USAID FROM THE AMERICAN PEOPLE NREL Transforming ENERGY CARILEC An Association Of Electric Energy Solution Providers CAREC CARILEC Resilient Energy Community pacc2030 U.S.-Caribbean Partnership to Address the Climate Crisis 2030

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

June 27, 2024

IMAGE FROM ISTOCK | 673891964

# 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:

REexplorer MAPPING OUR ENERGY FUTURE | Greening the Grid | I-JEDI | Resilient Energy Platform

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

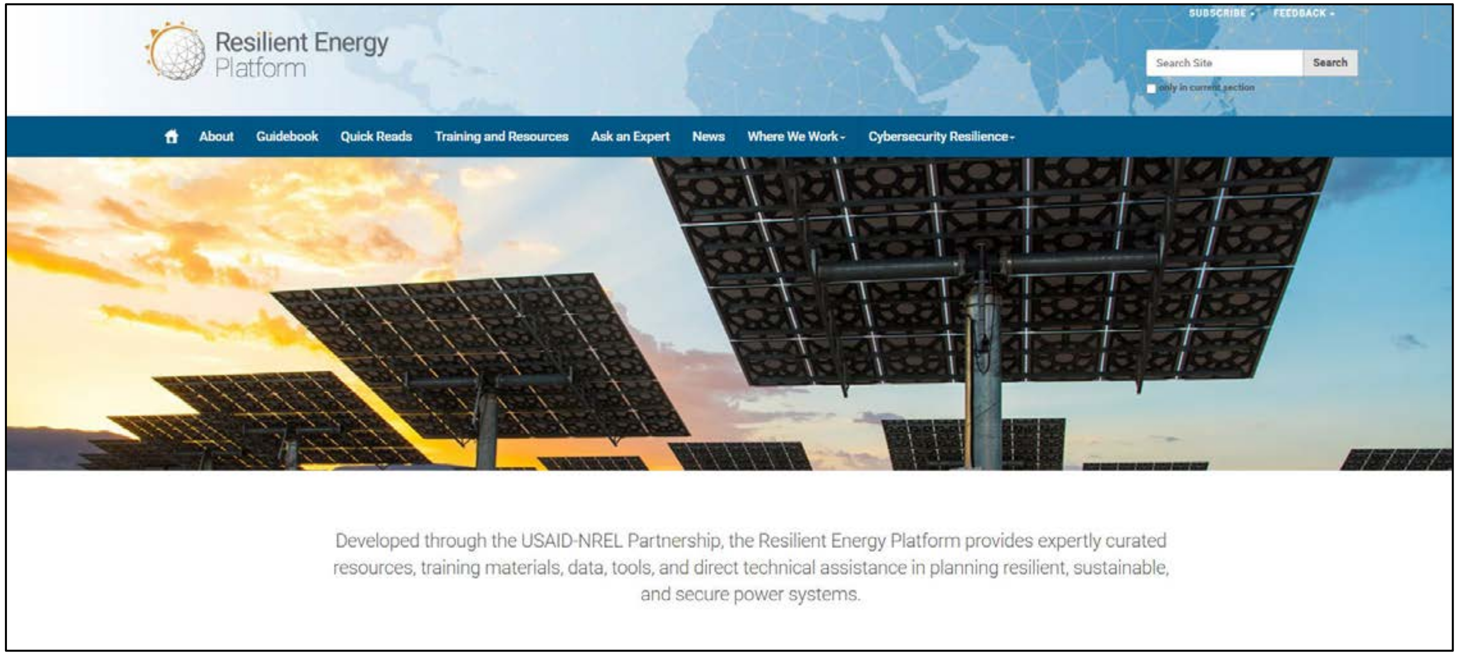
USAID FROM THE AMERICAN PEOPLE | NREL Transforming ENERGY | CARILEC An Association Of Electric Energy Solution Providers | CAREC CARILEC Resilient Energy Community | pacc2030 U.S.-Caribbean Partnership to Address the Climate Crisis 2030

# Resilient Energy Platform

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.



