Landis+Gyr

manage energy better

April 1, 2013

TO: Diane Honeycutt,
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

RE: Developing a Framework to Improve Critical Infrastructure Cybersecurity

COMMENTS OF LANDIS+GYR COMPANY

Landis+Gyr Company ("L+G") submits these comments to the National Institute of Standards and Technology (NIST) in response to the NIST Request For Information (RFI) "Developing a Framework to Improve Critical Infrastructure Cybersecurity" issued on Feb-26-2013 under Executive Order 13636. The RFI solicits comments to help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop the Framework (hereafter "Framework").

L+G is a leading provider of integrated energy management solutions tailored to energy company needs. With a global presence and a reputation for quality and innovation, L+G is unique in its ability to deliver true end-to-end advanced metering solutions. Using a combination of Part 101 Multiple Address System licenses and unlicensed spread spectrum Part 15 devices, L+G has deployed a low-cost, private internal telemetry services network that allows it to transmit and receive data for the remote monitoring and control of devices, primarily utility meters and grid management devices in the energy sector.

Landis+Gyr comments below on the specific items that are most relevant to our Critical Infrastructure products, services and expertise in grid management.

Landis+Gyr

manage energy better

COMMENTS OF LANDIS+GYR COMPANY ON:

Current Risk Management Practices

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

In Landis+Gyr's view, this question is rather broad and may not receive a consensus answer. However, we do feel a response on a specific aspect of our business may be useful. Landis+Gyr strongly believes energy distribution critical assets are complementary (not necessarily interdependent) with information technology assets. For example, DA or SCADA grid management applications do not require Advanced Metering Infrastructure (AMI) that is in the Information Technology and/or telecommunications realms. However, AMI can also be implemented in an interdependent fashion with DA or SCADA to give the utility a much clearer picture of what is happening with the DA or SCADA equipment.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

L+G recommends that such organizations follow an open-standards approach in the Framework to allow full review and conformity assessment by the Energy sector to promote highest levels of cyber-security. Once robust security standards are available publicly and ratified, this removes barriers for all companies to efficiently improve their physical and logical security while allowing technical innovation to continue. Private mechanisms exist to ensure systems comply with such standards (e.g., Penetration Testing). Further inter-operability must be factored into the Framework to reduce implementation and operations costs.

Landis+Gyr

manage energy better

COMMENTS OF LANDIS+GYR COMPANY ON:

Use of Frameworks, Standards, Guidelines, and Best Practices

This section intentionally left blank.

Landis+Gyr

manage energy better

COMMENTS OF LANDIS+GYR COMPANY ON:

Specific Industry Practices

1. Are these practices widely used throughout critical infrastructure and industry?

- Separation of business from operational systems – Yes
- Use of encryption and key management - Yes
- Identification and authorization of users accessing systems - Yes
- Asset identification and management - Yes
- Monitoring and incident detection tools and capabilities - Yes
- Incident handling policies and procedures - Yes
- Mission/system resiliency practices - Yes
- Security engineering practices - Yes
- Privacy and civil liberties protection - Yes

2. How do these practices relate to existing international standards and practices?

Landis+Gyr believes the items above are each examples of existing energy-sector standards and practices. There are opportunities to improve cybersecurity practices in domestic and international standards to reduce vulnerabilities to Critical Infrastructure. Further, our international customers will be directly affected when Framework details ultimately become product features. Therefore, we advise an open stance to encourage international review and adoption of the Framework.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

There is readily available and abundant information on standards and guidelines utilized in the Energy sector. As an example, the SGIP 2.0 serves as a private thought-leader to clarify standards and guidelines for the energy sector.

Landis+Gyr strongly believes in leveraging existing standards and guidelines for IT operations and security practices. Many other industries are dealing with similar concerns and have developed standards that address many of these issues (e.g., HIPPA, PCI Compliance).

For example, currently our Network Operations Center adheres to best practices from SAE16. Additionally, this operations center is currently implementing ITIL guidelines with substantial completion expected in early 2014. Finally, although not required to be compliant, many of the NISTIR recommendations have been incorporated within our operations. These standards and guidelines influence our practices in the following areas:

- Consistent, repeatable operations processes with clear ownership coupled with annual evaluation for suitability going forward.

- Protecting the company and its assets.
- Management of risk through identification of assets, classification of sensitive data and threat discovery practices.
- Confidentiality – ensuring that there is the necessary level of secrecy enforced in the data processing and taking preventative measures for unauthorized disclosure of that data.
- Data Integrity – assurance of accuracy and reliability of data provided and prevention of unauthorized access or modification to that data.
- Availability – reliability and timely access to resources and data for authorized persons.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Landis+Gyr, as well as others in the industry, have adopted such methodologies. Further, Landis+Gyr strongly believes organizations should use existing models for the proper allocation of resources to invest in, create, and maintain IT standards.

For example, as mentioned elsewhere in our response, Landis+Gyr has made a significant investment in and commitment to ITIL. 10 leaders in our Customer Operations division are certified at multiple levels of ITIL expertise.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Landis+Gyr strongly believes organizations should have an escalation process in place to address cybersecurity risks that increase in severity. Examples of such escalation models are part of the COBIT model and Landis+Gyr has formal ISO documented process and procedures around this type of activity.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

Privacy is of the utmost importance when dealing with any kind of personal data whether from an end user's data, or from an operator of the grid. In any case, the best way to protect privacy of data is to keep it at its source. Landis+Gyr believes that for purposes of grid operation and grid optimization there should be deep thought as to what private data is required in order to guarantee the best operation of the grid while minimizing intrusion upon people's privacy. The mode of operation should be to limit to the very minimum, at all levels, the collection, transport and storage of personal data. It is for the regulator to define that minimum set and it is for technology to offer the right solutions to collect, transport and store that data with the best possible protection.

Even after defining a minimum data set, there are still significant risks that consumers who are the source of such data (e.g., electricity usage load profile) will see such data as a violation of civil liberties. In such cases, the American Council for an Energy Efficient Economy (ACEEE) has noted in recent report that a best practice is to ensure consumers have greater access to their data and to ensure consumers decide whether such data is made available to third parties either to help the consumer save on their energy costs or for any other commercial purposes.

10. What are the international implications of this framework on your global business or in policymaking in other countries?

This Framework, if adopted in the US, will definitely contribute to global adoption. We believe that NIST should also look outside the US for implications of the new Framework as well as leverage other Frameworks from outside the US.

11. How should any risks to privacy and civil liberties be managed?

Landis+Gyr strongly believes in following industry standard practices to protect privacy and civil liberties. The following are examples of specific steps to manage such risks:

- Identify, document, and review all protected information that is collected for its sensitivity
- Implement adequate cybersecurity measures to safeguard information
- Institute data accuracy, quality and retention procedures
- Establish privacy guidelines to be achieved through business process, technology and training ensuring authorized access to specific data sets.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the framework?

Landis+Gyr recommends considering the following additional items in the Framework:

Cybersecurity Metrics – Define Framework metrics and practices for gathering such metrics on attacks and vulnerability mitigation efforts.

Attack Communication and Response Coordination – Define a Framework mechanism for secure communication to Security professionals in similar sector companies of ongoing or past attacks to improve mitigation and overall respons