NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

February 12, 2014

The Honorable Harry Reid
Majority Leader
United States Senate
Washington. DC 20510

Re: February 7, 2014 letter regarding physical security

Dear Majority Leader Reid:

I am responding to your February 7, 2014 letter to NERC and the Federal Energy Regulatory Commission asking us to consider whether additional actions regarding physical security at critical substations and other essential electric facilities are needed to assure the reliable operation of the bulk power system.

Cyber and physical security have long been priorities for NERC and the electricity industry. In the wake of the September 11, 2001 attack, NERC and the industry adopted a broad set of physical security guidelines that have been updated over time and remain in place today. NERC and the industry adopted the first set of cyber security standards in August 2003. The industry employs threat mitigation known as "defense-in-depth" that focuses on preparation, prevention, response, and recovery.

NERC addresses physical and cyber security through guidelines, mandatory standards, outreach efforts and training exercises in coordination with industry and the federal agencies. NERC currently has a mandatory standard requiring reporting to NERC and law enforcement of physical damage or destruction of a facility or threats to damage or destroy a facility (Reliability Standard EOP-004-2).

NERC operates the Electricity Sector Information Sharing and Analysis Center ("ES-ISAC") on behalf of the entire electric industry. ES-ISAC's primary function is the rapid and secure sharing of information with the electric industry and governmental entities regarding real and potential threats to the electricity sector, as well as methods and tools to avoid or mitigate the potential impact from these threats. The ES-ISAC gathers information from the disparate electricity industry participants about security-related events, disturbances, and off-normal occurrences within the electricity sector and shares that information with its partners in the government. In turn, the government provides information regarding risks, threats, and warnings to the ES-ISAC, which then disseminates that information throughout the electricity industry.

Three days after the April 16, 2013 Metcalf substation incident you reference in your letter, the ES-ISAC, after consultation with Commission staff, issued an industry advisory, "Substation Sabotage Incident

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Marks Increasing Adversarial Sophistication," that went to more than 1,900 entities with responsibility for the reliable operation of the bulk power system. As a follow-up, NERC and industry subject matter experts are collaborating with the Department of Homeland Security, the Department of Energy, the Federal Bureau of Investigation, and Commission representatives to bring the lessons learned from the Metcalf incident to utilities and law enforcement officials in a series of outreach sessions across North America. Sessions have been completed in the National Capital Region, Chicago, Denver, Tampa, and Houston. Remaining sessions are scheduled for San Jose, Albuquerque, Seattle, Boston, New York, Ottawa and Toronto in Ontario, and Calgary, Alberta in the next few weeks.

In November 2013 NERC conducted a two-day cyber and physical security exercise involving over 2,000 individuals from 231 industry and government organizations in the United States, Canada and Mexico. NERC designed GridEx II to stress the bulk-power system through a simulated series of prolonged coordinated cyber attacks against certain automated systems used by power system operators. The scenario also included simulated coordinated physical attacks against key transmission substations and generation facilities. The exercise gave participants the opportunity to activate their crisis action plans and assess their response and recovery capabilities, including communicating with industry peers and government organizations. On the afternoon of the second day, NERC involved industry executives from across North America in a tabletop discussion to examine the policy-level issues and decisions that would need to be made to manage the impact of an even more severe national security event impacting public health and safety. The U.S. federal government also participated and was represented by senior officials from the White House, Department of Energy, Department of Homeland Security, Federal Emergency Management Agency, Department of Defense, National Security Agency, U.S. Cyber Command, North American Aerospace Defense Command, U.S. Northern Command, National Guard, Federal Bureau of Investigation, and FERC. Reports detailing the findings and recommendations from the distributed play and executive tabletop exercises will be posted to NERC's website in the first quarter 2014. I would be pleased to make those reports available to you.

Your letter asks that we consider whether additional minimum reliability standards regarding physical security may be necessary. I agree with you that section 215 (added to the Federal Power Act ("FPA") by section 1211 of the Energy Policy Act of 2005) is sufficiently broad to give both NERC and FERC authority to consider reliability standards pertaining to physical security for the bulk power system, including the authority of FERC under FPA section 215(d)(5) to direct that NERC develop a reliability standard addressing physical security matters. However, while NERC has the ability to develop such standards, and to do so in a way that addresses imminent and confidential issues, I do not believe it makes sense to move to mandatory standards at this time. There are more than 55,000 substations of 100 Kv or higher across North America, and not all those assets can be 100% protected against all threats. I am concerned that a rule-based approach for physical security would not provide the flexibility needed to deal with the widely varying risk profiles and circumstances across the North American grid and would instead create unnecessary and inefficient regulatory burdens and compliance obligations.

NERC believes that the significant training and education exercises discussed above have caused industry participants to further enhance their efforts to address physical security issues, and that significant investments are being made to address the risks related to physical and cyber security. For now, I believe the most effective approach in dealing with physical security issues will be the continued engagement of utilities, law enforcement and appropriate government agencies on identifying critical assets and putting appropriate protections and response capabilities in place. NERC will continue its commitment to outreach, education, and facilitating coordination between utilities and law enforcement, emergency response officials and appropriate government agencies to that end, as well as assessing the effectiveness of these efforts consistent with its role as the Electric Reliability Organization.

I assure you that NERC takes physical and cyber security very seriously, and I know the industry does as well. Together we are committed to ensuring the reliability of the North American grid.

Sincerely,

Gerry Cauley
President and CEO

cc: Cheryl LaFleur
Acting Chairman
Federal Energy Regulatory Commission