Department of Energy
Washington, DC 20585

March 14, 2013

Mr. Gerry Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326

Dear Mr. Cauley,

I would like to extend my thanks on behalf of the United States Department of Energy (Department) to you and your staff for your efforts to build the capabilities and resources of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Department recognizes and appreciates the importance of effective and efficient information sharing in an environment with increasing threats to the United States' electric power systems. The Department supports the ES-ISAC's efforts at NERC to enable sector-wide cybersecurity coordination, trust, and engagement among participants, as well as rapid analysis and information sharing with the sector and its partners. These efforts complement those of the Department to ensure that the Energy Sector is reliable, survivable, and resilient in the face of growing challenges.

The Department's vision for the ES-ISAC is to establish robust situational awareness, incident management, coordination, and communication capabilities within the Electricity Sector through timely, reliable, and secure information exchange. Both industry and government need credible, timely, and actionable threat and hazard information to ensure that the most appropriate security investments, programs, and decisions are made to protect sector assets. The ES-ISAC, in collaboration with the Department and the Electricity Sector Coordinating Council (ESCC), should serve as the primary communications channel for the Electricity Sector and enhance the ability of the sector to prepare for and respond to cyber and physical threats, vulnerabilities and incidents. As the designated ISAC of the Electricity Sector, the ES-ISAC is expected to support the protection of the Electricity Sector by assisting both the ESCC and the Department as follows:

- Identify, prioritize, and coordinate the protection of critical power services, infrastructure service, and key resources

- Facilitate sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures and practices

- Provide rapid response through the ability to effectively contact all member companies when required
- Provide and disseminate campaign analysis, which includes capturing the data for historical analysis, correlating it, finding patterns, and sharing that information within the sector
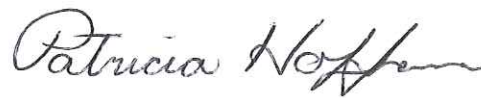
In addition, the ES-ISAC should continue to serve as follows:

- Receive incident data from private and public entities

- Assist the Department, the Federal Energy Regulatory Commission, and the Department of Homeland Security in analyzing event data to determine threat, vulnerabilities, trends, and impacts for the sector, as well as interdependencies with other critical infrastructure. (This includes sitting on the National Cybersecurity and Communications Integration Center floor.)

- Analyze incident data and prepare reports based on subject matter expertise in security and electric power systems

- Disseminate threat alerts, warnings, advisories, notices, and vulnerability assessments to the entire sector

- Maintain a close working relationship with other information sharing and analysis centers to share information and provide assistance during actual or potential sector disruptions whether caused by intentional, accidental or natural events

- Develop and maintain an awareness of private and government infrastructure interdependencies

- Provide an electronic, trusted capability for ES-ISAC participants to exchange and share information on all threats in order to defend critical infrastructure

- Participate in government critical infrastructure exercises

- Conduct outreach to educate and inform sector stakeholders

All of these ES-ISAC activities would be enhanced by efforts to reach a greater percentage of the over 3200 companies in the sector by more clearly disassociating from the compliance arm of NERC. To that end, I support NERC's revised policy statement that clarifies the "firewall" between the ES-ISAC and the NERC Compliance Monitoring and Enforcement Program. This policy statement signals to the Electricity Sector that information shared with the ES-ISAC will not be shared with enforcement staff. It is essential that organizations across the sector trust the ES-ISAC to maintain confidentiality and the revised policy statement should reassure the sector that the ES-ISAC understands the importance of confidential treatment.

The ES-ISAC is poised to serve a vital role within the Electricity Sector to increase the knowledge and understanding of physical and cyber threats that could potentially affect sector operations and grid reliability across the United States. If there is anything that I or my organization can do to support the ES-ISAC, please contact me or Deputy Assistant Secretary William Bryan, William.Bryan@hq.doe.gov.

Sincerely,

Patricia Hoffman
Assistant Secretary
Office of Electricity Delivery and Energy Reliability
U.S. Department of Energy