May 28, 2010

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

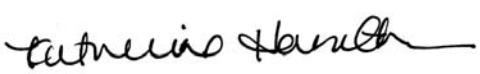
Dear Ms. Lee,

The GridWise Alliance appreciates the opportunity to provide comments on the second draft NISTIR 7628 document. These comments were developed in a consensus process by members of the GridWise Alliance's Interoperability and Cybersecurity Work Group.

We hope that NIST will continue to view the Alliance see as a resource on smart grid cybersecurity and interoperability issues and in developing the NISTIR 7628 final document is finalized. The GridWise Alliance members, as you know, are invested in smart grid and want to assist NIST in any way possible to ensure a successful outcome to the Interoperability Standards process.

Please contact me should you have any further questions regarding our comments. Thank you for your consideration.

Regards,



Katherine Hamilton
President, GridWise Alliance

1155 Fifteenth Street, NW Suite 500 Washington, DC 20005 Phone (202) 530-9740 Fax (202) 530-0659
www.gridwise.org

GridWise Alliance
Comments on the NIST Interoperability Report (NISTIR 7628)

Comment Number: 01	Submitted by: GridWise Alliance, Katherine Hamilton, President	Comment Type: _X_ Tech. __ Editorial __ Gen.

Reference: Executive Summary /Chapter 1	Comment
	The Executive Summary and/or Chapter One would be improved by including language that addressed the following technical issues:
	Rationale/Recommendation
	Convergence of Standards – In order for the industry to move forward with confidence and the necessary speed, it is important that the activities of various government and non-government standards development organizations converge with respect to cyber security. The NISTIR should contain language promoting the coordination of the 7628 document with NERC CIP, IEEE standards, and others to clarify the responsibility for the baseline requirements and specifications, and the basis for the ultimate certification/verification process. *Defense in Depth* – Given the complexity of the electric power grid and the communications/control infrastructure, no single requirement can fully assure protection of a critical element. Using a concept of layers of security, also known in the industry as 'Defense in Depth', a combination of requirements provides a reasonable assurance of sufficient protection. If a single security element failed, a backup or redundant requirement provides a secondary level of protection. In the nuclear power industry, this concept is extended to include "qualified isolation devices", used to limit the jeopardies posed by interfaces between critical safety functions and less critical systems and devices. Other protective measures such as independence, diversity and redundancy are selectively applied to mitigate specific event or failure scenarios. *Matching Requirements to Severity of Consequences* – Different elements of the grid, while still defined as critical, may have a different level of functional importance in the operation of the overall system. Requirements need to be based on graded levels of functional importance such as: • Protecting the integrity of the Bulk Transmission System • Protecting single components (such as substations) with large impact on the distribution system

Comment Number: 01	Submitted by: GridWise Alliance, Katherine Hamilton, President	Comment Type: _X_ Tech. __ Editorial __ Gen.

- Restoring power to customers as soon as possible
- Restoring market functions as soon as possible after an immediate contingency has been mitigated

Matching Requirements to Likelihood of Event – Relative likelihood of events as opposed to other equivalent threats and alternative methods of mitigation are also considerations which should be included:

- A disgruntled employee in an Energy Control Center or Substation could alternatively initiate physical rather than cyber damage
- Component failures, particularly on radial portions of the power systems, may have a much higher probability of failure than the likelihood of their susceptibility to a cyber attack
- Physical multiple simultaneous attacks are also possible on many of our existing infrastructures that are widely geographically deployed (water, oil and gas as well as electric infrastructure)

Defining Audience and Use of the Document – The NISTIR will be used by a number of constituent groups and stakeholders, each of which may have overlapping but different perspectives and objectives. The document should set out the target audience and the objectives and intended use of the NISTIR for each. As an example, the following audience categorization may be helpful.

- *Utilities/asset owners/service providers* – may use the NISTIR 7628 as guidance for a specific cyber security implementation, normally relying on some combination of technological and physical or compensating controls and alternative approaches to meet the objectives and requirements specified.
- *Industry/smart grid vendors* – may base product design and development, and implementation techniques on the guidance provided by the NISTIR, ensuring that smart grid component technologies, when implemented properly, meet the objectives and requirements specified.
- *Regulators/policy makers* – may use the NISTIR as guidance to inform legislative and regulatory decisions and positions, ensuring that governing directives are aligned with appropriate power system and cyber security needs.

It is important that the NISTIR state clearly for all users that it defines the goals and requirements for cyber security, providing for flexibility in solutions to meet those goals and requirements, as necessary to satisfy the specific business context of the user. The NISTIR should identify what must be addressed, without prescribing how it is to be implemented. The NISTIR should

Comment Number: 01	Submitted by: GridWise Alliance, Katherine Hamilton, President	Comment Type: _X_ Tech. __ Editorial __ Gen.

also explicitly recognize the need for each utility's implementation of cyber security controls to evolve as warranted by changes in technology and systems as well as changes in techniques used by adversaries.

Practicality of Implementation – The NISTIR should explicitly encourage a pragmatic approach to implementation, recognizing that the grid itself, to a greater extent than many other infrastructures, has additional methods of coping with events of different geographic size, severity and scope:

- Special protection features
- Special operating modes, in anticipation of or response to significant emergency events or anomalous system conditions
- Mobile transformers and generators
- Excess capacity for large portions of the year and the day

The smart grid itself could be used to further expand and make these alternatives even more robust with features such as:

- Anti-cascade protection,
- Islanding capabilities,
- Tie-line protection,
- "Life line" throttling or reduction of electric service to assure continuity of a minimum level of electric service

All of the above considerations should be included in developing the overall strategy and requirements for a specific power system as it moves over time to broader applications of cyber assets and smart grid functions. (Note: this comment may best be applied only in Chapter 1.)

