April 8, 2013

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

RE: Request for Information on Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

On behalf of the GridWise Alliance (GWA), I am pleased to submit the attached comments responding to the National Institute of Standards and Technology (NIST) Request for Information (RFI) on a "Cybersecurity Framework" that was published in the Federal Register on Tuesday, February 26, 2013.

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 NIST RFI:

Developing a Framework to Improve Critical Infrastructure Cybersecurity

The GridWise Alliance (GWA) welcomes the opportunity to submit comments in response to the Request for Information (RFI) that the National Institute of Standards and Technology (NIST) has issued with respect to developing a "Cybersecurity Framework" i.e., a Framework to reduce cyber risks to critical infrastructure. The GWA appreciates the open and collaborative nature of this process. Please note that we have responded to most, but not all, of the questions herein. At the outset, GWA urges NIST to build on what already has been developed to date in this area, rather than starting this process from "scratch."

Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

For those that have found themselves in a cyber threat-related situation, several have found that they were unable to come to a quick resolution – some of this depends on a firm's size, as well as the ability to determine the nature of the incident being faced, and other factors; relatedly, financial and business impacts often accrue. Thus, collaboration with other companies is important, as is looking across a company's entire supply chain to assess cyber threats.

Evaluating the business risk that a cyber threat or attack poses can vary substantially from one sector to another. Determining appropriate-scale solutions must be done in relation to the evaluated risks.

Beyond these points, some of the greatest challenges GWA sees in improving cybersecurity practices across critical infrastructure are as follows:

- Establishing the appropriate "cybersecurity" culture within an entire organization. Because this is not a static issue and threats can and will evolve quickly, organizations must similarly be able to prevent and respond to threats rapidly and nimbly.
- Obtaining cooperation across organizational silos of an organization. The magnitude of this issue requires such broad cooperation. Beyond a single organization, entities are trying to determine ways in which to work better with key providers of systems that could be susceptible to cyber attacks.

- Devoting the necessary level of human and financial resources to address the challenge; a risk management approach should be adopted within organizations.
- Developing, attracting and retaining skilled staff.
- Not all tools that are needed are available at this juncture; a number of solutions remain in the "beta testing" phase. Those that do exist will need to evolve quickly as threats evolve.
- Being able to quickly deploy new tools or "patches" without disrupting business.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

The greatest challenges in this realm are as follows:

- Unique requirements and factors for addressing cyber-related threats exist for different critical infrastructure sectors. And, different sectors are at different stages in dealing with or managing cyber threats.
- Attempts to cover all sector-specific requirements could result in overly broad, cumbersome, and/or unwieldy standards that are difficult to implement. Along the same lines, applying a "one size fits all" approach to different sectors likely could be too vague and/or unworkable in reality in a range of other ways.
- Depending on how this Framework is developed, as at least one expert recently noted, when entities develop their own cyber threat protection measures on a voluntary basis, typically, the result would be greater security for the company and compliance with relevant standards or regulations, as a result. On the other hand, if requirements are imposed and companies are audited for compliance and enforcement purposes, company resources tend to be more focused on compliance, and not necessarily on building the most secure environment; companies also typically will be less inclined to share information or otherwise cooperate with the government, if focused on compliance, and security protections might not be as great for fear of being found in violation of a given requirement.
- Owners/operators must take responsibility for, and be in charge of, their plans and responses to addressing cyber threats, which can be difficult, at times.
- The involvement of multiple federal agencies in this process could be challenging. The agencies should coordinate, so the private sector does not have to reconcile competing and/or conflicting requirements.
- Terminology and definitions differ from one sector to another, in some instances, which could pose issues in the development of this Framework.

