Assessment and Coordination of DER Cybersecurity Standards

Principal Investigator: Danish Saleem, National Renewable Energy Laboratory (NREL)

Team Members: Chelsea Neely (NREL), Emily Waligoske (NREL), Kazunori Nagasawa (NREL), Megan Culler (INL), Jordan Waggoner (INL), Chris Lamb (SNL), Jenna deCastro (SNL)

Presented on: 09/12/2024

Project Overview

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Outcomes

- DER cyber standards gap analysis
- DER cyber maturity baseline report
- DER cyber standards library
- DER cyber testing methodology
- DER cyber standards advisory group
- Harmonization of cyber requirements and certification programs for DERs

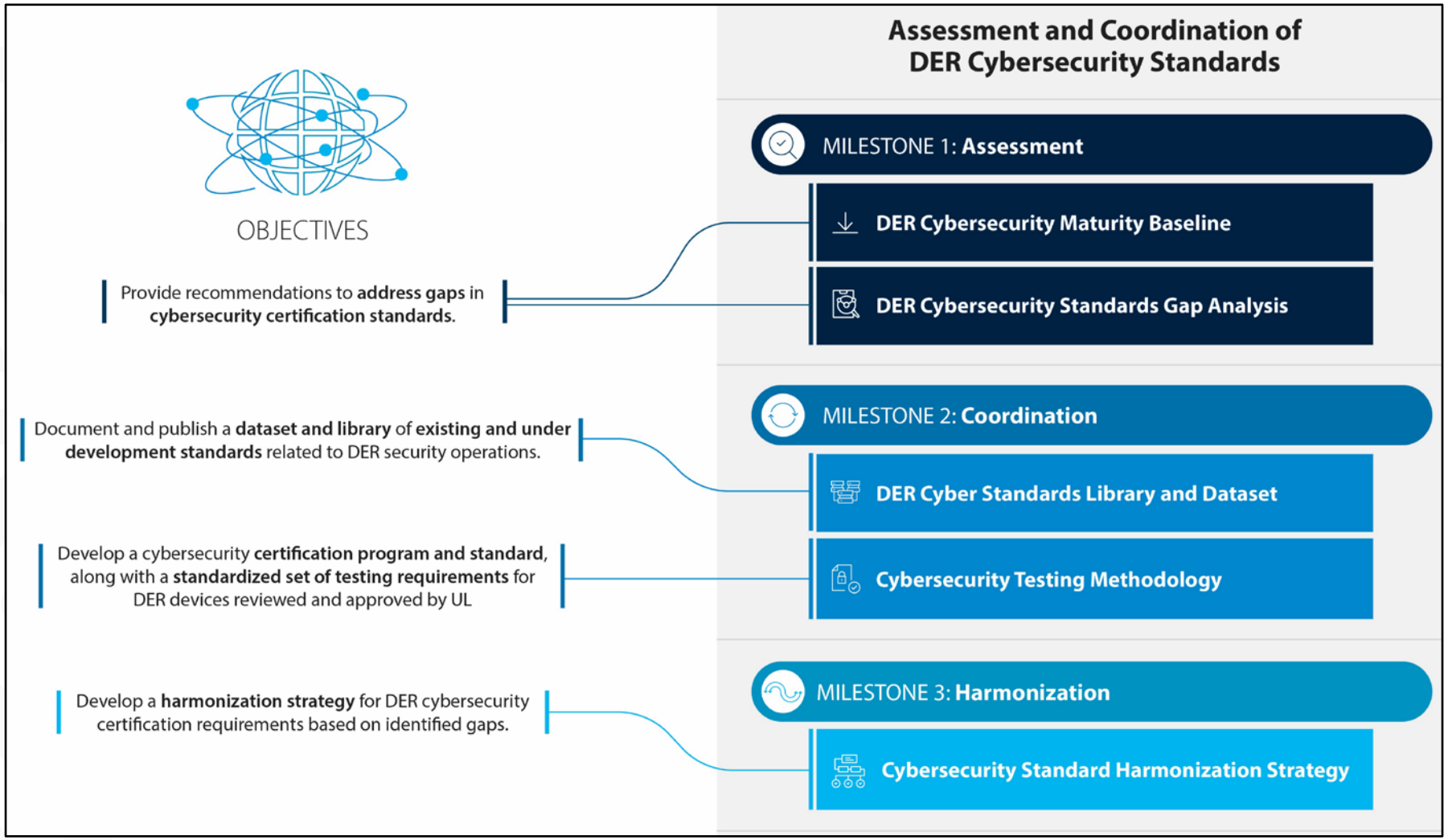
Key Partners

Idaho National Laboratory

Sandia National Laboratories

UL Solutions

solaredge



Defining a DER

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

What is a distributed energy resource (DER)?

- Energy resource at the distribution level **connected at 20 MW and under**:
  - The types of assets included in this project, but are not limited to, DERs for energy storage, distributed solar, distributed wind, hydrogen fuel cells, building loads, etc.
  - The work in this project also require understanding of supporting technology infrastructure such as demand response, DERMS, and microgrids.
  - Current focus of GMI 2.2 project is wind, solar, storage, hydrogen, and building loads
  - Controllable thermostats, demand response, etc., can be added to the next project cycle

- Informed by DER definitions from:
  - NERC, FERC, IEEE 1547-2018, DOE's *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid*, and project 2.2 proposal.

DER Standards Library

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Cybersecurity

- IEEE 1547.3
- UL 2941
- NIST SP 800-82
- IEEE P2658
