



**Joint Statement for the Record by the
AMERICAN PUBLIC POWER ASSOCIATION (APPA) and the
NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION (NRECA)**

**Submitted to the
HOUSE ENERGY AND COMMERCE SUBCOMMITTEE ON ENERGY
For the February 1, 2017, Hearing on
“The Electricity Sector’s Efforts to Respond to Cybersecurity Threats”**

The American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) appreciates the opportunity to submit a statement for the record for the House Energy & Commerce Committee’s Subcommittee on Energy hearing on “The Electricity Sector’s Efforts to Respond to Cybersecurity Threats.” APPA and NRECA supports and agrees with the testimony of Mr. Scott Aaronson of the Edison Electric Institute.

The electric power grid is a complex, interconnected network of generating plants, transmission lines, and distribution facilities. The electric power industry continuously monitors the bulk electric system and responds every day to events large and small. Consumers are rarely aware of these events primarily because of the sector’s system operation expertise, planning, coordination, response, and resiliency activities. Protecting the nation’s electric power grid and ensuring a supply of safe, reliable, and affordable electricity is a top priority for the electric power industry.

The electric power industry employs threat mitigation known as “defense-in-depth” that focuses on preparation, prevention, response, and recovery to a wide variety of hazards to electric grid operations, including natural events, such as severe weather or geomagnetic disturbances (GMDs) caused by solar storms, as well as malicious events such as physical or cyberattacks directed at the grid.

The Energy & Commerce Committee developed important grid security provisions in the comprehensive energy bill that were ultimately passed into law as part of H.R. 22, “Fixing America’s Surface Transportation Act” (“FAST Act”). These provisions included establishing DOE as the sector-specific agency (SSA) for the electric utility industry, giving DOE authority to direct industry to take action in the event of a grid security emergency, protecting critical electric infrastructure information (CEII) from public disclosure and devising a plan for a spare transformer program. We appreciate and applaud the hard work that went into moving these issues forward.

The electricity sector continuously strives to improve on its history of protecting its assets from security threats, including longstanding programs and protocols designed to protect utility systems. Key to reliability efforts are the crisis management and site-specific security plans developed by electric utilities to ensure that operations and infrastructure systems are properly supported. In addition, a number of redundancies are built into the system, in many cases allowing utilities to re-route power around damaged facilities. Utilities also partner with federal, state/provincial, and local government and law enforcement agencies in both the United States and Canada to ensure that they can respond effectively to any event that may impact their operations.

To maintain and improve upon the high level of reliability consumers expect, electric cooperatives, public power utilities, and investor-owned utilities all work with each other and the North American Electric Reliability Corporation (NERC), the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC) on matters of critical infrastructure protection – including sharing needed information about potential threats and vulnerabilities related to the bulk electric system.

In 2013, the electric utility industry reorganized the Electricity Subsector Coordinating Council (ESCC) to ensure high level engagement. The new ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC includes utility CEOs and trade association leaders representing all segments of the industry. Their counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

The electric sector and its subject matter experts will continue to partner with government agencies like DHS, DOE, and FERC on matters of critical infrastructure protection to improve physical and cyber security for its assets. It is important to note, however, that to help maintain operational security, the industry is careful not to publicize clearly sensitive information about critical infrastructure that might provoke new threats or endanger the safety and well-being of the North American public or the integrity of the electric power grid.