3. **Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?**

It is worth noting that risk-related policies and procedures vary widely across the industry depending on the size of the organization, the resources available, and organizational regulatory requirements. That being said, the electric utility industry has developed risk management processes at the enterprise level to deal with a multitude of operational risks. These practices can serve as a basis for addressing cyber security. In addition:

- Many companies have Chief Risk Officers that oversee the policies and procedures governing risk, including ensuring that risks are effectively identified and managed within an organization.
- The Boards of Directors of many companies assess and compare the results of actual risk management efforts against enterprise risk management plans to ensure the organization's risk-related policies and procedures achieve maximum effectiveness.

Furthermore, the U.S. Department of Energy's (DOE) Cyber Security Risk Management framework and tools, as well as the mandatory, enforceable cybersecurity standards enforced by the North American Electric Reliability Corporation (NERC), under the jurisdiction of the Federal Energy Regulatory Commission (FERC), as well as regulations established and implemented by the Nuclear Regulatory Commission (NRC) establish a solid base for the electric utility industry to utilize.

Going forward, recommendations include:

- Organizational review of respective security policies and plans should be conducted at least annually. Any issues that arise or exceptions should be documented and approved by an "Executive Sponsor" (see description in the next bullet). This approval should be contingent on business needs and mitigating controls. Any issues or exceptions should be entered into a "Risk Register" that is reviewed at least annually.
- A "best practice" for senior management is for them to formally select an "Executive Sponsor" who is responsible for ensuring that a cyber threat/risk awareness and training program is implemented. The training should be readily available to all relevant employees.

4. Where do organizations locate their cybersecurity risk management program/office?

This varies by organization, and must match an organization's culture and be driven from the top.

- Many organizations locate their corporate risk management offices or programs in a finance or audit business unit.
  - A Physical Security Office often is responsible for controlling access to facilities and for issuing facility entrance/security badges.
  - Information technology (IT) organizations are tasked with securing computers and networks.
  - And, typically, an Operational Technology (OT) business unit protects and oversees SCADA and field devices.
  - While these disparate units typically have had minimal interaction in the past, they appear to be collaborating more and adopting a more unified approach.

- A recommended "best practice" appears to be consolidation of the Physical, IT and OT security operations, where appropriate, and then feeding information obtained about risks into the finance business unit, with regular oversight by the audit business unit.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

A generic formula for defining and assessing risk is as follows:
Threat x Vulnerability x Consequence = Risk.

Basic components of risk assessment consist of:

- Access management;
- Identity management; and
- "Patch" management (i.e., implementing "fixes" from vendors to software, when a risk is identified, much like with computers/software).
- "Defense in depth" strategies and processes. A "defense in depth" approach to cyber security is an established best practice. Such practices balance focus between people, technology and operations.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

The extent to which cybersecurity risk is incorporated into an organization's overarching enterprise risk management varies a great deal from one organization to another and depends on a range of factors, including some of those referenced in this document. Most, if not all, organizations are incorporating cybersecurity risks into

their overarching enterprise risk management to some extent but, again, the degree to which this is occurring differs significantly from company to company.

No general design or framework currently exists with which all organizations conform. Some organizations delegate these responsibilities to dedicated staff; often staff turnover contributes to variations or changes in approach to the incorporation of cyber risks into overall risk management strategies.

Some have suggested that cybersecurity risk management should be fully incorporated into an organization's enterprise risk management practices, to the extent practicable.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

- Many product vendors use the ISO 27000 series, including ISO 27001.
- NISTIR 7628, Guidelines for Smart Grid Cyber Security, is being used, though it currently is undergoing review and revisions. This has been a focus for the NIST SGIP Cybersecurity Working Group.
- The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) developed as part of a White House initiative led by the U.S. Department of Energy (DOE) in partnership with the U.S. Department of Homeland Security (DHS) and in close collaboration with the private sector and other Federal agencies, allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity.
- International Electrotechnical Commission (IEC) work is being discussed. Commission drafts should be forthcoming.
- Tools are prevalent; they can be purchased on the open market and include Security Information Management System (SIMS); specific software; and, spreadsheets, as examples.
- With respect to the financial services industry, the PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, and education regarding PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. These standards have enabled new and innovative secure payment options. They are applied at all levels from the smallest merchant to the largest financial institutions. Efforts at the local and national levels will drive best practices, compliance, and so forth.
- The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body of the United States Government empowered to prescribe uniform principles, standards, and report forms for the federal examination of

financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions.