- ISO/SAE 21434

Interconnection

- IEEE 1547
- IEEE P2800
- IEC TR 62351
- CA Rule 21
- Hawaii Electric Rule 14H

Communication

- IEC 61850
- IEEE 1815 (DNP3)
- Modbus
- IEEE 2030.5
- REST
- Open ADR

Safety

- UL 1741
- UL 9540
- IEC 62109-1
- IEEE 2030.2

Data Dictionary

- The data dictionary provides uniform identifying information about each standard in the library.
- Categories were chosen based on relevancy to the user of the library and are meant to add value to the library:
  - Governing body
  - Standard
  - Title
  - Working group
  - Family
  - Obligation to comply
  - Current revision
  - Standard type
  - Geographic scope
  - Functional scope
  - Applicability to DER type
  - Intended organizations
  - Related or referenced standards
  - NIST CSF functions
  - Encryption type
  - Device authentication
  - Key exchange algorithms
  - Accessibility
  - User cost
  - Source/link.

Sample of Database

	Governing Body	Standard	Title	Working Group	Family	Obligation to Comply	Current Revisio
2	IEC	IEC 62351	Power systems management and associated information exchange - Data and communications security	IEC TC57 WG15, cybersecurity standards for power system communications	62351	Voluntary	variable based on subsect
3	IEC/IEEE	IEC 62270/IEEE 1249	Guide for computer-based control for hydroelectric power plant automation	Energy Development and Power Generation Committee of the IEEE Power & Energy Society	N/A	Voluntary	2013
4	ISA/IEC	ISA/IEC 62443	Security of Industrial Automation and Control Systems	ISA99 committee	62443	Voluntary	variable based on subsection
5	IEEE	IEEE 1686™-2022	Standard for Intelligent Electronic Devices Cybersecurity Capabilities	Power System Communications and Cybersecurity Committee S1 Working Group, IEEE Power and Energy Society	N/A	Voluntary	2022