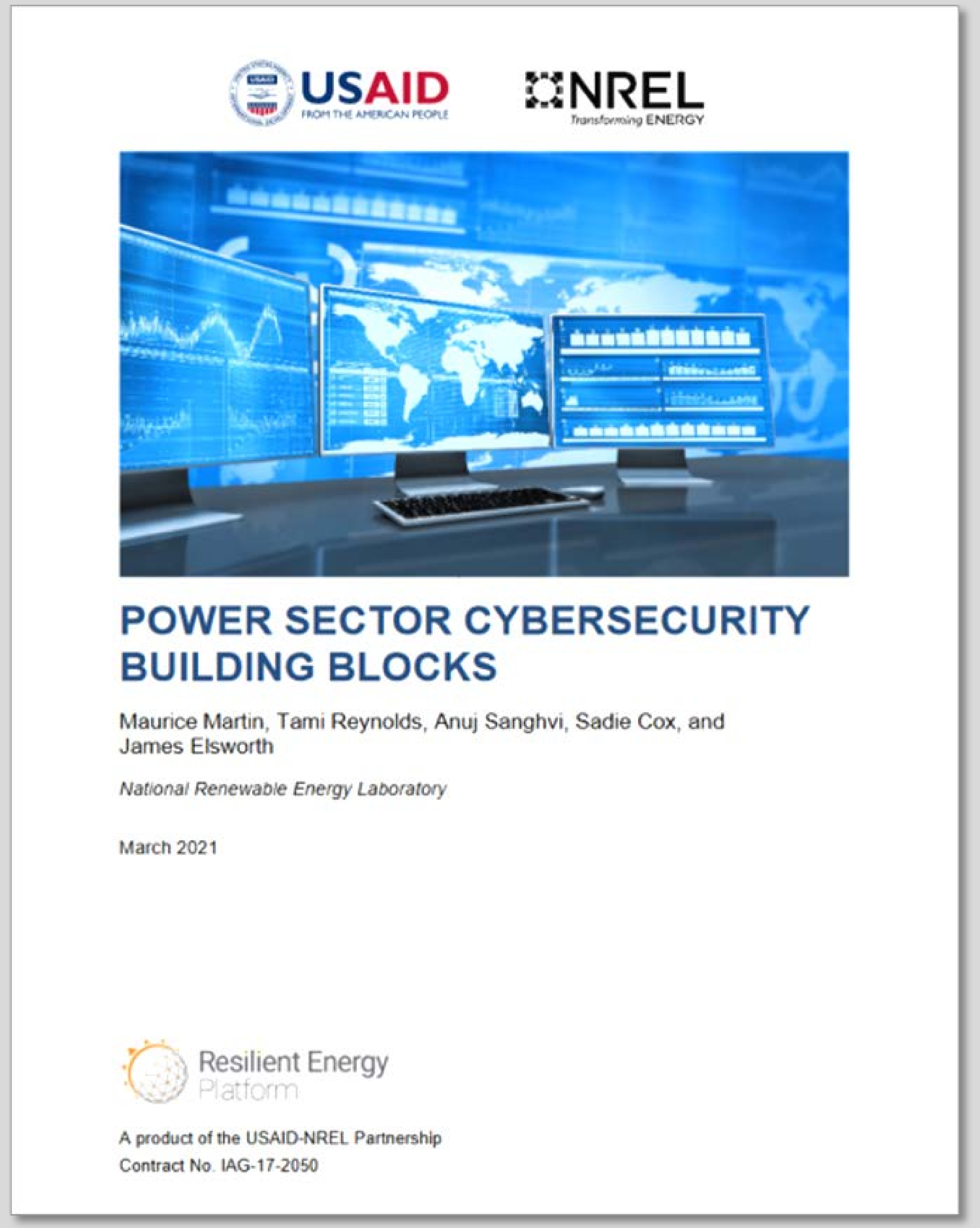
Developed through the USAID-NREL Partnership, the Resilient Energy Platform provides expertly curated resources, training materials, data, tools, and direct technical assistance in planning resilient, sustainable, and secure power systems.

