USAID's SUPER Program and the Caribbean Cybersecurity Work Assignment

Goals and Objectives

- The United States Agency for International Development's (USAID) Strengthening Utilities and Promoting Energy Reform (SUPER) Program aims to promote equitable, effective reforms and enhance the financial viability and sustainability of developing countries' electricity systems
- One of the Work Assignments under SUPER is focused on building the capacity of Caribbean energy sector and cyber entities to improve their cybersecurity awareness, posture, and preparedness in light of the rising threat of cyberattacks
- Deloitte has been tasked with implementing the activities under this Work Assignment. Deloitte will focus on local, national, and regional delivery of assistance, through local consultants, businesses, and industry groups. Deloitte is in the process of engaging national and regional stakeholders to understand issues, design assistance, and plan projects that advance USAID's SUPER goals.
- Deloitte will partner with the National Renewable Energy Laboratory (NREL) on many of these initiatives

Why Focus on Cyber Now?

The Caribbean Council reports that the costs of cyber incidents in the Latin America and Caribbean region total **$90B annually**.

Computer viruses increased by 131% in Latin America and the Caribbean between March 2019 and March 2020.

One utility in the region reported that the number of **identified attacks increased by 650%** since March 2020 compared to an average year.

Momentum is building: Internet searches for the term "cybersecurity" increased fivefold in the region between 2016 and 2019.

The threat is real, and regional stakeholders are beginning to prepare for this threat. **Now is the time to leverage resources, share knowledge, and coordinate strategies** to fight the increase in cyberattacks, ransomware, and other malware.

USAID SUPER and Other USG-Sponsored Initiatives

The SUPER program's cybersecurity work in the Caribbean aligns to a broader strategy of U.S. Government (USG) engagement in the region. The USG is funding the SUPER program's goals to align with USAID's Caribbean Energy Initiative (CEI) and with the Caribbean Energy Security Initiative (CESI) involving a broader coalition of partners. To learn more about the CEI, see the fact sheet here. To learn more about CESI, see the CESI page on the U.S. Department of State website here.

Caribbean Energy Initiative (CEI)

- USAID's CEI focuses on building energy sector resilience across the region, in recognition of the critical role that a steady, reliable energy supply plays in the daily economy of the region and in post-disaster recovery
- The CEI will promote local and U.S. private sector partnerships and investment in building energy sector resilience
- The CEI focuses on reducing electricity prices, raising service quality, and enhancing energy sector resilience in the Caribbean
- The CEI's geographic scope includes the Eastern and Southern Caribbean, Haiti, the Dominican Republic, and Jamaica

Caribbean Energy Security Initiative (CESI)

- The U.S.-Caribbean Climate and Energy Security Initiative 2030 (CESI 2030) is a partnership intended to increase the Caribbean's resilience to the impacts of climate change and extreme weather events, strengthen energy security, and advance economic growth by advancing clean energy and climate resilience in the region
- CESI 2030 will incorporate the lessons learned from previous U.S. government support in the region as well as explore innovative ways for encouraging the deployment of clean energy and other sector specific solutions that promote the region's ability to adapt to the impacts of climate variability and change

Key Cybersecurity Issues in the Caribbean Energy Sector

1. **Competitive market for dedicated cyber resources:** for many utilities and regulators, capacity is an issue. Many utilities are focused on keeping the lights on in the near term and eschew hiring cyber professionals.

2. **Opportunity for enhanced regional coordination:** Without a regional E-ISAC or ISAO and with only four countries in the region operating a CSIRT, there is ample opportunity to improve regional responses to the growing threat of cyberattacks.

3. **Lack of training and certification options:** University courses are relatively limited and there is no region-specific designation for cybersecurity professionals, hindering the talent development pipeline.

4. **Need for long-term cybersecurity strategy planning:** many organizations do not know where they stand from a cyber standpoint. The lack of tools and cyber infrastructure in place to assess capabilities and hinders planning capability.

5. **Poorly-defined or non-existent procurement standards:** the lack of procurement standards for grid modernizing technology means that utilities often purchase equipment at the least-cost, without factoring in the cost of increased vulnerability.

Potential Consequences of a Successful Cyber Attack on an Electric Utility

- Damage to critical physical infrastructure
- Financial loss from successful ransomware or other malware attacks
- Loss or theft of data, including sensitive financial and personal identifiable information (PII)
- Disruption in service and power outages, including large scale power outages
- Reduced confidence in grid modernizing technology and indigenous resource development in the Caribbean region

How the USAID SUPER Program Can Help Your Organization

The SUPER team wants to work with your organization to accomplish cybersecurity goals. Below are some of the illustrative areas where USAID, Deloitte, and NREL can engage to advance your cyber priorities.