- The risk-management based strategies employed by the gaming industry could serve as a model.

In addition, the mandatory, enforceable cybersecurity (Critical Infrastructure Protection (CIP)) standards developed as a result of requirements established in the Energy Policy Act of 2005 (EPAct 2005), and enforced by the North American Electric Reliability Corporation (NERC), under the jurisdiction of the Federal Energy Regulatory Commission (FERC), as well as regulations established and implemented by the Nuclear Regulatory Commission (NRC) establish a solid base for the electric utility industry to utilize.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

NERC CIP cyber security requirements and requirements established by NRC for the nation's nuclear fleet currently exist, as noted in #7 above.

One drawback of mandatory requirements is that this approach often creates a mindset of doing the minimum to ensure compliance, due to the risk of incurring a violation. This mindset thereby focuses critical resources on ensuring no violations are found during the audit process versus proactively focusing on increasing security against emerging threats.

Cyber threats cross state and national boundaries; therefore, any regulations or mandates must ensure that they do not inadvertently prohibit an owner/operator of critical infrastructure from being able to address the risks it faces in a holistic manner.

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

For the electric sector, there are many interdependencies – particularly with the telecommunications and information technology (IT) sectors.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

No response being provided here.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

The electric utility industry deals with significant federal and state regulations today, many of which overlap. There need to be clear lines of accountability and verification that authorities do not overlap with respect to cybersecurity, if the desire is for the ability to successfully manage identified or emerging threats in a timely manner.

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

- NERC Critical Infrastructure Protection (CIP) cybersecurity standards apply to the bulk electrical system.
- NRC develops standards for the nuclear industry.
- DOE and DHS, in partnership with the private sector, have undertaken the Electricity Subsector Cybersecurity Capability and Maturity Model (ES-C2M2) to strengthen the industry's cyber readiness by enabling electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their security investments. The ES-C2M2 is a flexible, risk-based and cost-effective framework. It helps gauge industry readiness and can be used to provide guidance for policy making. Some are using this Model to make resource allocation decisions. Others indicate this Model might be a valuable tool or starting point for NIST in developing the Cybersecurity Framework at hand.
- The NIST Smart Grid Interoperability Panel (SGIP) is coordinating the development of guidelines, principles, standards and best practices for smart grid technologies.
- Standards development organizations develop voluntary standards. Following is a *partial* list of standards organizations that engage in this space:
  - ISO – the ISO 27000 series - Information Security Management Systems (ISMS);
  - American National Standards Institute (ANSI);

- Institute of Electrical and Electronics Engineers (IEEE);
- Internet Engineering Task Force (IETF);
- World Wide Web Consortium (W3C);
- North American Energy Standards Board (NAESB);
- International Telecommunications Union (ITU);
- International Society of Automation (ISA);
- National Electrical Manufacturers' Association (NEMA); and
- Organization for the Advancement of Structured Information Standards (OASIS).

Part II: Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?

At a minimum, GWA is aware of the following approaches that address cyber threats and protection efforts with respect to the electricity sector. GWA urges NIST to avoid duplicating existing relevant efforts in the course of this Cybersecurity Framework process.

- **NERC CIP Standards:**

  As you likely are aware, the Energy Policy Act of 2005 (EPAct 2005) gave the Federal Energy Regulatory Commission (FERC) authority to oversee the reliability of the bulk power system, commonly referred to as the bulk electric system or the power grid. This includes authority to approve mandatory cybersecurity reliability standards.

