NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Announcement

E-ISAC Expands Key Cybersecurity Program

November 30, 2020

WASHINGTON, D.C. – NERC's Electricity Information Sharing and Analysis Center (E-ISAC) recently partnered with the Department of Energy (DOE) on an expansion of the Cybersecurity Risk Information Sharing Program (CRISP) to include operational technology. The CRISP expansion, to include two operational technology pilots, marks a major milestone to improve E-ISAC capabilities that strengthen grid security in North America.

The purpose of the new pilots is to identify potential cyber threats to utilities' industrial control systems by capturing raw and/or refined operational technology data and comparing it to CRISP information technology data.

"The CRISP operational technology pilots are an important advance in E-ISAC capabilities and reflect a maturation of our partnership with DOE," said Frank Honkus, E-ISAC associate director, Intelligence Programs and CRISP Manager. "These pilots will help the E-ISAC meet its core responsibility of advising utilities on the detection and mitigation of industrial control system threats from the most advanced and persistent international adversaries."

Under the first pilot, E-ISAC analysts will leverage operational technology sensors that are already installed across the electricity industry to identify anomalous or potentially malicious cyber behavior. The objective of the second pilot, primarily funded by DOE, is to gain unique cybersecurity insights from the correlation and analysis of CRISP information technology data and operational technology data from the DOE-funded, National Rural Electric Cooperative Association (NRECA)-led Essence program. Essence uses sophisticated real-time anomaly detection to identify and warn of possible network breaches.

In partnership with DOE, this pilot will expand to include five utility members of NRECA, and the Essence program will be expanded to include the CRISP community.

CONTACT:
Kimberly.Mielcarek@nerc.net

In addition to the two operational technology pilots, the Pacific Northwest National Laboratory (PNNL) and E-ISAC are improving CRISP through a new information technology project that facilitates detecting anomalous and malicious activity on utilities' business networks. The E-ISAC manages CRISP under an agreement with PNNL, which installs network monitoring equipment at participating utilities and supports CRISP analysis that the E-ISAC produces for asset owners and operators (AOOs) across North America.

"CRISP is a unique capability for utilities, providing threat and trend analysis that participants cannot get anywhere else," Honkus noted. "The pilots and the strong public–private partnership with DOE and PNNL ensure that CRISP continues to evolve to meet emerging threats to industry."

Under the CRISP information technology project, the E-ISAC will integrate the analysis of email and website traffic data to improve the identification and mitigation of broader cyber threats to AOOs. These new data sources will inform CRISP analysis and provide more robust product lines for the CRISP community. Contact the E-ISAC for information about becoming a member.

###

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable and secure North American bulk power system. Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.