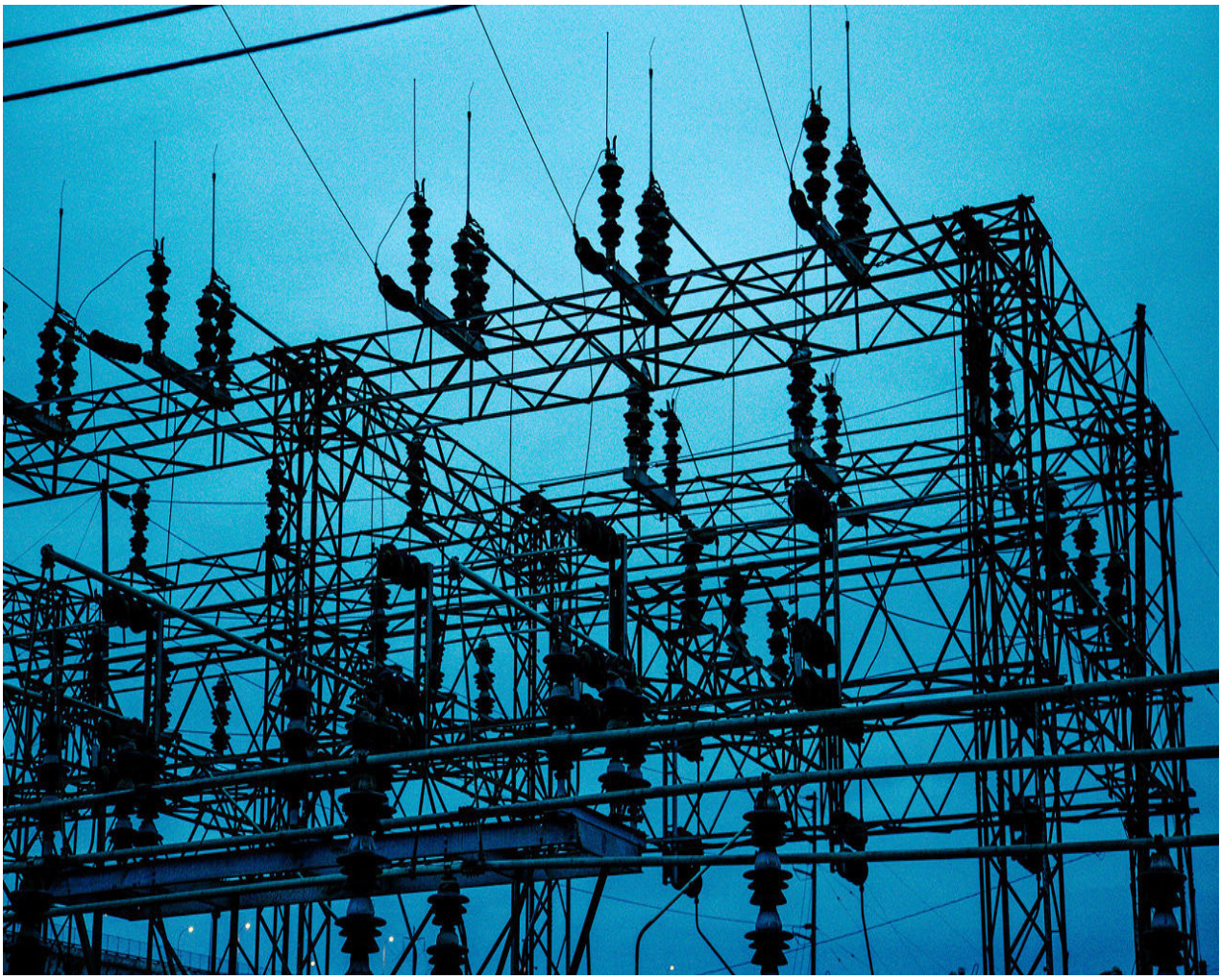
The Virgin Islands Consortium

WAPA And Energy Industry Partners Continue Dialogue On Threats Of Cyber Attacks On Electrical Systems

Business / **Published On June 02, 2017 06:40 PM /**

Staff June 02, 2017



ST. THOMAS -- Personnel from the Virgin Islands Water and Power Authority were among the participants in a continued discussion on Friday about the risks of cyberattacks on electric generating and distribution systems, WAPA has made known.

The Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA) project is a three-year-old initiative, funded through the Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE-OE) program, under the Cybersecurity for Energy Delivery Systems (CEDS) initiative. The DOE-OE/CEDS mission is to help the

energy sector by developing cybersecurity solutions for energy delivery systems. Under CEDS, the CYMSA project seeks to increase situational awareness and visibility into the potential threat of cyberattacks against energy delivery systems such as power plants and electrical transmission systems, and defines how such systems can be protected. The program aims to enhance both the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

"The presentation highlighted technology and techniques that can be used to detect and respond to adversarial cyber activity which seeks to evade detection while manipulating the operation of power grid components," said WAPA's Chief Executive Officer Julio A. Rhymer, Sr. He noted that companies such as WAPA can never take too lightly the possibility that its vast security systems can be either manipulated or defeated, allowing a cyberattack to disrupt energy delivery to thousands of customers.

The CYMSA project is developing a cybersecurity situational awareness technology suite to detect adversarial manipulation of power grid components and communication networks. The project involves novel cyber-physical modeling and simulation research on communications networks and substations.

Mr. Rhymer noted the technical objectives include research and development, test and validation and technology demonstration. At the end of the project the research results will include: the cybersecurity situational awareness technology suite, enhanced modeling and simulation technologies, network security sensors based on open-source intrusion detection and prevention systems and protective rule generation, consensus and synchronicity protocols.

The presentation also included a tour of WAPA's electrical substation at the Estate Donoe solar facility on St. Thomas.