Northwest Hydro Operators Regional Forum

Thursday, May 22, 2008
Skamania, Washington

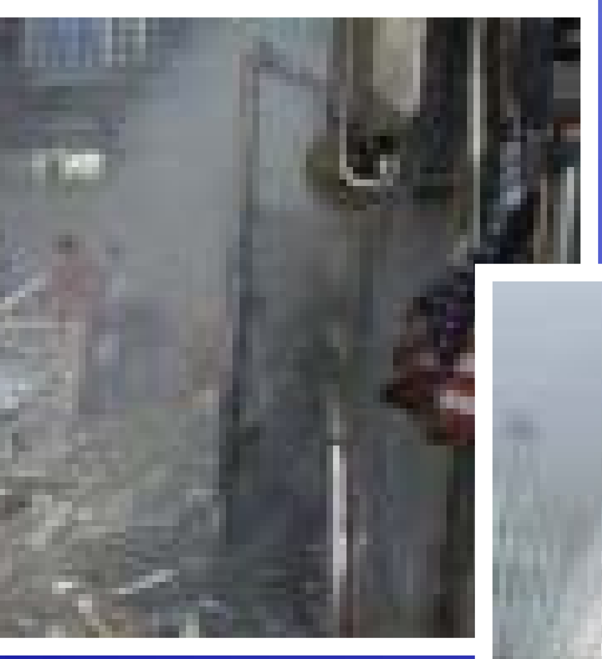
MANAGEMENT ISSUES

NERC CIP STANDARDS

Dick Robert, Chelan County Public Utility District, Wenatchee, Washington

CRITICAL INFRASTRUCTURE PROTECTION

911 – THE CAUSE



WHY THE CIP STANDARDS:

DOE

NERC

FERC

U.S. Congress

NIST

ELECTRICITY: Cybersecurity standards under review (05/19/2008)

A House Homeland Security subcommittee will receive an update this week on new security measures to protect the nation's bulk power system from cyber attacks.

The standards created by the North American Electric Reliability Corp. (NERC) -- the electricity reliability organization created by the Energy Policy Act of 2005 -- require managers and owners of the interconnected bulk power system throughout North America to enact policies and measures to protect physical and electronic access to grid control systems.

Wednesday's hearing will examine eight mandatory standards (CIP 002 – 009) the Federal Energy Regulatory Commission approved in January.

Subcommittee Chairman James Langevin (D-R.I.) said at the hearing "the disruption of electricity to chemical plants, banks, refineries, hospitals, water systems and military installations presents a terrifying scenario."

He added, "Why [NERC] would have standards below NIST is beyond me. This is something we're going to [pay] close attention to; perhaps legislation will be required."

Standard CIP-001-1 — Sabotage Reporting

Purpose: Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

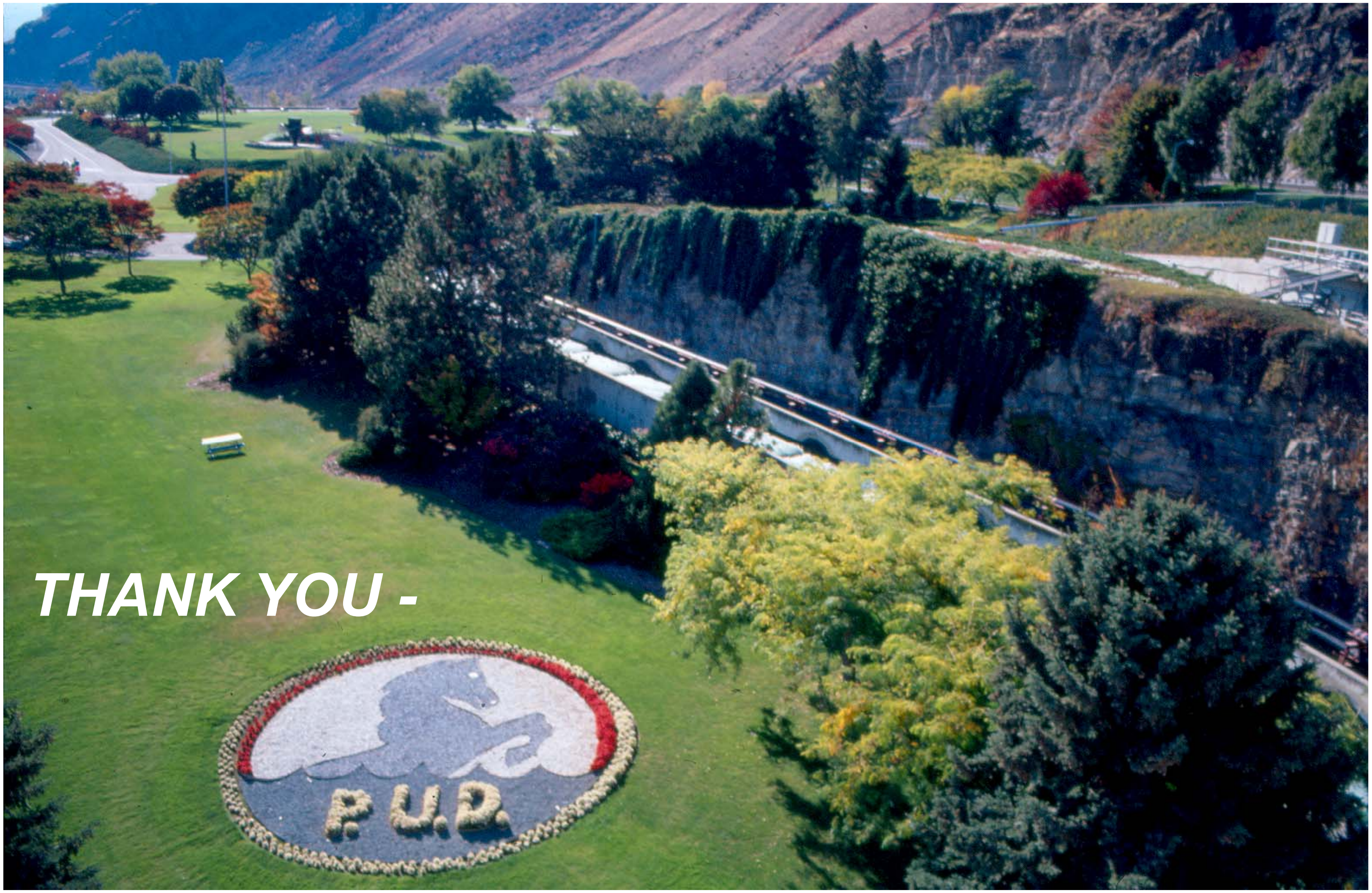
Standard CIP–004–1 — Cyber Security — Personnel and Training

Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

Standard CIP–008–1 — Cyber Security — Incident Reporting and Response Planning

Standard CIP-008 ensures the reporting of Cyber Security Incidents.

Questions



THANK YOU -

DICK ROBERT
Director - Security Division
CHELAN COUNTY PUBLIC UTILITY DISTRICT No. 1
dick.robert@chelanpud.org