December 13, 2013
Attention: Mr. Sedgewick
From: Southern California Edison
RE: Request for Comments on the Preliminary Cybersecurity Framework

Southern California Edison (SCE) appreciates the National Institute of Standards and Technology (NIST) efforts to bring large and small entities within the critical infrastructure sectors to a common ground of cybersecurity practices and principles. We believe that all critical infrastructure companies could use the Cybersecurity Framework (Framework) as a starting point to develop or improve upon their existing cybersecurity programs.

SCE has participated in the NIST workshops, collaborated with Edison Electric Institute (EEI) on its comments, and is providing written feedback on the Framework to emphasize or supplement EEI's points.

SCE completed the NIST template with more detail, but the following points are worth highlighting:

- The Framework needs to clarify its scope, and explain how users should evaluate risk and apply risk management within the Framework. The focus should be on risks relevant to critical infrastructure. Adopting a broader scope could dilute valuable resources and make the Framework less effective. Clearly defining the Framework's scope can also assist in how the risk management process will be used.
- The Framework should provide additional implementation guidance and define the roles of legislators and regulators with respect to the Framework. If state legislatures and regulators begin to independently address cybersecurity concerns inconsistently, the lack of cohesion could have the effect of reducing our nation's overall defenses.
- The December 4, 2013 "Update on the Development of the Cybersecurity Framework" stated that the discussion at the Raleigh Workshop resulted in a "general consensus" for a particular definition of Framework "adoption." However, it is unclear what general consensus was reached, other than a concern that the term was not well defined.
- In Appendix E, the Framework should clarify that each entity should use definitions such as Personal Identifiable Information (PII) already approved by applicable state law. Creating a new definition could be detrimental and more confusing. As a good example, reference an approved definition that is specific in its terms.
- Implementation Tiers should have a progression path that meets certain objectives in order reach a more mature tier.

Please refer to the NIST template for more detailed comments, which also includes the points above.