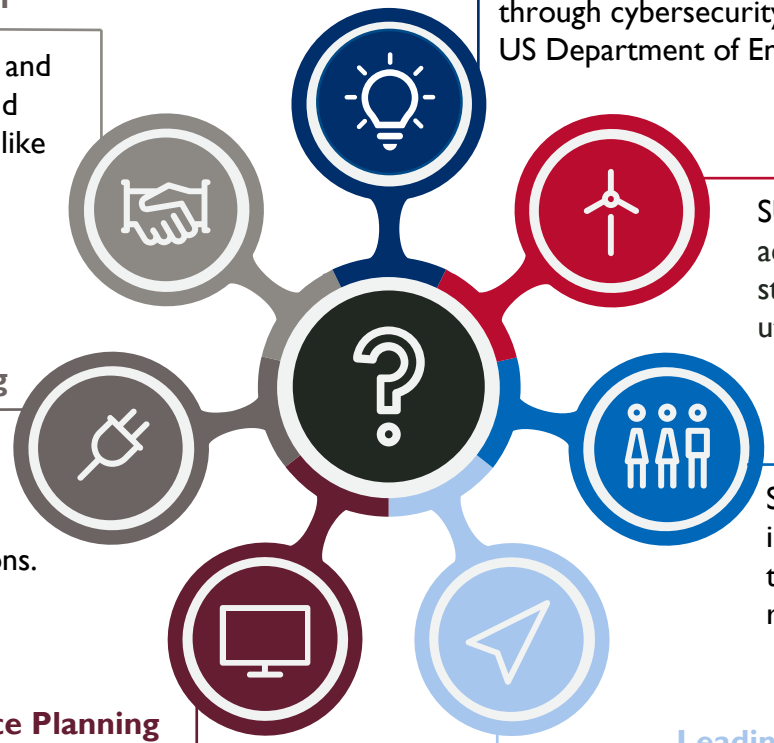
Illustrative offerings for your organization from USAID's SUPER Program. Assistance can be tailored to org-specific needs.

Utility Cybersecurity Assessments

SUPER/Deloitte can build the cybersecurity capacity of utilities through cybersecurity assessments with leading tools, such as the US Department of Energy's (DOE) DERCF tool.

Enhancing Regional Collaboration

SUPER/Deloitte can help support regional and national organizations, such as CSIRTs,, and contribute to the development of entities like ISACs to promote the ability of regional utilities to learn from one another.



Strategies, Plans, and Roadmaps

SUPER/Deloitte can work with utilities to develop activities that will help utilities create cybersecurity strategies both in response to and outside of the utility-specific assessments.

Knowledge Sharing and Learning

SUPER/Deloitte will facilitate the Cybersecurity Building Blocks webinar series and a regional forum to promote regional learning and facilitate connections.

Tools and Training

SUPER/Deloitte can identify and help utilities implement low-cost or no-cost cybersecurity tools that will improve their cybersecurity posture while recognizing budgetary and human capital limitations.

Capacity Building and Workforce Planning

SUPER/Deloitte can develop and deliver trainings on topics such as cyber hygiene and critical infrastructure at the executive, management, or front-line employee level.

Leading Practice Material Development

SUPER/Deloitte can work with regional and national energy sector players to create procurement standards, scale successful approaches from one country to another, and develop region- or country-specific strategy guides for building cyber resilience.

The Deloitte SUPER Cyber Team

The Deloitte team will lead and manage many of the technical activities under the SUPER program, including helping utilities develop strategies, plans and roadmaps; building regional capacity through leading practice materials and cyber training tools; building out knowledge sharing capabilities in the region; and hosting and facilitating regional events.

Sophia Peters

Sophia is a Senior Manager within the Strategy and Operations group for Deloitte Consulting LLP. She supports a variety of projects focused on international clients in emerging markets: clean energy policy, access to finance, electricity markets, and power project development

Anne Robbins

Anne is a Manager in the Cyber and Strategic Risk group with over 20 years of experience designing, implementing, securing, and managing operational technology systems that support critical business functions, such as SCADA, industrial control systems, virtualization platforms, data repositories, and general system and user support, primarily in the U.S.

Crissy Godfrey

Crissy is a Specialist Leader with 20 years of experience in the energy sector, specializing in energy governance, regulation and market reform. Her technical specialties include energy efficiency, demand response, renewable energy, distributed generation, smart grid as well as competitive retail and wholesale markets in domestic and international spaces.

Alex Brillman

Alex is a Consultant with experience across both energy and cybersecurity activities, including assisting the U.S. Navy to develop a cybersecurity employee training program and to implement programs pertaining to automated metering infrastructure, LTE deployment, facility-related control systems, direct digital control systems standardization.

Michaela Palmer

Michaela is a Business Analyst who is passionate about solving complex problems in the public sector, especially as they relate to the incorporation of technology to promote efficiency and effectiveness in addressing environmental issues and international development.

The NREL Cyber Team

The NREL team will lead the cybersecurity assessments of regional utilities through the Distributed Energy Resource Cybersecurity Framework (DERCF) tool; shape the technical assistance resulting from these assessments; and continue to help facilitate webinars in the Power Sector Cybersecurity Building Blocks webinar series.

Maurice Martin

Maurice Martin is a senior cybersecurity research leader in NREL's Secure Cyber-Energy Systems Group. Martin provides program development and system-level analysis for cybersecurity initiatives in the utility space. His work includes developing strategic research objectives, impact analysis, and experiment design. He engages large and diverse groups of stakeholders on efforts to improve technology, security, and resilience and serves as liaison to utilities, vendors, and associations.

Tami Reynolds

Tami Reynolds is a project manager and lead for NREL's Secure Cyber-Energy Systems Group. She provides technical leadership in building out and marketing the Distributed Energy Resources Cybersecurity Framework tool to industry and federal partners. She works closely with chief information officers and chief information security officers of private industry partners to conduct cybersecurity assessments in the electric sector, and she provides support to the USAID in developing cybersecurity programs in developing countries.

Laura Leddy

Laura is a Cybersecurity and Resilience Researcher in NREL's Energy Security and Resilience Center. Her work focuses on integrating cyber and physical resilience in U.S. and international energy systems, with an emphasis on supporting partner organizations in developing cybersecurity best practices. Laura has supported a number of cyber-physical resilience projects for the U.S. Department of Energy, including under the Grid Modernization Laboratory Consortium and Federal Energy Management Program.