Sample of Database

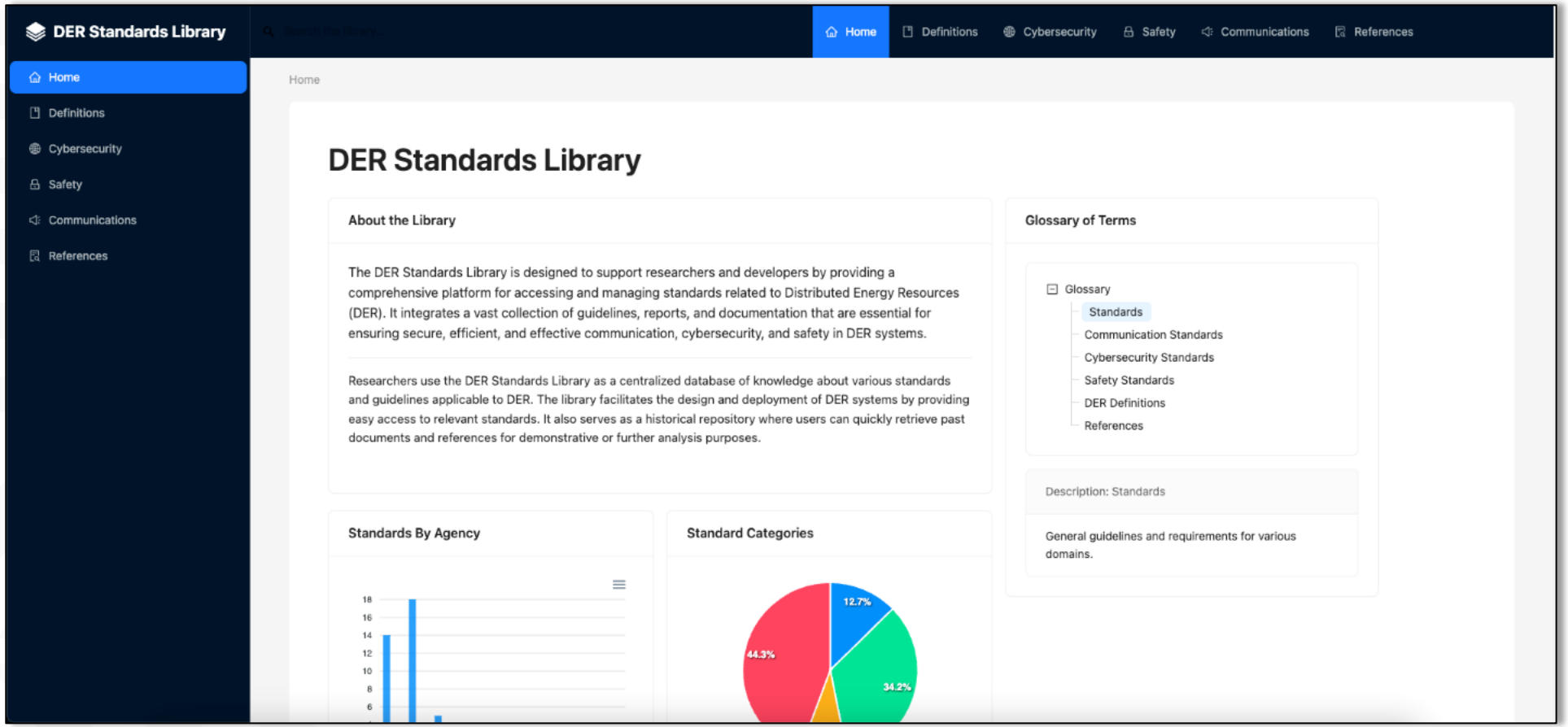
	L	M	N	T	U
1	**Applicability to DER Type**	**Intended Organizations**	**Related or Referenced Standards**	**Govern**	**Identify**
2	agnostic to specific DERs	Asset Owners and Operators, Original Equipment Manufacturers, Third-Party Suppliers, Systems Integrators, OT Services Providers, Cybersecurity Services Providers	IEC 60870-5 series (including IEEE 1815 (DNP3) as a derivative standard), the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. there is not a one-to-one correlation between the IEC TC57 communication protocol standards and the IEC 62351 security standards. This is because many of the communication protocols rely on the same underlying cybersecurity standards at different layers.		
3	hyroelectric plants	Asset Owners and Operators, Systems Integrators			
	agnostic to specific DERs, a 'horizontal' standard, supposed to apply across a broad range of industries, including electric sector all industry sectors that use IACS, including building automation, electric power generation and distribution, transportation, etc.	Asset Owners and Operators, Original Equipment Manufacturers, Third-Party Suppliers, Systems Integrators	ISO/IEC 27000 series; EU cybersecurity c	Part 1-3: System security conformance metrics; Part 2-1: Establishing an IACS security program; Part 2-2: IACS security program ratings; Part 2-3: Patch management in the IACS environment; Part 2-4: Security program	Part 1-4: IACS security lifecycle and use cases; Part 3-1: Security technologies

