December 1, 2009

Annabelle Lee
National Institute of Standards and Technology
100 Bureau Dr., Stop 8930
Gaithersburg, MD 20899-8930


Dear Ms. Lee:

Thank you for the opportunity to provide these brief comments in the above-referenced docket. Schweitzer Engineering Laboratories, Inc. (SEL) is a U.S.-based manufacturer of products used in electric power systems around the world. SEL became the original “smart grid” manufacturer in 1984 when SEL’s founder, Dr. Edmund O. Schweitzer III, invented the world’s first digital relay. SEL’s mission is Making Electric Power Safer, More Reliable, and More Economical®. We deliver on this mission every day by developing and supporting intelligent products designed to meet power system demands such as increasing integration of distributed and intermittent sources of generation and optimizing asset utilization.

SEL actively participates in technical forums and activities, including standards development work and working with NIST on the Cyber Security Coordination Task Group (CSCTG) to develop the draft NIST Interagency Report 7628 (NISTIR). SEL places a high priority on cybersecurity and is actively engaged in developing security solutions that support the demanding safety and reliability requirements of today’s electric infrastructure. SEL believes that the NISTIR is an important opportunity to provide guidance to utilities implementing a wide range of grid modernization projects, and appreciates the enormous commitment of time and resources by NIST and our industry and government colleagues that this draft represents.

SEL believes that the primary objective of the NISTIR is to improve the overall security of the electric grid as utilities proceed with implementing smart grid projects. The NISTIR will best serve this objective by being clear and easy-to-use for the utilities implementing those projects, and by serving as a framework to facilitate discussions between utilities and their smart-grid suppliers. Utilities and their suppliers should, then, be the primary audience of the document.

Attached are SEL’s recommendations for making the NISTIR clear and easy-to-use for this audience. SEL looks forward to continuing to participate in the development of the NISTIR. Should you have questions, please contact me at laura_hussey@selgs.com or at 703-647-6248.

Sincerely,

/Laura L. Hussey/

Laura Hussey, Director of Government Affairs – Cybersecurity Policy
SEL Recommendations for Draft NISTIR 7628

SEL has participated in the CSCTG and subgroups of the CSCTG, and has provided specific technical comments within those groups. Therefore, the following recommendations are limited to suggestions on organization and scope, with the intent of making the NISTIR more useful to electric utilities and their smart grid suppliers.

1. **Incorporate a brief user guide to make the NISTIR more approachable.** The user guide could take many forms, but one suggestion is to provide one or more step-by-step guide(s) to illustrate how it could be used by utilities and their vendors. Another possibility is a decision tree that directs the reader to the relevant portions of the document for information. It will also be helpful for the user guide to state that there is no single “one-size-fits-all” security solution; and that each project needs to be evaluated individually to incorporate appropriate security controls.

2. **Add a paragraph or two in section 1.2 or 1.3 that puts cybersecurity into its appropriate context in electric power systems, which is as a component of power system reliability, and something that must support safety and reliability but should not compromise either.** Cybersecurity in the context of power systems is different than cybersecurity of corporate networks and other IT systems. Electric utilities are accountable for power system safety and reliability, and cybersecurity of power systems must always be placed into that context. Because not all of the readers of this document will have this fundamental knowledge, such a discussion is important to avoid misinterpretations of the material and to ensure that all stakeholders have a common frame of reference for the recommendations in the NISTIR.

3. **The scope of the document should be limited to recommending cybersecurity controls for the smart grid applications we know of today (by listing the use cases). The “Overview” section (currently section 1.1) of the final document should define the scope of the document.** A clearly defined scope will help set the reader’s expectations, and will also help the authors of the document by reducing the inclination to try to be exhaustive. There is a psychological barrier associated with a 200-plus page document. Bearing in mind how the document will be used by utilities and smart grid suppliers, NIST should resist being exhaustive in scope, in favor of being sufficiently clear within the scope described above. Anything that reduces barriers to using the information in the NISTIR, including increased clarity and manageable volume, will likely be helpful to improving cybersecurity.

4. **Be explicit in the Overview about indicating that the document is not exhaustive, and about deliberately excluding certain topics, such as physical security.** Given that one of the policy objectives of EISA is innovation, it is possible that new interfaces, categories of interfaces, as well as impacts and constraints may arise, while other categories, constraints, and impacts may diminish in importance. Neither NIST nor any of the stakeholders involved in writing the NISTIR can foresee every security consideration that may arise, and therefore, the NISTIR is limited to describing recommended security considerations and appropriate controls to be considered for 18 (?) categories of interfaces that we believe capture the vast majority of smart grid projects envisioned today.

5. **Consider removing Chapter 2 (on Privacy) from this NISTIR and creating a separate NISTIR or other document to address smart grid privacy considerations and recommended approaches.** SEL believes that trying to address both cybersecurity and privacy in a single report creates the potential to delay important guidance on cyber security for aspects of smart grid architecture that do not involve customer data, and do not, therefore,
invoke privacy concerns. Utilities implanting smart grid projects with ARRA funding need to have cybersecurity guidance in hand as soon as possible in order to ensure that they are fulfilling their obligations under the terms of the DOE grants.

In addition, inclusion of the privacy chapter adds to the volume of the NISTIR, potentially making the document more challenging to use as guidance for the intended audience. Two separate, authoritative reports, each with a clear focus, would likely be more user-friendly.

6. **Consider other ways to make the document more concise.** One possibility for reducing the volume of the document without reducing the content would be to remove the use case diagrams and associated lists categorizing the logical interfaces for each use case, and instead provide a single listing of the categories of logical interfaces with a detailed list of examples for each category, might reduce the redundancy of the document.

7. **Think about ways to create useful job aids for the primary utility and smartgrid supplier audiences.** For example, the cross-walk in Appendix B is a useful reference that may lend itself to printing separately. Any future formatting of the NISTIR should be done to ensure that a user of the NISTIR could easily print the crosswalk as a handy reference. In addition, there may be other