https://resilient-energy.org/

USAID FROM THE AMERICAN PEOPLE
NREL Transforming ENERGY
CARILEC An Association Of Electric Energy Solution Providers
CAREC CARILEC Resilient Energy Community
pacc2030 U.S.-Caribbean Partnership to Address the Climate Crisis 2030

# 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.



POWER SECTOR CYBERSECURITY BUILDING BLOCKS

Maurice Martin, Tami Reynolds, Anuj Sanghvi, Sadie Cox, and James Elsworth

*National Renewable Energy Laboratory*

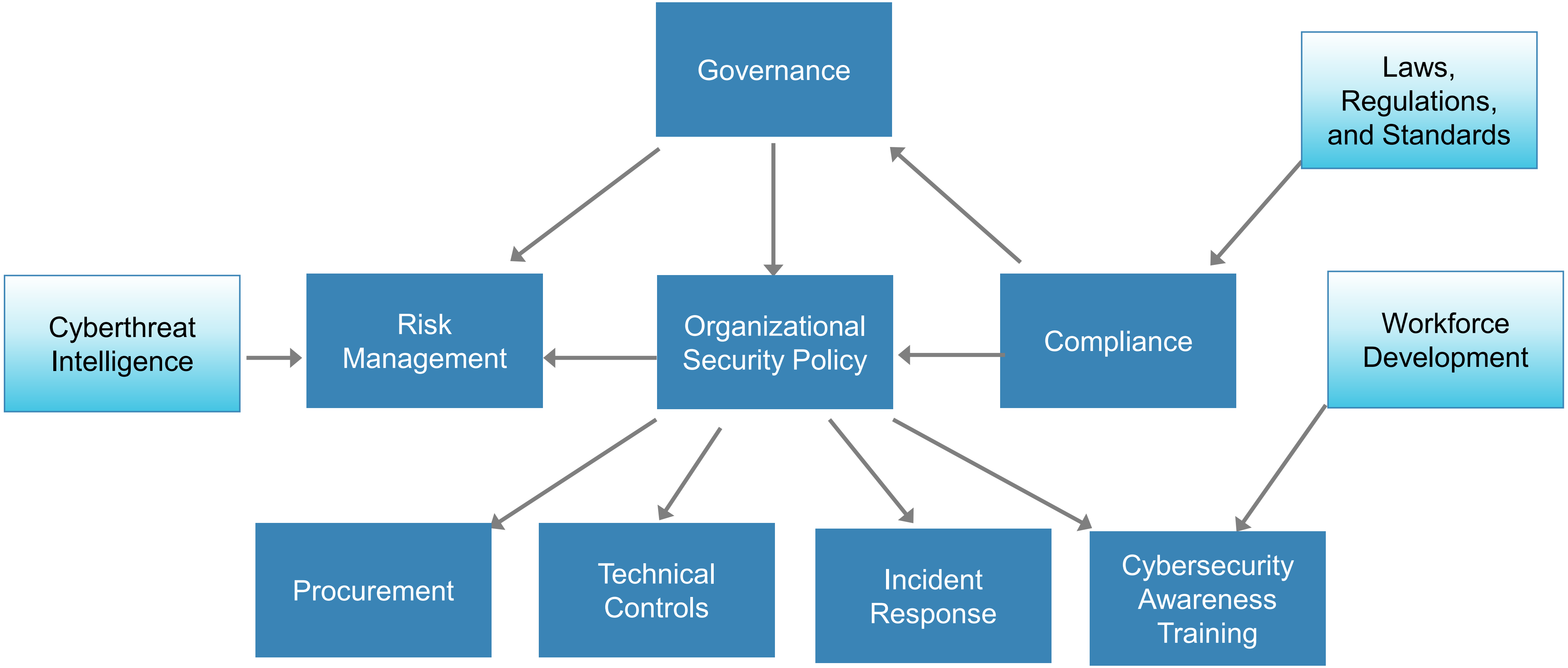
March 2021

Resilient Energy Platform

A product of the USAID-NREL Partnership
Contract No. IAG-17-2050

**Read the full report at:**
https://resilient-energy.org/cybersecurity-resilience

# Building Blocks Structure

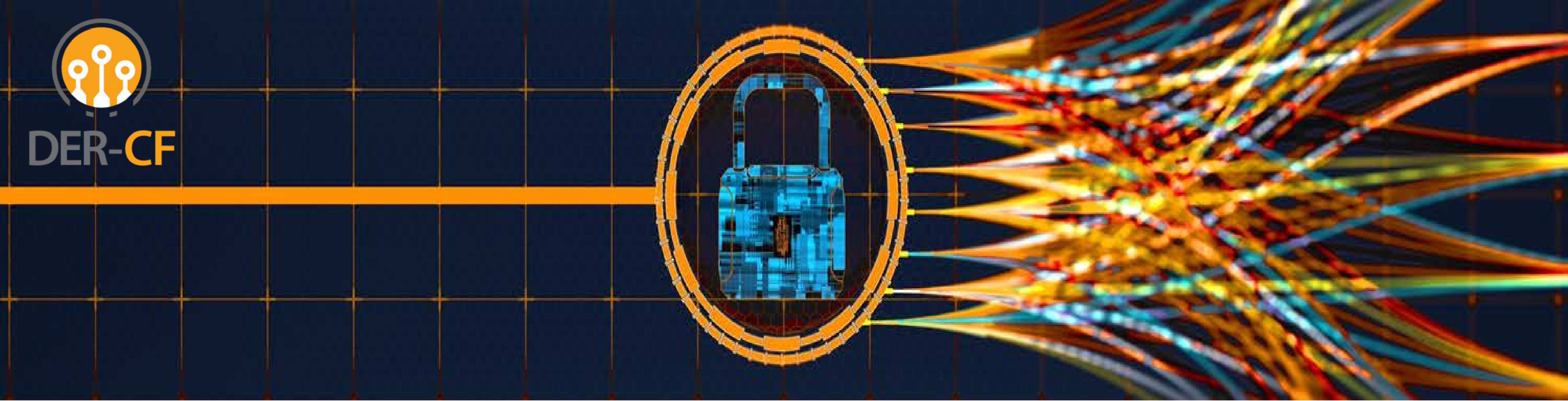


# Overview of NREL’s Distributed Energy Resource Cybersecurity Framework (DER-CF) Tool

---

Tami Reynolds, NREL

Group Manager, Cyber Risk Optimization Group


Graphic by NREL

# 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.

USAID FROM THE AMERICAN PEOPLE · NREL Transforming ENERGY · CARILEC · CAREC CARILEC Resilient Energy Community · pacc2030 U.S.-Caribbean Partnership to Address the Climate Crisis 2030

# 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
  - *Role-based access control*
  - *Anomalous behavior in system logs*
- Configuration Management
  - *Access restrictions*
  - *Configuration settings*
  - *Configuration change control*
  - *Internal/external user management*
- Systems/Device Management
  - *Fail-safe procedures*
  - *Ports and input/output device access*
  - *Cryptographic protection*
  - *Software integrity/patch management*

## Physical Security Assessment

Domains:

- Administration Controls
  - *Audits*
  - *Holistic security/contingency planning*
  - *Personnel security planning*
- Asset Controls
  - *Equipment*
  - *Maintenance*
- Structure Controls
  - *Distancing practices for sensitive assets*
  - *Intrusion detection/prevention assets*
  - *Response teams/force protection*

USAID FROM THE AMERICAN PEOPLE
NREL Transforming ENERGY
CARILEC An Association Of Electric Energy Solution Providers
CAREC CARILEC Resilient Energy Community
pacc2030 U.S.-Caribbean Partnership to Address the Climate Crisis 2030

