CARILEC Resilient Energy Community CoP for Cybersecurity Workshop
Series: Cybersecurity Assessment Tools

June 27, 2024
Introductory Remarks
John Garrison, U.S. Agency for International Development (USAID)
Senior Energy and Climate Change Advisor
Environment and Energy Team
Office of Regional Sustainable Development
Latin America and the Caribbean Bureau
Martyn Forde, Caribbean Electric Utility Services Corporation
Strategic Consultant
CARILEC Resilient Energy Community
Laura Leddy, National Renewable Energy Laboratory (NREL)

Researcher

Energy Security and Resilience Center
The USAID-NREL Partnership

NREL partners with USAID to deliver clean, reliable, and affordable power in the developing world. Together, we help countries with policy, planning, and deployment support for advanced energy technologies.

The USAID-NREL Partnership’s global technical platforms provide free, state-of-the-art support on common and critical challenges to scaling up advanced energy systems:

https://www.nrel.gov/usaid-partnership/

To learn about additional resources, sign up for the quarterly USAID-NREL Partnership Newsletter:
https://www.nrel.gov/usaid-partnership/newsletter.html
Resilient Energy Platform

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

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

https://resilient-energy.org/
Cybersecurity Building Blocks

• Support a well-rounded cyber program by suggesting clusters of related activities

• Encourage utilities to think about different areas of cybersecurity

• Draw from established best practices

• Span multiple stakeholders

• Interconnected and mutually supporting

• These building blocks are not the last word.

Read the full report at: https://resilient-energy.org/cybersecurity-resilience
Building Blocks Structure

- Governance
- Organizational Security Policy
- Compliance
- Laws, Regulations, and Standards
- Cyberthreat Intelligence
- Risk Management
- Procurement
- Technical Controls
- Incident Response
- Cybersecurity Awareness Training
- Workforce Development
- Workforce Development
Overview of NREL’s Distributed Energy Resource Cybersecurity Framework (DER-CF) Tool

---

Tami Reynolds, NREL
Group Manager, Cyber Risk Optimization Group
Introducing the DER-CF Tool

The **DER-CF** helps organizations mitigate gaps in their cybersecurity posture for distributed energy systems.

**Resources:**
- [DER-CF website](#)
- [DER-CF fact sheet](#)
- [Guide to the DER-CF](#)
Assessing Three Key Areas for Cybersecurity

Governance  Technical Management  Physical Security
<table>
<thead>
<tr>
<th>Cyber Governance Security Assessment</th>
<th>Cyber-Physical Technical Management Security Assessment</th>
<th>Physical Security Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains:</td>
<td>Domains:</td>
<td>Domains:</td>
</tr>
<tr>
<td>• Risk Management</td>
<td>• Account Management</td>
<td>• Administration Controls</td>
</tr>
<tr>
<td>• Asset, Change, and Configuration</td>
<td>• Role-based access control</td>
<td>Audits</td>
</tr>
<tr>
<td>• Identity and Access Management</td>
<td>• Anomalous behavior in system logs</td>
<td>Holistic security/contingency</td>
</tr>
<tr>
<td>• Threat and Vulnerability</td>
<td>• Configuration Management</td>
<td>planning</td>
</tr>
<tr>
<td>Management</td>
<td>• Access restrictions</td>
<td>Personnel security planning</td>
</tr>
<tr>
<td>• Situational Awareness</td>
<td>• Configuration settings</td>
<td></td>
</tr>
<tr>
<td>• Information Sharing and</td>
<td>• Configuration change control</td>
<td></td>
</tr>
<tr>
<td>Communication Management</td>
<td>• Internal/external user management</td>
<td></td>
</tr>
<tr>
<td>• Incident Response</td>
<td>• Systems/Device Management</td>
<td></td>
</tr>
<tr>
<td>• External Dependency Management</td>
<td>• Fail-safe procedures</td>
<td></td>
</tr>
<tr>
<td>• Cybersecurity Program</td>
<td>• Ports and input/output device access</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>• Cryptographic protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Software integrity/patch management</td>
<td></td>
</tr>
</tbody>
</table>
Unique From Other Assessment Tools

The tool expands to distributed energy resources, specifically:

- Solar
- Wind
- Electric vehicles (charging stations)
- Buildings
- Storage.

