2015 - 07

NATIONAL SHERIFFS' ASSOCIATION RECOGNIZES THE SEVERITY OF THREATS TO THE ELECTRICITY GRID NETWORKS AND THE URGENCY OF ACTIONS NEEDED TO ASSESS, PLAN, AND IMPLEMENT MORE SECURE NETWORKS

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 and the government have historically recognized these threats and attempted to mitigate them 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 Electric Reliability Corporation (NERC) was certified by the Federal Energy Regulatory Commission (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 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*), published by The National Academy Press, Washington, DC, and;

WHEREAS, since those national reports were published, the threats of cyber-attacks to industrial control systems — such as Supervisory Control and Data Acquisition (SCADA) equipment — and 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 NERC GRIDEX II exercise that simulated a concurrent physical and cyber-attack; and by several incidents; and;

WHEREAS, a well-planned attack on the Metcalf substation 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 coordination between local law enforcement and relevant federal agencies, i.e., FERC, NERC, DHS, and others, 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, the National Sheriffs' Association (NSA) recognizes the urgency and severity of this threat environment, both physical and cyber, and especially acknowledges 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, including DHS and the FBI, leading up to this specific incident that could have resulted in cascading effects through the Western Interconnection, and;

WHEREAS, NSA also recognizes the need for a thorough and diligent cost-effective analysis of the mitigation measures and solutions for physical security by NERC, and;

WHEREAS, FERC has acted promptly under the leadership of Chairperson Cheryl LaFleur and her colleagues to direct NERC to promptly 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 National Sheriffs' Association acknowledges that protection of "critical facilities" of the electric delivery system

is a shared regulatory oversight responsibility of FERC; NERC; the State Commissions, led by the National Association of Regulatory Utility Commissioners (NARUC); and local law enforcement, and;

BE IT FURTHER RESOLVED, that utilities and the National Sheriffs' Association 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 a State comply with such a standard — recognizing that the circumstances and geographies in each State may differ substantially — while coordinating with local law enforcement in ultimately assessing, planning, and implementing a more secure electric grid with the best available and certified solutions, and;

BE IT FURTHER RESOLVED, that the National Sheriffs' Association should endeavor to work with regulated utilities to ensure that the CIP 014 standard is reviewed promptly and in an appropriate forum, in accordance with a cost-benefit methodology used by each agency and Commission.