# Unique From Other Assessment Tools

## The tool expands to distributed energy resources, specifically:

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

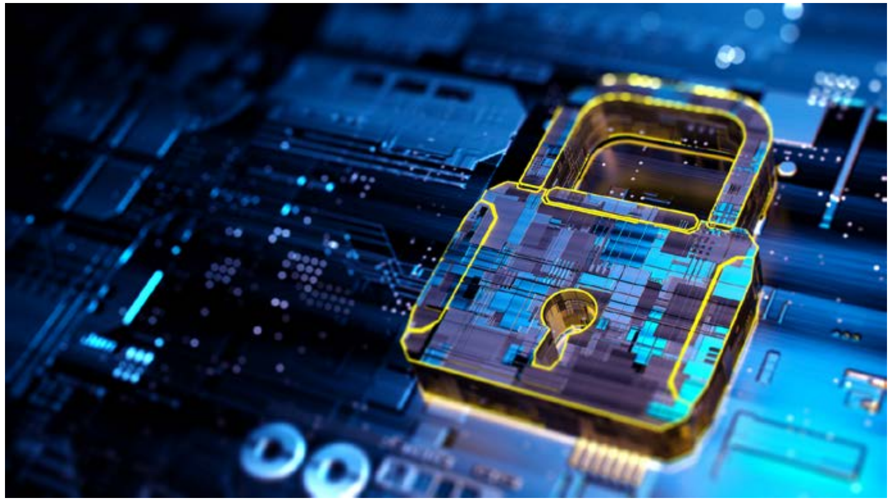
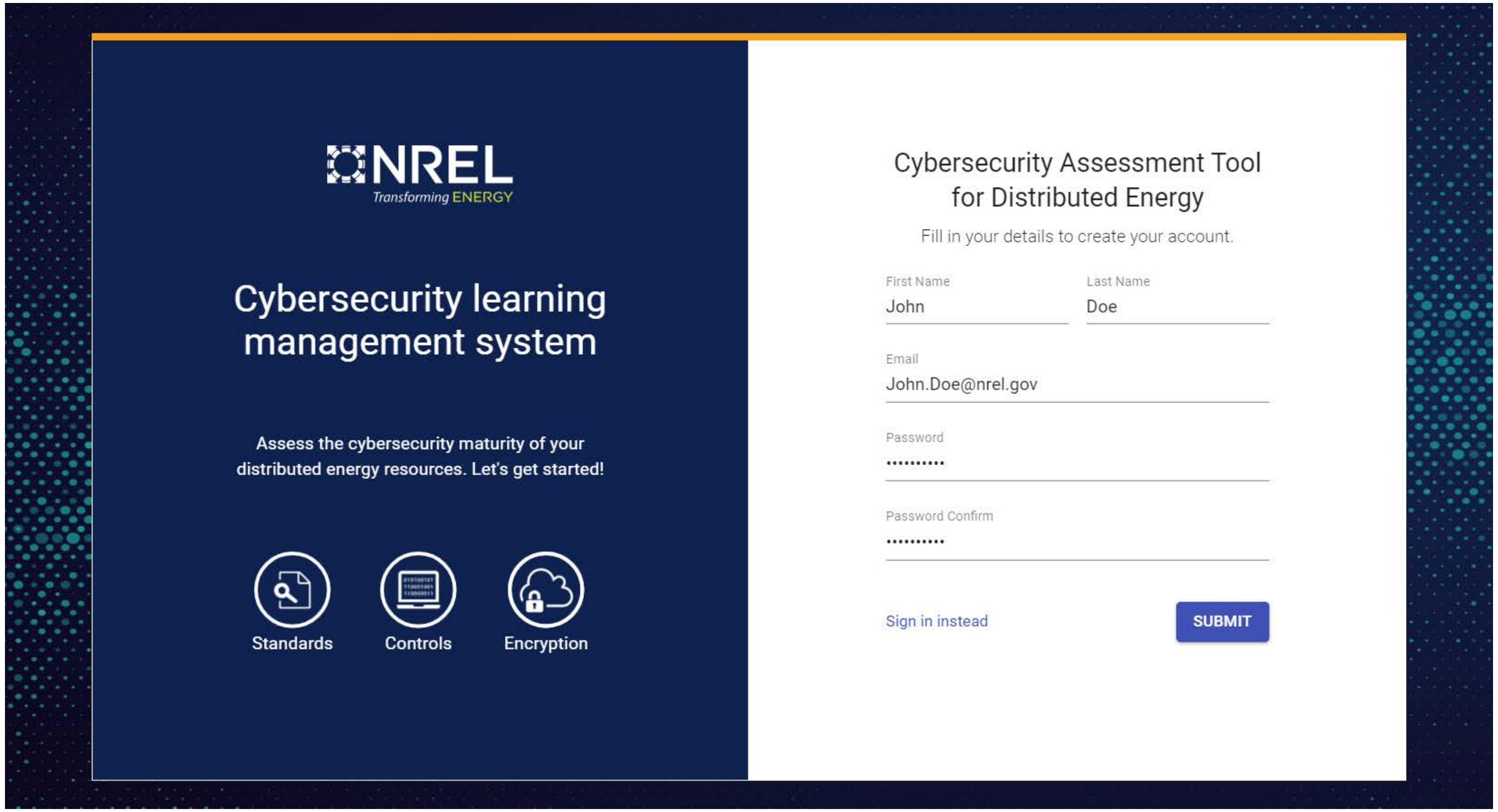