Web Interface (Beta)

GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

Features under development:

- Look-up
- Keyword search
- Sorting by
- Group by NIST functions
- Compare
- Visualize
- Version history



Proposed Approach for Cybersecurity Standards Harmonization

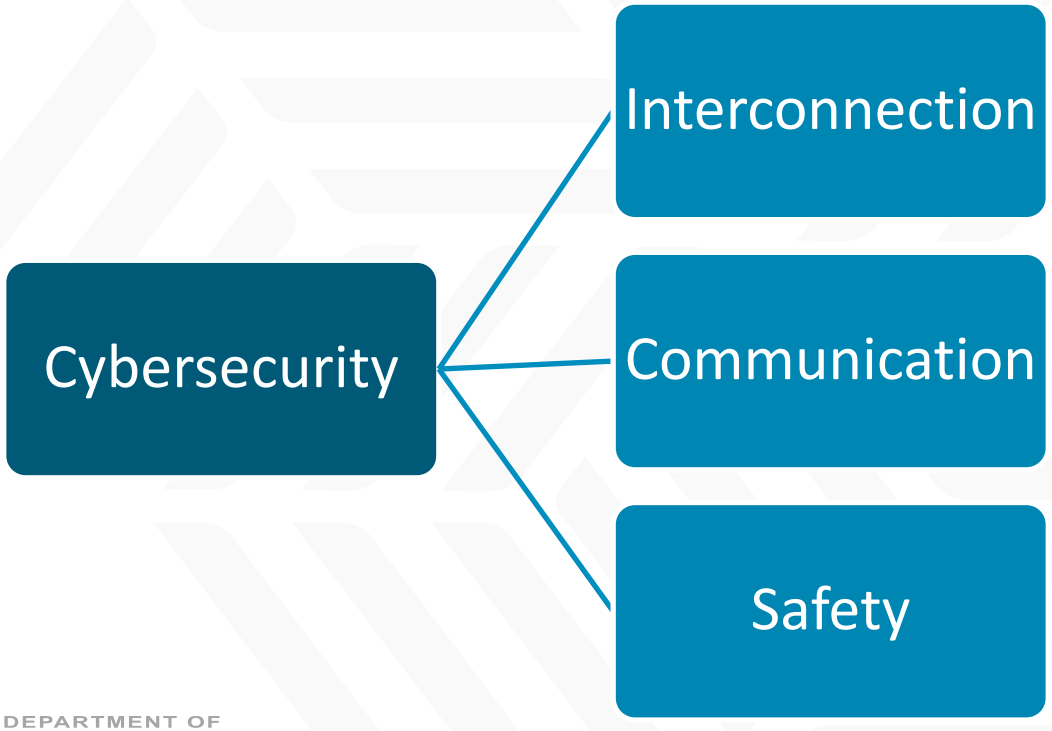
GRID MODERNIZATION INITIATIVE
U.S. Department of Energy

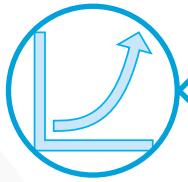
- **What** is harmonization?
  - The adoption of a consistent set of technical requirements that minimize redundant or conflicting standards that may have evolved independently.
    - Through this project, national labs intend to support harmonization for DER cybersecurity standards.

- **Why** harmonization?
  - Conflicting and divergent technical standards make it difficult to implement a cohesive DER cybersecurity policy
  - Diverse standards challenge a sector-wide approach that supports collective defense
  - Due to non-uniform regulations, DER ownership, operation, and maintenance is difficult to effectively manage cybersecurity risk across state lines (e.g., VPPs)
  - Establish guidance for smaller DER owners and operators who don't have the resources to establish sound cyber controls on their own

Need for Harmonizing DER Cybersecurity Standards

- Few standards directly address cybersecurity for DERs.
- Some broader cybersecurity standards apply.
- Adjacent areas may include cybersecurity requirements.