  This led to NERC CIP standards for the bulk power system. Hence, as discussed elsewhere in this document, the bulk power system is subject to NERC mandatory Critical Infrastructure Protection (CIP) cybersecurity standards, under the jurisdiction of FERC.

  In the course of this Cybersecurity Framework under consideration, it is important that NIST and the other relevant stakeholders examine the way(s) in which the NERC CIP standards evolved, and note that the desired results are not necessarily being achieved across the board, and the reasons for these shortcomings – and an example which highlights that mandatory standards are not always the best approach.

  More specifically, while this was intended to be an open, collaborative public-private sector process to identify critical infrastructure assets that warrant higher levels of cyber protections, the NERC compliance audits and potential for mandatory fines has discouraged the private sector from sharing information, because of concerns that such information ultimately could be used against them during audit, compliance and enforcement procedures. Consequently, the process has become somewhat adversarial. This being said, the bulk power system is being operated reliably.

- **NIST SGIP:**

  Under the Energy Independence and Security Act of 2007 (EISA 2007), NIST was given "primary responsibility to coordinate development of a framework

that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems."

The NIST Smart Grid Interoperability Panel (SGIP) exists to help drive and expedite this "smart grid" interoperability process. The process was funded by NIST. Due to federal fiscal constraints, it is now member-based, and funded by its members. Portions of the SGIP have worked well and could be drawn upon for the Cybersecurity Framework for which these comments are being sought.

However, there have been some challenges with the SGIP, which should be avoided in this Cybersecurity Framework development process. For example, the SGIP is 100 percent consensus-based. Sometimes it is difficult to attain complete consensus and, thus, to move the process forward and achieve results. GWA recommends ***not requiring complete consensus*** for the Framework process at hand.

In addition, of the 22 stakeholder categories that comprise the NIST SGIP, all of the investor-owned utilities (IOUs) only have one Board of Governor seat and therefore one vote. We suggest better proportional representation within and across critical infrastructure sectors.

GWA also urges ***avoiding development or issuance of mandatory standards.*** Rather, standards should be voluntary to foster true security gains.

- **NIST SGIP Catalog of Standards:**

  As part of the NIST SGIP, a Catalog of Standards has been developed, which Lists best practices, standards, guidance, and so forth.

- **NISTIR 7628:**

  Emerging cyber threats that target power systems have highlighted the need to integrate more advanced security to protect these critical assets. To address the cross-cutting issue of cybersecurity, NIST established the SGIP Cyber Security Working Group (CSWG). In August 2010, the CSWG produced NIST Interagency Report 7628, *Guidelines for Smart Grid Cyber Security*. Since then, the group has moved on to focus on specific topics such as risk management processes, key management within the Smart Grid, developing a "smart grid" security architecture, testing and certification issues, Advanced Metering Infrastructure security, and privacy within the "smart grid." One subgroup has also conducted reviews of several "smart grid-related" standards to see how these standards address cybersecurity.

This is a good example of a Group and process that address cybersecurity holistically, and could be drawn upon by NIST for this Cybersecurity Framework.

- **NRC:**

  As also noted earlier, nuclear energy facilities are subject to extensive regulation by the Nuclear Regulatory Commission (NRC) to ensure cyber protection, which were implemented in 2002 and expanded upon in 2009. A NERC-NRC Memorandum of Understanding (MOU) exists to ensure coordination and avoid gaps in cyber protections for nuclear generators.

- **ES-C2M2:**

  Also cited above, the Electricity Subsector Cybersecurity Capability and Maturity Model (ES-C2M2) has been created by the U.S. Department of Homeland Security (DHS) and the U.S. Department of Energy (DOE), in partnership with the private sector, to strengthen the industry's cyber readiness by enabling electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their security investments.

  In addition, DOE has open group architecture guidelines. Internet Telephony (ITel) also has approaches to address cyber threats. And ISO, as noted elsewhere in this document, has standards to help prevent and address cyber threats.