IMAGE FROM ISTOCK | 468171529

## 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



Cybersecurity learning management system

Assess the cybersecurity maturity of your distributed energy resources. Let's get started!

Cybersecurity Assessment Tool for Distributed Energy

Fill in your details to create your account.

First Name: John

Last Name: Doe

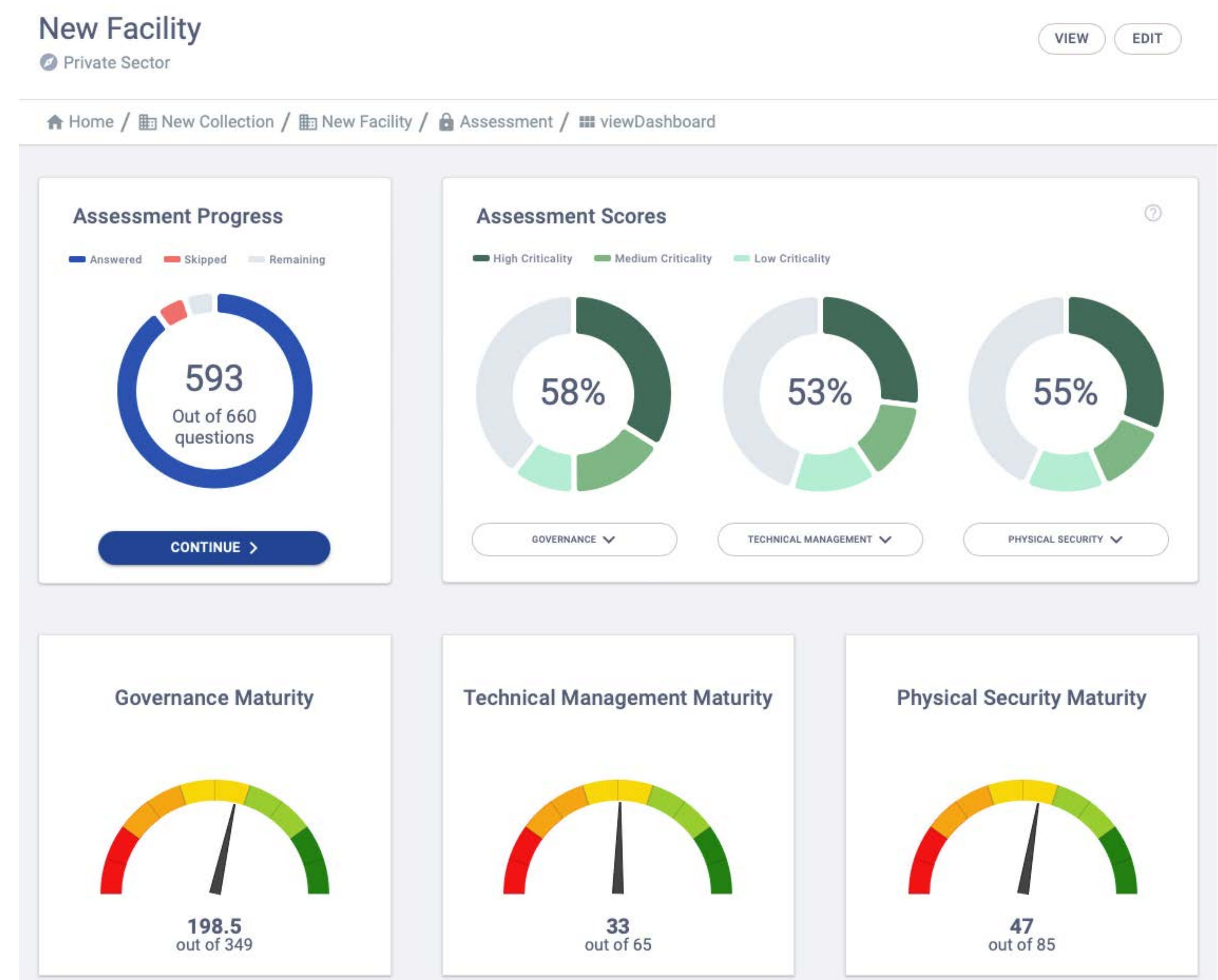
Email: John.Doe@nrel.gov

Password: ••••••••••

Password Confirm: ••••••••••

- 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



New Facility

Private Sector

Home / New Collection / New Facility / Assessment / viewDashboard

Assessment Progress

Answered · Skipped · Remaining

593 Out of 660 questions

Assessment Scores

58% · 53% · 55%

Governance Maturity: 198.5 out of 349

Technical Management Maturity: 33 out of 65

Physical Security Maturity: 47 out of 85

- 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.

USAID FROM THE AMERICAN PEOPLE · NREL Transforming ENERGY · CARILEC · CAREC CARILEC Resilient Energy Community · pacc2030 U.S.-Caribbean Partnership to Address the Climate Crisis 2030

# 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

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

- ✓ 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

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.

