December 13, 2013

Information Technology Laboratory
ATTN.: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899-8930

RE: Request for Comments on the Preliminary Cybersecurity Framework

Dear Mr. Sedgewick:

On behalf of the GridWise Alliance (GWA), I am pleased to submit the attached comments to the National Institute of Standards and Technology (NIST) in response to the October 29 notice of a public comment period on the Preliminary Cybersecurity Framework.

Please contact Ladeene Freimuth at: Ladeene@freimuthgroup.com or at (202) 550-2306, should you have any questions about this submission.

Sincerely,

Becky Harrison

Becky Harrison
CEO
GridWise Alliance

GridWise Alliance Comments on Preliminary Cybersecurity Framework

The GridWise Alliance (GWA) appreciates the collaborative and open nature of this NIST Framework process thus far, and looks forward to a continued productive and collaborative approach going forward. To this end, GWA welcomes the opportunity to submit comments on the Preliminary Cybersecurity Framework, i.e., a Framework to reduce cyber risks to critical infrastructure.

GWA continues to urge NIST to build on what already has been developed to date in this area, rather than starting this process from "scratch." We urge NIST to ensure the Preliminary Framework is easily implementable (or "adopted").

Following are some overarching comments in response to whether the Preliminary Cybersecurity Framework achieves the objectives raised on page i of this document. We then provide more detailed comments.

1. **Ensure the Preliminary Framework focuses on reducing cyber risks and does not have inadvertent broader implications.** Having reviewed this Preliminary Cybersecurity Framework (hereinafter referred to as "Preliminary Framework"), as well as having attended some of the Workshops, and having submitted comments in response to the NIST Cybersecurity RFI in April 2013, our observation is that the Preliminary Framework needs to remain focused on reducing cyber risks or threats, as intended in the purpose of the Framework and the February 2013 Cybersecurity Executive Order. However, there are aspects that appear to go, or could be interpreted to go, beyond cyber risks or threats to broader business- and/or management-related risks.

   We urge NIST to maintain the voluntary, flexible and cost-effective approach intended by and for this Framework, while ensuring that the focus on cybersecurity risks and threats remains clear throughout.

   To the question posed about whether this "appropriately integrates cybersecurity risk into business risk" (page i), the frame of this question perhaps should be changed and/or narrowed – and reflected as such in the Preliminary Framework. That is, we (instead) would encourage NIST to incorporate a flexible risk management process. We call attention to the *Electricity Subsector Cybersecurity Risk Management Process* (RMP), which was developed by the electricity sub-sector in cooperation with DOE, NIST and the North American Reliability Corporation (NERC), leveraging the methodology provided by the March 2011 NIST Special Publication

(SP) 800-39, *Managing Information Security Risk*. The RMP provides a "consistent and repeatable approach to managing cybersecurity across the electricity subsector."[1]

We further recommend that the Framework's focus remain on *the systems and assets "essential to critical infrastructure" (rather than broader types of risks and/or rather than systems and/or assets that are not "essential to critical infrastructure") – and cyber risks to such systems and assets.*

We also urge NIST to ensure that the Framework does not inadvertently cause undue harm or burden (e.g., financially) to entities to which this Framework would, or could, apply.

2. **Ensure the voluntary approach of the Preliminary Framework is retained.** We want to express our strong view that "adoption" or implementation of the Preliminary Framework should not translate to any process(es) or measure(s) that could be interpreted as mandatory or used in an audit or any type of enforcement procedure or action against a given entity.

3. **Ensure recognition of existing processes, standards, and guidance, as well as differences within and across sectors, and throughout the entire supply chain.**

   We want to reiterate and underscore comments that our organization and others have made previously with respect to ensuring that this Preliminary Framework recognizes – and avoids duplication of – existing standards and processes, such as the mandatory, enforceable, cybersecurity (Critical Infrastructure Protection (CIP)) standards that were developed as a result of requirements established in the Energy Policy Act of 2005 and enforced by NERC, under the jurisdiction of the Federal Energy Regulatory Commission (FERC), and others.

In terms of more specific comments, we offer the following:

1. **Appendix B should be revised to focus on protecting those privacy and civil liberties associated with critical infrastructure cybersecurity activities.**

   Protecting privacy and civil liberties, of course, is important to our members and, important, in general. However, we are concerned that, Appendix B could be construed to recommend independent privacy protections unrelated to the protection of critical infrastructure, rather than on means to limit the privacy impacts of the Framework.

[1] U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process*, May 2012, http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.

We, therefore, recommend that NIST clarify the intention to protect only those privacy and civil liberties associated with critical infrastructure cybersecurity activities, and, that it accordingly revise the methodology in Appendix B to be tailored to improve critical infrastructure cybersecurity.

Additionally, it is critical that the privacy methodology is clear and actionable. The existing Appendix B does not readily allow companies to discern how to use the methodology or determine whether current practices already incorporate its elements. We understand that NIST has received at least one recommendation that contains some concepts and principles that directionally could provide a more actionable approach in this regard. We hope NIST will seriously consider improvements in this area/Appendix.

2. **The definition for Framework "adoption" has not yet obtained general consensus and should be modified.**

In the December 4, 2013 "Update on the Development of the Cybersecurity Framework" (hereinafter referred to as "Update"), NIST discusses a definition of Framework "adoption." This definition was proposed by the U.S. Department of Homeland Security (DHS) specifically with respect to the Voluntary Critical Infrastructure Cybersecurity Program. In the Update, NIST stated that "general consensus" was developed for this definition of Framework "adoption," based on deliberations during its November Workshop, held in Raleigh, NC. However, our members and CEO who participated in that Workshop did not observe such a consensus. Rather, we observed that the Workshop audience did *not* generally accept the term or clearly understand the definition of "adoption."

We recommend that NIST simplify the current "adoption" definition to: "an organization adopts the framework when it voluntarily uses the framework as a part of its risk management process."[2]

[2] Current definition: "An organization adopts the framework when it uses the Cybersecurity Framework as a key part of its systematic process for identifying, assessing, prioritizing, and/or communicating: cybersecurity risks, current approaches and efforts to address those risks, and steps needed to reduce cybersecurity risks as part of its management of the organization's broader risks and priorities." NIST, Update on the Development of the Cybersecurity Framework, December 4, 2013, http://www.nist.gov/itl/upload/nist_cybersecurity_framework_update_120413.pdf.