2. Which of these approaches apply across sectors?

NIST provides guidance across numerous overarching security requirements (NIST 800-53 is a great example).

3. Which organizations use these approaches?

- Utilities that own/operate transmission and transmission organizations (RTOs/ISOs) are subject to the NERC CIP standards.
- Nuclear facility owners and operators are subject to the NRC standards.
- Smart grid project implementers and vendors are using the NIST interoperability standards, which are not mandatory.

4. **What, if any, are the limitations of using such approaches?**

- In terms of NERC CIP standards, for example, sometimes a new standard is issued while entities are still implementing a previous standard, so there is a lag time issue. Change in the cyber arena occurs dramatically (i.e., by orders of magnitude), rather than incrementally, so it is generally difficult to know how to address and organize around this issue.
- Sometimes there is confusion associated with certain approaches (e.g., PCI compliance, but not with PCI 1.2).
- Some of these approaches are mandatory, while some are voluntary.
- Organizations must balance speed of implementation, cost, and actual and perceived risks in determining how to apply NIST SGIP.
- Non-prescriptive guidance is open to interpretation.
- It is possible to encourage organizations to take action to document compliance (i.e., to instill a "culture of compliance") instead of truly enhancing security (i.e., instilling a "culture of security"), as one expert recently noted.

5. **What, if any, modifications could make these approaches more useful?**

A clear picture of what is needed up front is necessary, however, this is difficult, due to the rapidly-evolving nature of the cyber arena and risk management approaches to this topic.

Product requirements should be established that can be certified to enable vendors to build in the appropriate level of security into their products without worrying about pricing themselves out of competition, due to others not incorporating sufficient security protections. Utilities should include in Requests for Proposals (RFPs) requirements that vendor products are certified in this manner.

6. **How do these approaches take into account sector-specific needs?**

Standards, guidelines and best practices have been and are being developed specifically for the electric utility industry, which incorporate a base level of general security practices, particularly in the information technology (IT) arena.

It is worth noting that sometimes sector-specific needs can conflict with higher, overarching objectives.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

Both already exist in the electric sector. These might need to be expanded on in particular areas, but existing organizations and processes should be relied on to accommodate any needed expansions. No new organizations should be added.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

These agencies and/or councils need to be able to effectively share information with the sector stakeholders, including vendors of products and systems that would need to incorporate various guidelines or standards. Also, these entities should assist smaller organizations in implementing relevant best practices, processes and/or standards. A formal structure to assist with peer-to-peer information sharing and review processes is worth considering. GWA urges avoiding mandatory approaches, as noted elsewhere in this document, that could drive resources to compliance activities versus "value-add" activities.

9. What other outreach efforts would be helpful?

State-federal coordination efforts could prove useful. In addition, aligning state regulatory and legislative bodies to ensure coordination and cost effective implementation and cost recovery efforts likely would be valuable. States also need to ensure that the utilities under their jurisdictions are engaged and active in protecting their systems.

Part III: Specific Industry Practices

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

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

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

The practices listed just above generally are implemented by larger organizations. Smaller organizations may face greater challenges in implementing such practices or might not have implemented them at all thus far. Finding ways to make adopting these practices cost effective for businesses is important.

- Utilities have adopted practices on both the IT and OT (process system) sides of their business to protect their infrastructure and data as well as to ensure business continuity.

- Although these practices might not currently be applied to distribution process systems in all cases, efforts have been progressing across the industry to identify and implement best practices.

- The American Recovery and Reinvestment Act of 2009 (ARRA) "smart grid" grant program required grantees to submit cybersecurity plans. These cyber plans have been audited by DOE as part of the Department's ongoing oversight activities for these grants.

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

ISO standards are used extensively in the U.S. and around the world by organizations and reflect that an organization's products and processes meet or exceed industry best practices in a given area. It would be valuable to implement these practices domestically in a manner that is consistent with international standards and practices.

