Response to U.S. Department of Commerce – Incentives To Adopt Improved Cybersecurity Practices Notice of Inquiry
April 30, 2013
Southern California Edison

Southern California Edison (SCE) appreciates the opportunity to participate in this process. SCE, a regulated electric utility, is one of the largest electric utilities in the nation, serving more than 14 million people in a 50,000 square mile area of central, coastal, and Southern California. SCE has been providing electric service in the region for 127 years and has a service territory that includes more than 180 cities.

Both Edison Electric Institute (EEI) and the Utilities Telecom Council (UTC) have submitted responses that raise good points for the U.S. Department of Commerce's consideration. SCE is responding independently to provide additional comments in the following areas.

(1) **Threat information-sharing raises awareness, which encourages cyber protection investment**. **In addition, low-cost cybersecurity protection solutions increase the likelihood of adoption.**

Government led cyber intelligence sharing programs, such as the Department of Defense (DoD) Defense Industrial Base (DIB) network, and the Department of Homeland Security (DHS) Enhanced Cybersecurity Services (ECS) program, provide companies with sensitive and classified cyber threat information. These programs can be very low cost for participants as well. By focusing on threat information-sharing through participation in these programs, the need for cybersecurity protection investments will be promoted. The DoD DIB network appears most relevant for companies with critical infrastructure and greater risk profiles, while companies with lesser risk profiles could benefit by participating in the DHS ECS program.

(2) **Vendors selling products in the critical infrastructure space should adhere to cybersecurity standards that enable interoperability and drive desired security levels**.

Some vendors' products are more secure than others', yet sharing information about product weaknesses cannot be easily achieved. Numerous legal constraints exist. One way to ensure that strong security reaches companies with critical infrastructure is to require vendors' products to adhere to specific security and interoperability standards. This would raise the security threshold across the nation.

(3) **Identify multiple ways that companies can claim Cybersecurity Framework participation.**

Due to the diversity across industries, and the diversity among companies within an industry, flexibility to address threats is crucial. By identifying a variety of ways that can suffice as Cybersecurity Framework participation, approaches to cyber security remain flexible.

For example, complying with NERC CIP standards might be considered Cybersecurity Framework participation. Another example of participation might be successful results from cyber audits performed by independent third parties.