

1 **Northwest Public Power Association**

2 **Resolution 2010-08**

3 **Protecting the Bulk Power System from Cyber Attacks**

4
5 **Background**

6
7 NWPPA supports protecting its infrastructure from cyber attacks. In 2007, the North American
8 Electric Reliability Council (NERC), acting as the Electricity Sector Information Sharing and
9 Analysis Center (ES-ISAC) for the U.S. Department of Homeland Security (DHS), distributed a
10 cyber-vulnerability alert developed by DHS to selected entities in the electric power sector. The
11 DHS “Aurora” alert was not subject to mandatory compliance under Federal Power Act (FPA)
12 Section 215, which mandates reliability standards for certain electric utilities. The alert was
13 intended to caution the industry to secure remotely accessible transmission relays and other
14 devices from cyber attack, based on simulations conducted at the Idaho National Lab which
15 demonstrated that remote access to bulk power system (BPS) relays could be used to damage
16 rotating machines—such as generators, pumps or motors— that are connected to the power
17 grid. The electric utility industry voluntarily complied with this alert.

18
19 Following the release of the DHS Aurora alert, in 2008 Congress conducted hearings to consider
20 the Federal Energy Regulatory Commission’s (FERC), NERC’s and industry’s response to the alert
21 and other related issues. FERC’s Chair argued at a congressional hearing that the Commission
22 needs additional authority, to supplement FPA Section 215, authorizing FERC to impose interim
23 reliability standards on an emergency basis when national security or intelligence agencies
24 identify an imminent cyber threat to the bulk-power system. NERC’s CEO agreed. Many in
25 Congress also agreed, resulting in House legislation giving FERC limited authority to direct the
26 electric utility industry to take certain steps in the event of a cyber-security emergency. The
27 Senate also drafted legislation that gave the Department of Energy a greater role.

28
29 **NWPPA’s Position**

- 30
31
- 32 • Should Congress consider legislation, NWPPA would encourage policymakers to focus
33 on legislation that is narrowly crafted and targeted to address the issues involving cyber
34 security without placing an unnecessary burden on the electricity industry that may
35 produce only limited results.
 - 36 • NWPPA opposes legislation to grant FERC broader powers to develop and implement
37 standards during an emergency.
 - 38 • NWPPA supports a method that relies on electric industry developed actions that
39 facilitate expedient identification and understanding of electric system vulnerabilities,
40 with standardized procedures for disseminating information to utilities.

41 Origination Date: 2009. Revised in 2010.