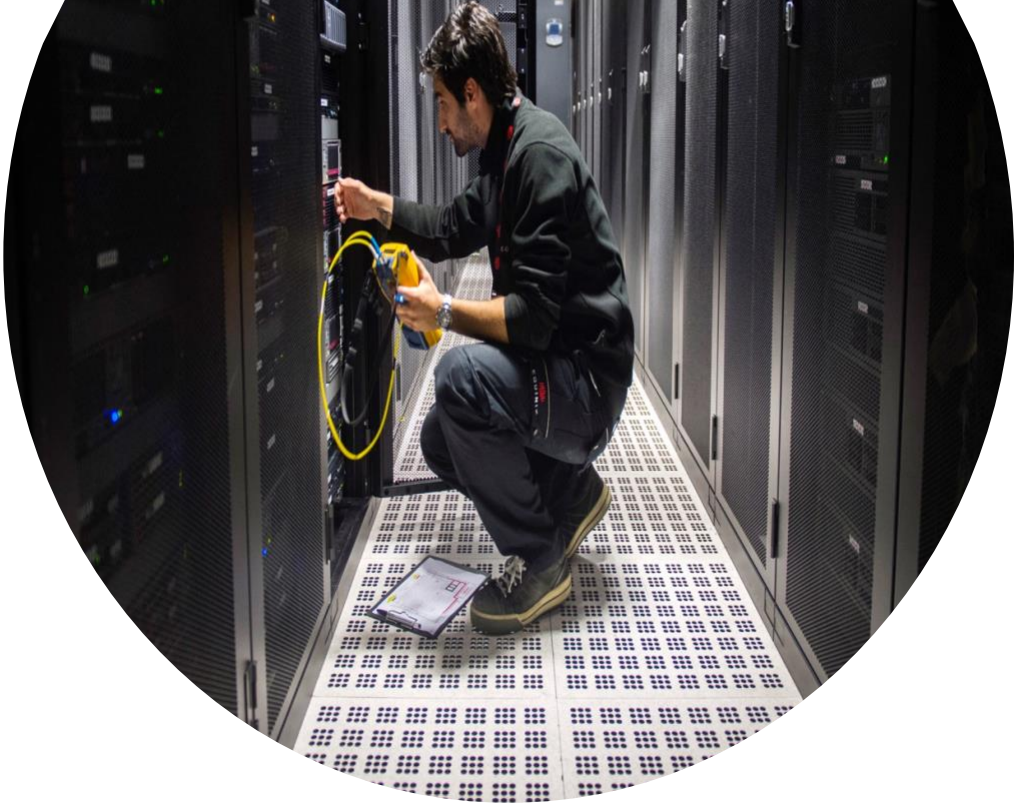
USAID
FROM THE AMERICAN PEOPLE



MARTIN BUREAU/AFP

COUNTERING ENERGY CYBERSECURITY THREATS

Preparing the next generation of skilled workers to reduce cyber risk and increase resilience

DIGITALIZATION

As the global power sector transitions to clean energy, digitalization is key to integrate renewables, improve the reliability of power grids, and reduce costs. Digital platforms can deliver much needed efficiencies and future resilience, creating jobs and economic growth while driving climate action. Digitalization is already improving the safety, productivity, accessibility and sustainability of energy systems. However, it is also raising new security and privacy risks, changing markets, businesses and employment. Today's digital transformation is a driver of emerging new business models and services. Over the next two years, 2.5 billion new industrial devices are expected to be connected to energy infrastructure, from gas turbines and microgrids, to electric vehicle charging stations. As technology evolves to become "smart," it is imperative for utilities and governments to strategically manage the avalanche of data coming from smart devices and other sources.

CYBERSECURITY

Grid modernization exposes utilities to potential threats from nation-states, criminals, disgruntled employees, and accidental misconfiguration. The risk of cyber attacks has risen with the increase in digital transformation. Global cyber attacks increased by 50% in 2021, compared to 2020. Global cybercrime costs are expected to grow by 15% per year over the next five years, reaching $10.5 trillion annually by 2025, up from $3 trillion in 2015. In parallel to these increasing risks, there is an undersupply of global cyber professionals who can provide leadership, test and secure systems, and train people in digital hygiene. Today, a severe cybersecurity workforce shortage and talent gap exists, with an estimated shortage of more than 3 million cybersecurity professionals globally.

Cybersecurity has traditionally been viewed as a technology issue, but is now also regarded as a key environmental, social and governance (ESG) concern. Companies can experience severe reputational damage and also be fined if information networks are not adequately protected.

APPROACH

The Countering Energy Cybersecurity Threats (CECT) program strengthens local partners' ability to counter cyberattacks on critical energy infrastructure by building skills to detect, protect, respond and recover from cyberattacks. This project introduces USAID partners to U.S. cyber standards, policies, and practices, while also providing insight for U.S. actors into the cyber threats and needs of USAID partner countries.

This program takes a holistic approach to cyber education for energy professionals with no technical prerequisite knowledge required. Participants will gain an understanding of, and appreciation for, the relationship between information and operational technologies. Hands-on experiences will help to illustrate technical challenges, risks, and vulnerabilities common in energy system hardware and business services. Attendees will be encouraged to consider how their role in the workplace contributes to the security of their organization and study best practices.

USAID's targeted workforce development training aims to minimize the knowledge gap and increase the talent pool in cybersecurity around the world, to help train operators to monitor equipment, detect intrusions, and defeat attackers. The project utilizes the vast experiences and knowledge of a diverse team as well as energy sector experts from around the world - offering an unparalleled network of utility and energy sector expertise to support the global energy transition.

Our goal is to dramatically reduce risk while increasing participants' ability to operate power systems in a more secure manner. Successful participants will earn Institute of Electrical and Electronics Engineers (IEEE) certification, the world's largest technical professional organization. A select group of participants will be eligible for Global Information Assurance Certification (GIAC), one of the most challenging and meaningful credentials in cybersecurity.

PARTNERS

UNITED STATES ENERGY ASSOCIATION (USEA): An association of public and private energy-related organizations, corporations, and government agencies. For 30 years, USEA has built peer-to-peer relationships in USAID-assisted countries to promote energy security, renewable energy, and the transition to a cleaner global energy economy.

ARIZONA STATE UNIVERSITY (ASU): ASU is a leading U.S. Center of Excellence in research that curates and advances innovations from idea to implementation. Global research and training networks led by ASU reach over 100 countries with a focus on varied energy themes and online workforce development programs.

SANS INSTITUTE (SANS): SANS is an industry-trusted resource for cybersecurity training, certifications, and research, setting the bar for cybersecurity education.

GLOBAL INFORMATION ASSURANCE CERTIFICATION (GIAC): GIAC certifications are a guarantee of critical skill mastery which tests for real-world skills and are considered the most rigorous global assurance of cyber knowledge.

CONTACT:

Kristen Madler
DDI/EEI/E Clean Energy Coordinator
kmadler@usaid.gov

Jamila Amodeo
DDI/EEI/E Senior Energy Advisor
jamodeo@usaid.gov