Resolution on Physical Security

WHEREAS, Multiple threats have challenged the security of electricity grid networks at both the high-voltage and distribution levels, including cybersecurity, physical security, electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) events, and potentially a black sky event of an all-hazards scenario; *and*

WHEREAS, Electric utilities have recognized these threats historically, and have attempted to mitigate such threats through a variety of measures, especially after the extensive black-out in the Northeast and Canada in 2003 that prompted Congress to mandate certain reliability standards for the bulk electric power system in legislation passed by Congress in 2005; *and*

WHEREAS, The North American Reliability Corporation (NERC) was certified by FERC as the Electric Reliability Organization (ERO) to develop mandatory reliability standards, and to also develop standards for cybersecurity and physical security measures, called the Critical Infrastructure Protection (CIP) standards, and has now adopted version 5.0; *and*

WHEREAS, Historically, the potential physical threats to the bulk electric system have been well documented in several national reports by electric grid experts that have received national attention from utilities, the press, and the Congress, such as the Office of Technology Assessment Report in June, 1990 (*Physical Vulnerability of Electric Systems to National Disasters and Sabotage*), and the National Research Council (NRC) report in 2012, *Terrorism and the Electric Power Delivery System*, The National Academy Press, Washington, D.C.; *and*

WHEREAS, Since those national reports have been published, the threats to industrial control systems such as SCADA equipment from cyber attacks, and the key critical assets from a physical security perspective have been increasing in frequency, sophistication, and persistence; *and*

WHEREAS, The interdependencies of other key critical infrastructure sectors, such as natural gas and water sectors, with the electric sector, have been highlighted in these studies, expert analyses, the GRIDEX II exercise that simulated a concurrent physical and cyber attack, and by several incidents; *and*

WHEREAS, A well-planned attack by certain perpetrator(s) on the Metcalf substation incident near San Jose, California in April, 2013, has prompted a necessary re-assessment by transmission owners and operators of enhanced physical security measures to protect critical infrastructure facilities in all regions of the country reflecting the most up-to-date security techniques and monitoring; *and*

WHEREAS, Most utilities and transmission grid operators recognize that certain vulnerabilities to physical and cybersecurity need to be addressed separately and in conjunction on a dynamic basis reflecting a constantly changing threat environment from a variety of potential actors who desire to harm such critical systems, including individuals and groups, non-State actors, organized crime syndicates, and potentially State actors (foreign governments); *and*

WHEREAS, NARUC members recognize the urgency and severity of this threat environment, both physical and cyber, and especially acknowledge the need to take certain actions in the aftermath of the Metcalf substation incident, and in the analysis and work by NERC, NRC, and other experts leading up to this specific incident that could have resulted in cascading effects throughout the Western Interconnection; *and*

WHEREAS, NARUC members also recognize the need for a thorough and diligent cost-effective analysis for the mitigation measures for physical security by NERC; *and*

WHEREAS, FERC acted promptly under the leadership of Chairman Cheryl LaFleur and her colleagues on March 7, 2014, to direct NERC promptly to develop certain physical security standards based on a definition of "critical facilities" and use of a broad risk assessment methodology by the utilities and transmission owners, without being prescriptive (Docket No. RD14-6-000); *and*

WHEREAS, NERC responded in a timely way by developing such a standard, called CIP 014-1, in a record time of about two months, approving it by 86 percent in a ballot that closed on May 6th, and subsequently submitting such standard in a petition to FERC on May 23rd, that largely followed the criteria in the "roadmap" that FERC set forth in its earlier Order of March 7th; *now, therefore, be it*

RESOLVED, That the Board of Directors of the National Association of Regulatory Utility Commissioners, convened at its Summer Committee Meeting in Dallas, Texas, acknowledges that the protection of "critical facilities" of the electric delivery system is a shared regulatory oversight responsibility of FERC, NERC, and the State Commissions, and commends NERC for taking prompt action to develop a standard based on a comprehensive risk assessment methodology, and urges FERC to give the CIP-014 standard favorable consideration; *and be it further*,

RESOLVED, That State Commissions should devote significant attention to such a standard, along with cybersecurity and other potential hazards to the electricity delivery system, in either a collaborative or other process so that the regulated utilities in the State comply with such a standard, recognizing that the circumstances and geographies in each State may differ substantially; *and be it further*,

RESOLVED, That State Commissions should endeavor to work with their regulated utilities to ensure that such a CIP standard is reviewed promptly in an appropriate forum, in accordance with a cost-benefit methodology used by each Commission.

Passed by the Committees on Critical Infrastructure and Electricity.
Approved by the NARUC Board of Directors July 16, 2014