CYBERSECURITY FOR THE ENERGY TRANSITION

Renewable energy technologies such as distributed energy resources, supervisory control and data acquisition systems (SCADA), and advanced metering infrastructure are critical to the digitalization of energy systems and the clean energy transition. However, these internet-connected and networked technologies also expose their power sector owners and operators to cybersecurity risks.

Malign actors are increasingly preying upon power sector stakeholders across the globe that do not adequately incorporate cybersecurity into power sector planning. Ransomware attacks from prominent hacker groups affected more than ten Caribbean countries in 2023 alone. These attacks targeted entities across various sectors, including the power sector. These malign actors exploit newly expanded grids, insecurely deployed and configured technologies, and underprepared and understaffed workforces to launch cyberattacks which can lead to data breaches, billing irregularities, blackouts, and damage to equipment. Cyber vulnerabilities in turn can undermine consumer-utility trust and hinder power sector development and the clean energy transition.

Organizations that do not take appropriate cybersecurity measures run the risk of jeopardizing the benefits that renewable energy and clean energy technologies provide. As such, cybersecurity should be part of every power sector's plan for a just and secure energy future.

THE USAID SUPER PROGRAM'S APPROACH TO CYBERSECURITY: The USAID Strengthening Utilities and Promoting Energy Reform (SUPER) program, in partnership with the National Renewable Energy Laboratory (NREL), collaborated with Caribbean power utilities between 2021 and 2024 to enhance their cybersecurity capabilities in response to an increasingly targeted Caribbean power sector. SUPER and NREL initiated support by helping four utility and regulatory counterparts conduct an initial cybersecurity assessment to identify vulnerabilities, using NREL's free online Distributed Energy Resource Cybersecurity Framework (DER-CF) tool derived from the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2). The DER-CF tool and C2M2 framework helped utility information technology (IT) and operational technology (OT) staff identify the critical tasks that they needed to undertake to reduce cybersecurity vulnerabilities. Once complete, the SUPER and NREL teams presented the results of the assessment to senior management to make them aware of the actions and resources required to achieve their organization's cybersecurity goals.

Maturity Indicator Level

- To measure progression, the C2M2 Framework uses a scale of maturity indicator levels.
- **MIL 1 –** practices basic cybersecurity activities.
- **MIL 2 –** practices are progressively more complete, advanced, and ingrained to the organization's operations.
- **MIL 3 –** practices are more advanced and ingrained than MIL2; aligned to risk management.

For each utility that completed the DER-CF assessment process, the SUPER program identified priority cybersecurity domains (e.g., incident response, risk management, workforce management) from the assessment. The SUPER program also worked with all counterparts to deliver workshops, facilitate tabletop exercises (role-playing activities during which participants respond to real-life cybersecurity scenarios), and develop plans and policies to enhance the cybersecurity maturity of each utility. The

Resources for Power Sector Stakeholders

The SUPER program and partner organizations developed these open-source resources for the benefit of power sector stakeholders globally.

- NREL Power Sector Cybersecurity Building Blocks webinar series
- Cybersecurity for Operational Technology (OT) Workshop
- MIL1 Domain Deep Dive Workshop
- Plan to Enhance Technical Controls
- Representative Cybersecurity Action Plan
- Sample Incident Response Tabletop Workshop
- Sample Cybersecurity Governance Workshop

SUPER program aimed to help each utility achieve Maturity Indicator Level 1 (MIL1) status, as defined by the C2M2 Framework. MIL1 status comprises the basic cybersecurity measures that an organization should perform. MIL1 status also enabled organizations to benchmark and evaluate their capabilities on an ongoing basis to contend with the cyber risks inherent to the energy transition. This cycle of assessment and planning is particularly critical in an era where utilities are rapidly digitizing their power grids to accommodate increased intermittent renewable energy which further exposes them to cyber threats.

USAID SUPER PROGRAM FINDINGS AND RESULTS: The SUPER program's recommendations and assistance strengthened the cybersecurity maturity of five Caribbean utilities, from Antigua, Guyana, Grenada, Saint Kitts, and Trinidad and Tobago. This effort helped them improve their risk management capabilities, implement organizational incident response plans, enhance leadership support of IT and engineering staff, and connect stakeholders both within countries and across the region. The program also furnished each counterpart with a robust action plan for continued cybersecurity maturity growth. Counterparts stated that the capacity building activities and recommendations provided played a pivotal role in strengthening their cybersecurity defenses. The SUPER program's efforts revealed several key findings for how utilities can best address cybersecurity vulnerabilities by:

- **Adopting a cybersecurity framework** such as C2M2, to guide organizational cybersecurity planning to enhance decision-making and iterative development.
- **Strengthening governance** by convening teams across the organization (IT and OT) to develop plans and procedures to identify, prevent, and recover from cybersecurity incidents. Utilities should also align cybersecurity goals across departments, with buy-in at the executive level.
- **Upskilling the workforce** through "cyber hygiene" trainings on topics like phishing, multi-factor authentication, and other common attack vectors and defenses for all staff, as well as providing certifications and specialized training for IT and cybersecurity staff.
- **Focusing on priority cybersecurity domains,** such as incident response, risk management, and workforce development. Though assessments should typically lead the way for determining areas of technical assistance, these areas are common gaps for most utilities.
- **Connecting with other key actors in the cybersecurity ecosystem** such as national cyber security incident response teams (CSIRTs) and regulators to align on cybersecurity priorities. These entities, along with ministries, academia, and standards organizations, also need to coordinate closely with utilities for a whole-of-sector approach to cybersecurity defense.
- **Addressing operational technology (OT) cybersecurity,** which refers to protecting the programmable devices and systems which interact with physical environments, such as SCADA and remote terminal units, and have different sets of considerations than IT systems. Other power utilities around the world can also benefit from the SUPER use cases.

Utilities in other countries and regions are encouraged to explore the many open source SUPER tools and make use of NREL's online DER-CF assessment tool, as well as other cybersecurity resources such as the United States Energy Association and USAID Cybersecurity Digitalization webinar series. These tools can help reduce their own vulnerabilities and contribute to a successful, effective energy transition.

The USAID Strengthening Utilities and Promoting Energy Reform (SUPER) Task Order runs through September 2025 and has a ceiling of $12.8 million. SUPER offers energy sector entities services that include strategies and tools for reducing technical and non-technical losses; cybersecurity enhancement through assessments and other technical assistance; policy development and governance strengthening; and toolkits for accessing alternative sources of climate finance. SUPER is funded through REFS and through buy-ins by USAID Missions for in-country Work Assignments. More information is available on the USAID SUPER website.

CONTACT

Matthew Ogonowski, Senior Energy Advisor and SUPER COR, USAID/Washington, mogonowski@usaid.gov
John Garrison, Senior Clean Energy Advisor, USAID/Washington, jgarrison@usaid.gov
Crissy Godfrey, SUPER Chief of Party, Deloitte Consulting LLP, crgodfrey@deloitte.com