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

- The U.S. Department of Energy’s Cyber Security Capability Maturity Model
- National Institute of Standards and Technology: 800-53, 800-30, 800-82, Cybersecurity Framework
- U.S. Department of Homeland Security cyber assessments of industrial control systems
- North American Electric Reliability Corporation Critical Infrastructure Protection security standards
- International Electrotechnical Commission 62351
- U.S. Executive Order 13800.
DER-CF Tool: Overview

- Publicly available interactive version of the DER-CF framework
- Hosted by NREL at www.dercf.nrel.gov
- User-focused assessment
- Detailed results and action items
- Userbase: site operations, energy managers, executive managers
- Tailor assessment to individual site.
DER-CF Tool: Unique Features

- Dynamic, content-driven approach
- Updated as research evolves
- Internal-facing application to help researchers based on user behavior
- User experience-focused application, which encourages reuse
- Data secured to meet FIPS-199 medium standards.

Test results from the DER-CF cybersecurity assessment tool. Review the framework at: https://dercf.nrel.gov.
DER-CF Summary

- The DER-CF is a holistic tool for evaluating the cybersecurity posture of sites, especially those with distributed energy resource systems.

- Networked grid devices are now being controlled by consumers or third parties, who are not always fully aware of the need for cybersecurity.

- The DER-CF offers a sharper focus on distributed energy technologies—and greater emphasis on physical security and technical management.

- Users will access DER-CF-guided assessments through a web-based application or a downloadable document, which presents users with questions about security controls and practices that relate to their use of information technology and operational technology assets and domains.

- The DER-CF web application tool will generate a score from the user’s responses that indicates their current cybersecurity posture—and how they can improve.
NREL’s Comprehensive Technical Assistance Addresses the Full Spectrum of Cybersecurity Risk Planning and Management

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

**Partners**
- U.S. federal agencies
- U.S. state and local governments and Tribes
- Private industry
- Emergency managers
- International governments
- Community leaders and nongovernmental organizations.

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

Image from iStock | 926497376
Photo by Werner Slocum | NREL 67843
Photo by Werner Slocum | NREL 78586
Image from iStock | 926497376
Cybersecurity Assessment Tools:
Discussion and Audience Q&A
USAID and NREL Resources


Access additional resources and information by visiting the *Cybersecurity Resilience Resources page* on the Resilient Energy Platform website.

Start exploring the DER-CF tool by visiting: [https://dercf.nrel.gov/](https://dercf.nrel.gov/)

Contact Us:
- Laura.Leddy@nrel.gov
- Tami.Reynolds@nrel.gov
- Steve.Granda@nrel.gov
Appendix: Cybersecurity Assessment Types and Publicly Available Tools
Types of Cybersecurity Assessments

Network Security Assessment
• Assessment Purpose: Analyze and secure network architecture
• Potential Tools: Nmap, Wireshark, Snort, Zeek, Suricata.

System and Application Security Assessment
• Assessment Purpose: Evaluate systems and applications
• Potential Tools: OpenVAS.

Endpoint and Device Security Assessments
• Assessment Purpose: Evaluate individual devices and endpoints
• Potential Tools: CVE-bin-tool, Yara, Virus Total.

Incident Detection and Response
• Assessment Purpose: Detect and respond to security incidents
• Potential Tools: Security Onion.

Threat Intelligence
• Assessment Purpose: Proactively gather and analyze threat data to manage organizational threats
• Potential Tools: MISP.

Policy and Compliance
• Assessment Purpose: Ensure adherence to regulatory requirements and internal policies
• Potential Tools: CISA CSET, NIST OpenSCAP.