NREL
Transforming ENERGY

Advancing Global Cybersecurity

Innovations in clean energy technology are beginning to transform electric grids around the world. It is more important than ever to understand and improve the resilience and security of the grid against natural and human disruptions as our energy systems become more distributed, intelligent, and interconnected. Through its advanced cybersecurity technical assistance portfolio, experts at the National Renewable Energy Laboratory (NREL) work with governments around the world to support secure and resilient deployment of renewable energy assets and address grid interconnection challenges. Cybersecurity technical assistance is tailored to the needs of our international partners.

> "As we adopt new technology for these emerging energy systems, cyber threats will evolve their capabilities to target and impact those energy systems. Action now is necessary to prepare for those threats."

Cybersecurity Expertise at NREL

With deep expertise in cybersecurity related to the design, integration, and operation of highly distributed energy systems, NREL can address the security and resilience of clean energy transformations as the grid continues to evolve and become increasingly autonomous and complex.

Cybersecurity Assessments

NREL's Distributed Energy Resource Cybersecurity Framework (DER-CF) assesses the cybersecurity posture—or health—of energy sites around the world. The DER-CF is designed for stakeholders who employ distributed energy systems or plan to implement distributed energy resources (DERs) for day-to-day operations. The DER-CF assessment is available at no cost as an interactive web tool (https://dercf.nrel.gov) focused on cyber-governance or policies, technical management, and physical security. The DER-CF currently presents users with a series of pertinent cybersecurity questions, which are used to generate a site-specific report and recommendations. NREL extended the scope of the DER-CF to include the National Institute of Standards and Technology Risk Management Framework to streamline the risk management processes for federal energy managers protecting DER systems. The National Institute of Standards and Technology Risk Management Framework is a cyclical process designed to incorporate principles of security and risk management into an organization's system policies and procedures. NREL's Distributed Energy Resources Risk Manager (DER-RM) is a downloadable, open-source tool (https://nrel-cyber.github.io/DER-RM) which allows users to focus on the Risk Management Framework process. 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.

Integration With ARIES Cyber Range

NREL's Advanced Research on Integrated Energy Systems (ARIES) Cyber Range (https://www.nrel.gov/security-resilience/cyber-range.html) 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 policy and technology by providing an integrated method of interacting with cybersecurity logs and alerts. With the help of NREL researchers, organizations can: use the 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; and improve organizational decision-making for procurement and third-party risk.

Aligning Cybersecurity Plans with Mission Function

Achieving a stronger cybersecurity posture and preparing for inevitable attacks requires clear definitions of support functions and alignment with an organization's core mission.

NREL can help ensure an organization's cybersecurity plans align with mission functions by reviewing cybersecurity and risk management processes; identifying gaps in cybersecurity policies, controls, and procedures; generating prioritized risk mitigation recommendations; and recognizing organization-specific workforce and cybersecurity awareness needs. NREL's technical assistance can achieve these goals through virtual or in-person interviews, in-depth assistance on DER-CF assessments, and delivery of customized technical trainings.

Identifying and Mitigating Cybersecurity Risks

Understanding and mitigating organizational risk is critical to producing security improvements and monitoring performance. This can be achieved through planning periodic risk assessments and highlighting areas that require additional support. Further technical assistance could include asset inventory, mission assurance mapping, and asset-secure life cycle planning; completion of a DER-CF assessment and gap analysis; implementation guidance for security controls; evaluation of supply chain security risks; development of risk acceptance criteria; and creating a cyber-operational technology road map as part of a comprehensive cybersecurity strategy.

Capacity Building and Technical Trainings

Cybersecurity challenges require continuous training and awareness for new and existing staff on current threat vectors, vulnerabilities, and overall organizational risks to proactively defend against malicious actors. NREL can deliver tailored webinars and virtual or in-person trainings, providing fundamental knowledge on common cybersecurity challenges with renewable energy resources. Other technical training and capacity building could include guidance on procurement and contract language to improve security, review of hardware or software testing procedures, documenting best practices for secure onboarding of energy management information systems, preparing for, and responding to cybersecurity incidents, and beyond.

International Cybersecurity in Action

Regional Cybersecurity Spotlight: Latin America and The Caribbean

Island nations in Latin America and the Caribbean are on the front lines of climate change and increasingly confront cybersecurity threats. Through partnerships with sponsors such as the U.S. Agency for International Development and the U.S. Department of State, NREL provides cybersecurity technical assistance to Latin America and the Caribbean at regional and national levels. NREL technical assistance in the region has included cybersecurity capacity building, workforce development and trainings, and assessing the cybersecurity posture of various power sector utilities through guided completion of DER-CF assessments.

Power Sector Cybersecurity Building Blocks

Developed through the enduring U.S. Agency for International Development-NREL partnership, NREL researchers developed a framework called the Power Sector Cybersecurity Building Blocks (https://www.nrel.gov/docs/fy21osti/79396.pdf), designed to help a wide range of stakeholders improve the cybersecurity of the electric grid. 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.

Resilient Energy Platform

Developed through the U.S. Agency for International Development-NREL Partnership, the Resilient Energy Platform (https://resilient-energy.org) provides expertly curated resources, training materials, tools, and technical assistance to enhance power sector security and resilience around the world. The platform enables decision makers to assess power sector vulnerabilities, identify resilient solutions, and make informed decisions.

National Renewable Energy Laboratory
15013 Denver West Parkway, Golden, CO 80401
303-275-3000 • www.nrel.gov

NREL prints on paper that contains recycled content.

NREL is a national laboratory of the U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy, operated by the Alliance for Sustainable Energy, LLC.

NREL/FS-5R00-87097 • October 2023