

Northwest Public Power Association
Resolution 2010-08
Protecting the Bulk Power System from Cyber Attacks

Background

NWPPA supports protecting its infrastructure from cyber attacks. In 2007, the North American Electric Reliability Council (NERC), acting as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) for the U.S. Department of Homeland Security (DHS), distributed a cyber-vulnerability alert developed by DHS to selected entities in the electric power sector. The DHS “Aurora” alert was not subject to mandatory compliance under Federal Power Act (FPA) Section 215, which mandates reliability standards for certain electric utilities. The alert was intended to caution the industry to secure remotely accessible transmission relays and other devices from cyber attack, based on simulations conducted at the Idaho National Lab which demonstrated that remote access to bulk power system (BPS) relays could be used to damage rotating machines—such as generators, pumps or motors— that are connected to the power grid. The electric utility industry voluntarily complied with this alert.

Following the release of the DHS Aurora alert, in 2008 Congress conducted hearings to consider the Federal Energy Regulatory Commission’s (FERC), NERC’s and industry’s response to the alert and other related issues. FERC’s Chair argued at a congressional hearing that the Commission needs additional authority, to supplement FPA Section 215, authorizing FERC to impose interim reliability standards on an emergency basis when national security or intelligence agencies identify an imminent cyber threat to the bulk-power system. NERC’s CEO agreed. Many in Congress also agreed, resulting in House legislation giving FERC limited authority to direct the electric utility industry to take certain steps in the event of a cyber-security emergency. The Senate also drafted legislation that gave the Department of Energy a greater role.

NWPPA’s Position

- Should Congress consider legislation, NWPPA would encourage policymakers to focus on legislation that is narrowly crafted and targeted to address the issues involving cyber security without placing an unnecessary burden on the electricity industry that may produce only limited results.
- NWPPA opposes legislation to grant FERC broader powers to develop and implement standards during an emergency.
- NWPPA supports a method that relies on electric industry developed actions that facilitate expedient identification and understanding of electric system vulnerabilities, with standardized procedures for disseminating information to utilities.

Origination Date: 2009. Revised in 2010. Approved 5-25-2010 by NWPPA membership.