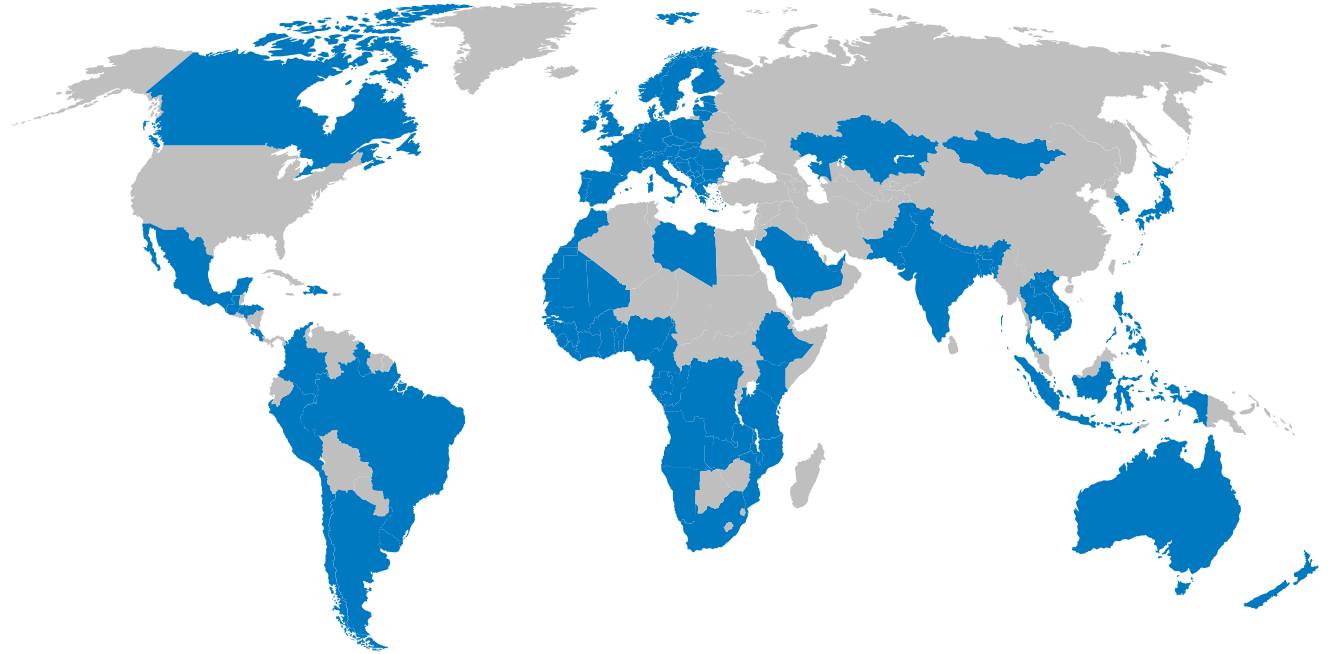
Energy Systems
Performance



Data-Driven Decision-
Making and Planning



Regional
Integration



Global Technical Toolkits developed with the U.S. Agency for International Development (USAID) provide free, state-of-the-art support on common and critical challenges to scaling up advanced energy systems.





Photo from iStock 950739780

NREL's Impact in the Caribbean

Risk assessment results serve as the basis for prioritizing organizational cybersecurity efforts and defining key areas on which to focus follow-on technical assistance efforts.

NREL's technical assistance offerings provide holistic support for developing, implementing, and monitoring an organization's cybersecurity strategy.

Partners: Caribbean Electric Utility Services Corporation, Deloitte

Sponsor: USAID

Power Sector Cybersecurity Building Blocks

Developed through the enduring USAID-NREL partnership, NREL researchers developed a framework called the **Power Sector Cybersecurity Building Blocks**.

The Building Blocks are clusters of related activities that support a well-rounded cyber program and encourage utilities to think about different areas of cybersecurity.

The Building Blocks bring together a variety of applicable cybersecurity guides, standards, and frameworks into **one user-friendly resource to help international stakeholders prioritize cybersecurity efforts and investments**.



Read the full report at:
<https://resilient-energy.org/cyber>

Resilient Energy Platform

Developed through the USAID-NREL Partnership, the Resilient Energy Platform provides **expertly curated resources, training materials, tools, and technical assistance** to enhance power sector resilience.

The Platform enables decision makers to **assess power sector vulnerabilities, identify resilience solutions, and make informed decisions** to enhance power sector resilience at all scales.



Developed through the USAID-NREL Partnership, the Resilient Energy Platform provides expertly curated resources, training materials, data, tools, and direct technical assistance in planning resilient, sustainable, and secure power systems.

www.resilient-energy.org



Photo by Werner Slocum NREL 63001

NREL's Impact

Risk assessment results serve as the basis for prioritizing organizational cybersecurity efforts and defining key areas on which to focus follow-on technical assistance efforts.

NREL's technical assistance offerings provide holistic support for developing, implementing, and monitoring an organization's cybersecurity strategy.

NREL's Unique Capabilities



**NREL Risk
Assessment Tools**



ARIES Cyber Range



**Cybersecurity
Technical Training**



**Cybersecurity Strategy
Development**



Incident Response

Thank you!

NREL/PR-5R00-87604

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. 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.