Disposition (for SGIP-CSWG use)

Comment Number: 02	Submitted by: Katherine Hamilton, President, GridWise Alliance	Comment Type: __ Tech. _X_ Editorial __ Gen.

Reference:	
Page 8, 2nd paragraph, first line and page 8, Chapter One, Cybersecurity Strategy, 2nd paragraph, line 1	**Comment**
	The basic requirement that "Cybersecurity must address… deliberate attacks… from disgruntled employees…" sets a high threshold for security.
	Rationale/Recommendation
	A separate concern for "multiple simultaneous" cybersecurity attacks from one or more remote locations is driving the current NERC-CIP revision. Although there is some possibility that a disgruntled employee could take part in a coordinated attack that included multiple simultaneous remote cybersecurity attacks, there is a much lower probability and risk of this specific compound event than the likelihood of either of these two event scenarios taken separately. This should be reflected in the application of requirements.
	Disposition (for SGIP-CSWG use)

Comment Number: 03	Submitted by: Katherine Hamilton, President, GridWise Alliance	Comment Type: __ Tech. _X_ Editorial __ Gen.

Reference:	
Page 1, Cyber Security Strategy For the Smart Grid, line 2	**Comment**
	"… mitigation strategy that also ensures interoperability…".
	Rationale/Recommendation
	Interoperability is needed to assure ease of interconnection now and overtime as the smart grid evolves, but it is not inherently part of cybersecurity.
	Disposition (for SGIP-CSWG use)

Comment Number: 04	Submitted by: Katherine Hamilton, President, GridWise Alliance	Comment Type: __ Tech. _X_ Editorial __ Gen.

Reference:	Comment
Page 4, Continuation of Top-down analysis from page 3, line 3 and page 15, last paragraph	"What are "script-kiddies?"
	Rationale/Recommendation
	Please include description in Appendix F, Glossary and Acronyms
	Disposition (for SGIP-CSWG use)

Comment Number: 05	Submitted by: Katherine Hamilton, President, GridWise Alliance	Comment Type: __ Tech. _X_ Editorial __ Gen.

Reference:	Comment
Page 5, Privacy Impact Assessment	The needs for addressing and balancing requirements driven by Privacy (customer information protection) versus Reliability (power system operational integrity) are fundamentally different, as are the methods that could be used to mitigate these two concerns through cybersecurity requirements, compensating security requirements or other alternative measures.
	Rationale/Recommendation
	They therefore should be segregated for separate evaluation and treatment rather than being similarly used as a common either/or driver for a high or medium level of cybersecurity requirements.
	Disposition (for SGIP-CSWG use)

Comment Number: 06	Submitted by: Katherine Hamilton, President, GridWise Alliance	Comment Type: __ Tech. _X_ Editorial __ Gen.

Reference:	Comment
Page 5, Task 4a. Development of a security architecture, 3rd paragraph, line 2	"...a single smart grid security architecture." At the last SGIP Meeting/Webinar Ron Ambrosio, the SGIP Architecture Work Group Chair noted that "There is no one smart grid architecture."
	Rationale/Recommendation
	This may be the case with the security architecture as well, and should be made a topic of discussion with the Architecture Work Group for resolution. [DEFER TO RON AMBROSIO OF GWA ON THE NEED FOR AND CONTENT OF THIS COMMENT]
	Disposition (for SGIP-CSWG use)

Comment Number: 07	Submitted by: Katherine Hamilton, President, GridWise Alliance	Comment Type: __ Tech. _X_ Editorial __ Gen.

Reference:	Comment
Page 7, Standards, line 6	Define or spell out "OSI", or include it in Appendix F, as appropriate.
	Rationale/Recommendation
	None
	Disposition (for SGIP-CSWG use)

Comment Number: 08	Submitted by: Katherine Hamilton, President, GridWise Alliance	Comment Type: __ Tech. ___ Editorial _X_ Gen.

Reference:	Comment
None	The following comments apply to the **application** of NISTIR 7628 document.
	Rationale/Recommendation
	In the opinion of GWA members, the NISTIR 7628 may be difficult for some asset owners to apply in its present form. In particular, the GWA is concerned about smaller utilities with fewer resources to understand, evaluate and apply the cyber security concepts embedded in the document. To help meet the need for broad industry application, GWA suggests the following: *Development of a Users Guide* – Either through a separate document, or as a part of the NISTIR 7628, a guide that walks the user through the use of the document is necessary. A Users Guide that describes the process to be followed, and explains the methodology for applying the requirements and logical interfaces would be very helpful for those asset owners not familiar with the subject matter. *Holding of Regional Workshops* – Direct instruction/discussion would help people who plan to implement the proposed requirements are needed to further the adoption and understanding of the NISTIR. GWA suggests that a series of regional workshops addressing the comprehensive scope of the NISTIR cyber security document would allow for greater participation by asset owner personnel. *Conducting Webinars* – In conjunction with the regional workshops, it would helpful to provide a series of webinars directed at specific topics. These events could be of a more limited duration, available to a wider audience.
	Disposition (for SGIP-CSWG use)