Opening Statement of Douglas R. Bauder
Southern California Edison

Federal Energy Regulatory Commission ("FERC") Technical Workshop

To the FERC Commission and staff, thank you for providing me with this opportunity to testify on behalf of Southern California Edison Company ("SCE") about electric utility supply chain risk management and current supply chain risk management practices.

As the Chief Procurement Officer and Vice President of Operational Services, Safety, Security, and Business Resiliency for Southern California Edison, I am familiar with the supply chain risk management issues identified by the Commission in its Revised Critical Infrastructure Protection Standards Notice of Proposed Rulemaking (NOPR) issued last year. In that NOPR, the Commission proposed to direct NERC to develop a mandatory reliability standard to address supply chain management for industrial control systems. Citing a variety of Federal government reports, the Commission asserted that there is a lack of security controls for managing supply chain risk to industrial control system hardware, software, and associated bulk electric system (BES) computing and networking systems.

Cybersecurity is an issue of paramount concern to SCE, and we devote considerable time and resources to protect the grid from cyber-attack. SCE shares the Commission's goal to enhance the safe and reliable operation of our electric grid. However, as I will discuss today, SCE believes development of new regulatory requirements or standards focused on supply chain issues would not assist in achieving that goal.

SCE shares the Joint Trade Associations'[1] view that there is no regulatory gap to be filled relating to supply chain cybersecurity. That issue was amply discussed in comments filed by the Joint Trade Associations to the NOPR on September 21, 2015. That said, SCE acknowledges that the Commission has expressed generalized concerns about supply chain cybersecurity risks that should be addressed. To that end, SCE believes that the CIP Version 5 framework, recently approved by the Commission, was designed to address and mitigate the various new and evolving threats. For example, the existing CIP-010 Cyber Asset Change Management controls require extensive testing and vulnerability assessments prior to connecting a system or device to the bulk electric system. The existing NERC CIP Standards also require entities such as SCE to develop prudent and effective vendor risk management processes. For example, CIP-011 includes information protection controls, and CIP-004 includes vendor personnel risk assessment and access management controls. Thus, entities such as SCE are already required by the NERC CIP Standards to manage supply chain risk, including those risks introduced by third party vendors. There is not a lack of security controls for managing supply chain risk.

In addition to the NERC CIP standards, understanding and managing the levels of risk from our diverse supply chain is an important part of our operating strategy. SCE expects each of its suppliers to deliver products and services that will not introduce threats to its environment and protect all SCE information that a supplier may have access to or generate in the course of doing business. We implement these expectations through a number of practices and protocols, including:

- Segmentation of suppliers based on a well-developed set of criteria and risk factors (e.g., safety, service reliability, financial capacity, environmental, and compliance);

[1] The Joint Trade Associations consist of: Edison Electric Institute, American Public Power Association, National Rural Electric Cooperative Association, Electric Power Supply Association, Electricity Consumers Resource Council, Transmission Access Policy Study Group, and the Large Public Power Council.

- Implementation of comprehensive supplier qualification and onboarding procedures for new and existing suppliers (e.g., Supplier Registration and Qualification, Information Governance Classification and Access Procedure, Vendor Solution Request Process);

- The use of cross-functional team evaluations and vendor risk assessments of various procurement efforts, grid related or otherwise (with participation from Supply Chain Management, IT, T&D, Legal, Enterprise Risk Management, and other stakeholder personnel); and, importantly,

- Inclusion of cybersecurity procurement language and contract protections in third party supplier contracts, including requirements for suppliers to undergo and successfully complete SCE's Computing System Access Security Audit and Review. As part of this review process, suppliers provide SCE with sufficient documentation to indicate the manner in which security of a supplier's information systems and facilities comply with applicable standards and relevant SCE policies; finally,

- Conducting regular contract administration (e.g., supplier scorecards and performance metrics) and contract close out activities.

These practices, and the existing NERC CIP Standards, provide utilities with the flexibility to remain versatile and effective in meeting the evolving supply chain cyber security threat landscape.

Next, SCE is concerned that the development of new regulations focused on supply chain management could have unintended consequences that end up hindering, rather than helping, entities protect the grid. For example, I have seen, first-hand, the impacts of some of the most restrictive supply chain regulations, in other fields, and fear that the adoption of such restrictions over all electric utilities will not address the concerns the Commission raised in the NOPR and could have far worse secondary impacts upon our electric utility sector.

For example, imposition of Nuclear Regulatory Commission (NRC) style regulations may drastically limit the base of suppliers available to electric utilities and stifle the innovation required to provide the security and reliability that the Commission seeks. This is not a theoretical concern. Compliance with the NRC procurement regulations model (specified in 10 CFR Part 50 App B) is expensive for vendors, and requires expertise in a specialized set of regulations that apply to a limited vendor base.

Thus, a few select vendors take on the burden to meet the requirements, and many choose, instead, to forego the market of NRC-regulated customers. This type of procurement regulation model stifles and constrains further developments in the field due to increased development costs for any cyber security solution applicable to electric utility systems in the United States. This means entities such as SCE could be forced to select protective equipment and systems from a small pool of offerings, rather than from a much larger pool.

The small size of available vendors in a very highly regulated environment also imposes operational and cost burdens onto entities such as SCE and their ratepayers. Those vendors that do adopt the regulatory burden increase their costs accordingly, to cover the added administrative controls. Those costs would, if a similar model were adopted as part of the CIP Standards, be passed along the electric utilities and, in turn, their consumers.

With these two concerns in mind, SCE's respectful recommendation to the Commission in this proceeding is as follows: First, the Commission should reconsider its proposal to develop new regulations focused on supply chain management. The existing NERC CIP standards already address the generalized concerns expressed by the Commission. Further, development of new requirements may hinder, rather than help, utilities from pursuing additional risk management efforts and new technologies that may protect the grid.

Next, SCE proposes the Commission encourage utilities to continue to identify and develop supply chain related cybersecurity best practices for possible, but not mandatory, use. For example, as cited by the Commission in the NOPR, the National Institute of Standards and Technology (NIST) has published supply risk management practices that provide entities, such as SCE, guidance and options for tailoring and implementing practices. However, because one size does not fit all, entities must be free to use, modify or not use, these practices to fit their own unique requirements. Similarly, the Department of Energy (DOE) published a set of cybersecurity procurement language that provides a starting point for entities to use when acquiring energy delivery systems or components.[2] Use of this DOE publication is voluntary and entities such as SCE are free to utilize the information provided by the DOE guidance to enhance their own cybersecurity supply chain practices.

SCE recognizes that the cyber related threats to its industrial control systems are constantly evolving. We remain vigilant and committed in implementing varied and heightened security measures, both physical and electronic, to ensure the reliability and protection of the grid. As such, we continue to monitor risks and take actions, as other utilities do, to address those risks introduced through the supply chain.

Thank you.

[2] DOE Cybersecurity Procurement Language for Energy Delivery Systems.