USAID FROM THE AMERICAN PEOPLE — NREL Transforming ENERGY — CARILEC An Association Of Electric Energy Solution Providers — CAREC CARILEC Resilient Energy Community — pacc2030 U.S.-Caribbean Partnership to Address the Climate Crisis 2030

# Cybersecurity Assessment Tools: Discussion and Audience Q&A

# USAID and NREL Resources

**Read the guidance document:** ***Power Sector Cybersecurity Building Blocks*** report available at: https://resilient-energy.org/cybersecurity-resilience

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/

**Contact Us:**

- Laura.Leddy@nrel.gov
- Tami.Reynolds@nrel.gov
- Steve.Granda@nrel.gov

USAID FROM THE AMERICAN PEOPLE | NREL Transforming ENERGY | CARILEC An Association Of Electric Energy Solution Providers | CAREC CARILEC Resilient Energy Community | pacc2030 U.S.-Caribbean Partnership to Address the Climate Crisis 2030

# Thank You!

This work was authored, in part, by the National Renewable Energy Laboratory (NREL), 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 United States Agency for International Development (USAID) under Contract No. IAG-22-22434. The views expressed in this report do not necessarily represent the views of the DOE or the U.S. Government, or any agency thereof, including USAID. 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.

NREL/PR-5T00-90390

# 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.