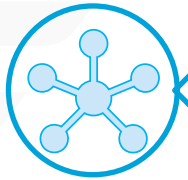


Rapidly developing technology

Increasing reliance on DERs for grid reliability

Diverse and complex stakeholder landscape

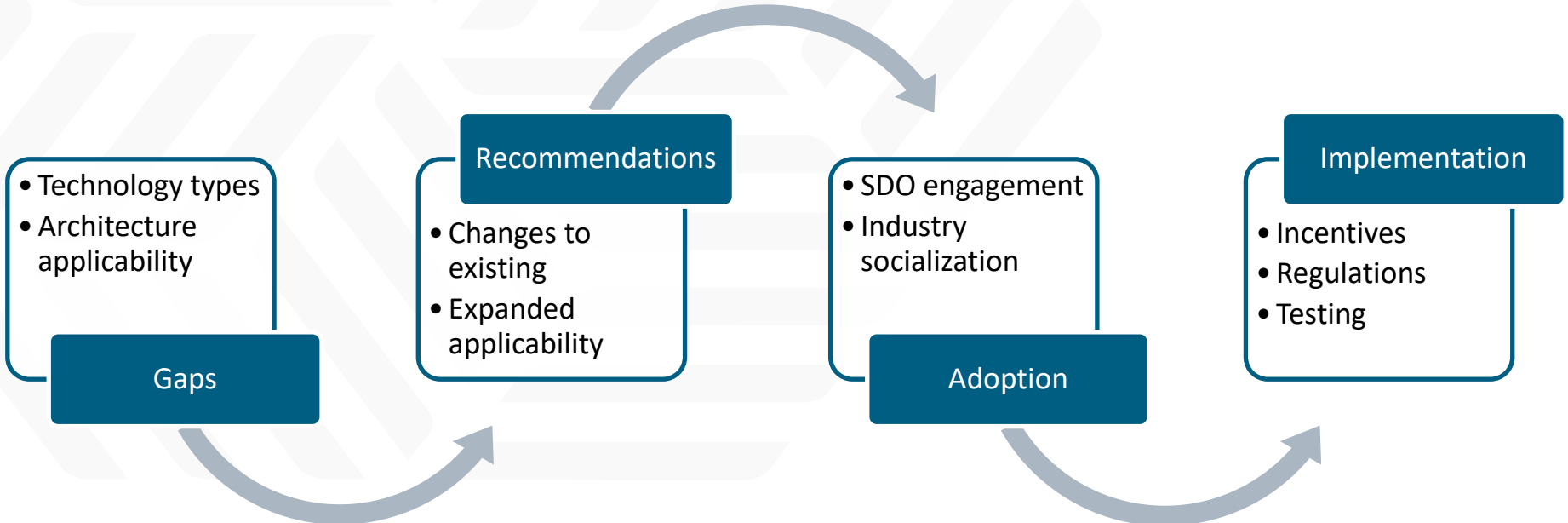
Non-uniform and/or not regulated policy among 50 states for IOU, co-ops, munis, aggregators or 3rd party



Full benefits of DERs reliant on digitization

How Can Harmonization be Achieved?

- Use the standards library to:
  - Create a one-stop-shop repository to gather and organize standards for reuse in a variety of ways, including the creation of learning modules, training, or testing guidance.
  - Easily share with a wide and diverse group of users.
  - Identify common elements and gaps to develop the harmonization strategy.
- Support the adoption and implementation of a consistent set of technical requirements for applicable cybersecurity standards.



Supporting a Harmonization Strategy

- Review, comment, and/or participate in working sessions on drafts of the standards library.
- Promote awareness among policymakers, standards developers, and technology developers of the strategic importance of standards harmonization.
- Help us understand how the implementation of a standards library can improve interoperability with assistive technologies and accelerate the overall progress of DER cybersecurity.
- Support the adoption and implementation of a consistent set of technical requirements for applicable cybersecurity standards.

NREL/PR-5T00-91354

This work was authored in part by NREL for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. 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.