Department of Energy
Washington, DC 20585

August 5, 2014

Mr. Tom Fanning
Chairman, President and Chief Executive Officer Southern Company
30 Ivan Allen Jr. Blvd, NW
BIN SC1500
Atlanta, GA 30308

Mr. Fred Gorbet
Chairman, Board of Trustees
North American Electric Reliability Corporation
3353 Peachtree Road NE, Suite 600, North Tower
Atlanta, GA 30326

Dear Mr. Fanning and Mr. Gorbet,

The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by the U.S. Department of Energy's (Department) Office of Electricity Delivery and Energy Reliability (DOE-OE) and industry. The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and develop situational awareness tools to enhance the sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure and key resources.

At the June Electricity Subsector Coordinating Council (ESCC) meeting, I was pleased to hear Tom pronounce that NERC and the ES-ISAC must be the center of the CRISP universe. This result is exactly what I hoped would take place. The Department's goal is now to ensure that the architecture is in place, both internally and at the ISACs, to support any company that wants to join CRISP and share cyber threat data. As CRISP transitions from a publicly-funded pilot to a private-sector program, DOE-OE will remain the U.S. Government sponsor, while also transitioning its role in the program. The ISACs will be the industry face of CRISP.

Last March I sent a letter to Gerry Cauley in which I stated:

> *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.

This latest effort to take the industry lead in managing CRISP is further evidence of NERC taking a laudable step to expand its responsibility in the sector and place the public interest ahead of all else. Aggressive bi-directional information sharing, with the significant improvements this brings to situational awareness, represents the epitome of public-private partnership in securing the grid.

The Department's vision for the ES-ISAC is to establish robust situational awareness, incident management, coordination, and communication capabilities within the Electricity Subsector through timely, reliable, and secure information exchange. The ES-ISAC, in collaboration with the Department and the ESCC, should serve as the primary communications channel for the Electricity Subsector and enhance the ability of the sector to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

The ES-ISAC is poised to serve a vital role within the Electricity Subsector 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 else that I or my organization can do to support the ES-ISAC, please contact me or Mike Smith (Michael.smith2@hq.doe.gov).

Sincerely,

Patricia Hoffman

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