Question for the Record, in connection with May 21, 2013 full Committee hearing
Submitted by NRECA on behalf of Duane Highley

Question posed by: Rep. Anna G. Eshoo

Question: **If you could ask Congress to address one unfinished piece of business relative to cybersecurity, what would it be?**

Response:

Thank you for your question. If we could ask Congress to pick up the ball and get it into the touchdown zone on one component of cybersecurity legislation, it would be information sharing. That phrase gets over-used to the point it has lost its meaning, but still, as a representative of a privately-owned business that owns and operates critical assets in the Bulk Electric System, I can tell you that we aren't yet to the point where there is "real-time collaboration" among government and industry. We want and need to get there but it will take building trust, collaboration, many conversations, and more clearances.

The risks and potential impacts are very different for public-facing elements of a utility's Internet-connected business systems, versus their industrial control systems, which typically are not Internet-connected, or if they are, they are protected with more aggressive security schemes. Given that millions of attempted cyber-attacks occur daily on our public facing sites, utilities will need to rely upon assistance from governmental authorities, particularly in the form of helping to identify threats as well as threat trends.

Much of the information needed to fully understand the nature of the cyber threats faced by our industry is classified at a level that is unavailable to our organizations. The DHS Private Sector Clearance Program (PSCP) has helped key electric utility staff obtain security clearances, which allow them access to basic information about such threats. However, a recent shutdown of the PSCP created a substantial backlog in the processing of clearance applications, and hampered the industry's access to important information. Processing of these applications has now resumed and we hope we can continue to expand our access to needed information. We also need a limited number of electric industry personnel to obtain top-secret "SCI" clearances, which are not typically provided by the PSCP; this would help immensely in achieving "real-time collaboration."

In addition to expanding the number of utility personnel with clearances, it is critical that government agencies regularly share clear, actionable information with industry personnel in cleared briefings. Our employees can be counted on to take the steps necessary to protect our systems – if they understand the nature of the threat against them. Effective information sharing should take the form of a timely and efficient mechanism to pass along threat data, warnings, and trend information. Examples of the kinds of information we need are: signatures of known viruses and malware; points of origination for known threat actors; known behavioral techniques of anonymous threats such as "Advanced Persistent Threats" (APT); information regarding potential vectors for introduction of cyber threats, such as counterfeit parts and software; and the sharing of best practices or policies to combat or defeat emerging threats and vulnerabilities.