NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Announcement

NERC Develops Practice Guide to Provide Clarity When Evaluating Network Monitoring Technology

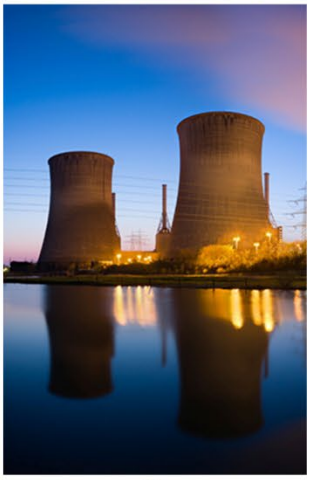
June 7, 2021

WASHINGTON, D.C. – NERC developed a practice guide to facilitate the deployment of network monitoring solutions in response to the Department of Energy's (DOE) 100-day plan. The guide addresses the application of NERC's Critical Infrastructure Protection (CIP) Reliability Standards during such deployments. DOE's initiative, which was launched on April 20, advances technologies that provide increased and/or enhanced cyber visibility, detection and response capabilities for utilities' industrial control systems (ICS) and operational technology (OT) networks to better protect the nation's grid.

While many entities have already deployed these types of technologies within their OT environments, NERC anticipates an increase in deployments across industry to enhance threat detection and response capabilities, in light of the 100-day plan. To provide additional transparency on how CIP standards apply in connection with these deployments, NERC developed the practice guide — formally titled the *ERO Enterprise CMEP Practice Guide: Network Monitoring Sensors, Centralized Collectors and Information Sharing*. The guide outlines a framework for a common approach to auditing compliance with the CIP Reliability Standards when a registered entity deploys detection and monitoring technologies that include network monitoring sensors and centralized data collectors and may involve the sharing of data collected with third parties.

NERC is supportive of the DOE's initiative encouraging the deployment of network monitoring solutions to enhance the overall cyber defenses of the electricity industry and promote increased information sharing.

"This guide adds clarity to the ERO Enterprise's framework on our auditing approach regarding our CIP standards and network monitoring solutions," said Jim Robb, NERC president and chief executive officer (CEO). "The ultimate goal is to drive consistency across the ERO Enterprise and provide a level of certainty for registered entities on how they will be evaluated should they choose to adopt these technologies. DOE's



CONTACT:
Kimberly.Mielcarek@nerc.net

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

100-day plan is a critically important initiative in bolstering our protections for critical electric infrastructure."

In addition to the practice guide, NERC's Electricity Information Sharing and Analysis Center (E-ISAC) is working with industry members and partners to support the implementation of measures or technologies that enhance detection, mitigation and forensic capabilities, particularly those focused on critical ICS and OT networks.

The E-ISAC and its partners will analyze and share across industry the information these monitoring technologies generate, enhancing industry's situational awareness and cyber security posture. The Cybersecurity Risk Information Sharing Program (CRISP), administered by the E-ISAC, will also play a role in the initiative, as DOE and utilities look to leverage existing sensor in the information technology environment as part of a defense-in-depth approach.

CRISP technology, data movement, reporting and notification processes — which are well established and understood by the participants, the E-ISAC and the government — will complement the understanding of the threat landscape. Finally, NERC and E-ISAC continue to work with the Electricity Subsector Coordinating Council and government agencies on information sharing practices and facilities to counter the growing threat.

"We appreciate the increased focus on cyber security in DOE's 100-day plan, in particular the emphasis on information sharing and the adoption of measures and technologies to enhance the cyber defense of ICS and OT networks," said Manny Cancel, NERC senior vice president and CEO of the E-ISAC. "The E-ISAC relies heavily on intelligence provided by government agencies and industry partners as well as the insight gained through voluntary information sharing from our asset owners and operators. Cooperation and collaboration are fundamental aspects of our ability to share timely and actionable information with members and partners required to mitigate their exposure to these threats."

NERC and the E-ISAC look forward to working with our partners to address the marked increase in cyber and physical security threats. As reducing cyber and physical security risk across North America continues to be a priority, NERC shares a commitment to reinforcing the reliability and security of the bulk power system by creating a strong, knowledge-based defense built on sharing and collaboration.

###

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.