In addition, most major product and services vendors operate globally. Efforts to coordinate standards internationally would be beneficial to vendors as well as their customers.

ISO standards "cross-walks" should be undertaken to ensure that international practices and standards can be mapped to comparable domestic ones and checked for consistency. This would help U.S.-based companies, or companies with a U.S. presence, determine whether their U.S.-produced goods and services meet standards deployed throughout global markets (and, if not, to make changes so they ultimately would meet such global standards). If so, then these American companies would be able to source components from the most competitive vendors, regardless of location, as well as deploy technologies globally, knowing their products meet such global standards.

In the North American region, critical infrastructures cross national borders and, therefore, standards, practices and regulations generally will need to incorporate consideration of this broader region into any efforts in this space.

In addition, as new standards and requirements are developed, the fact that the owner/operators of these systems have infrastructure in place and, therefore, are not dealing with a "green field" where new capabilities can be implemented more easily also must be taken into consideration. The legacy systems and infrastructure must evolve over time to make sure cost effective adoption of relevant standards and practices is achieved.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

A "defense in depth" approach to cyber security is an established best practice. Such practices balance focus between people, technology and operations. Some of the basic practices that all entities should apply include:

- Access management;
- Identity management;
- Patch management/version control;
- Data encryption; and,
- Training of personnel.

High priority should also be given to:

- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices; and,
- Separation of business from operational systems.
    - This latter practice can make sense if not taken too far. Separating business

and operational applications on the same desktop machine is not always practical and can limit value to operations. Training personnel on the risk of their behaviors is essential in any case.

- Dividing network traffic (business WAN/LAN and grid WAN/LAN) makes sense.

These points having been made, all of the practices listed at the beginning of this "Industry Practices" Section, i.e., Part III, of this RFI are important and should be taken into consideration.

In addition, privacy and civil liberty protections are essential to increase private industry sharing both with other private industry players and the government as reflected in a set of principles on cybersecurity by the GWA, as well as in the pending "Rogers-Ruppersberger" cybersecurity legislation.

Moreover, collaboration with other companies, with a view toward looking at an organization's entire supply chain, is vital in the cyber arena.

Law enforcement will need to change to deal with rapidly-evolving cyber threats, as well.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

No. In fact, all of these practices do apply to the electric utility sector.

5. Which of these practices pose the most significant implementation challenge?

Identity management is among the most significant implementation challenges being faced. In addition, monitoring and incident detection tools and capabilities pose challenges; these must evolve as the threats evolve. Getting the tools developed and deployed in a timely manner will be challenging.

Cost is a major issue. For any organization, resource allocations (funding and people) are always challenging. Since costs associated with addressing cyber security do not directly result in increased revenues to an organization or reduce day-to-day operating costs, determining the amounts to be spent in this area is challenging at best. A risk management approach helps frame these decisions within organizations.

Relatedly, due to the emerging nature of cybersecurity-related challenges, cost recovery practices within the energy sector need to be adjusted to allow for proper funding of these activities. Since these are generally "Operations & Maintenance"

(O&M) expenditures, it is critically important to ensure the appropriate funding levels are achieved.

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

A number of organizations look to adopt "best practices." Having these practices available to organizations at little or no cost will help with adoption. For smaller organizations, a hosted or services model may make sense and can help these organizations implement standards and best practices, where service providers or hosted services provide the expertise needed.

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

Please see response to #5 above.

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

Electric utilities are used to dealing with situations that have the potential to escalate. Their risk management practices include developing and exercising plans to respond to these types of situations. A cybersecurity risk should be treated as an enterprise risk with plans developed to address such threats that include the proper escalation procedures.

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

GWA's members perceive substantial risks to privacy and civil liberties in the application of these practices. For these reasons, GWA has identified the need for privacy and civil liberty protections as one of its core principles with respect to cybersecurity. The pending "Rogers-Ruppersberger" cybersecurity legislation also reflects the need for additional privacy and civil liberty protections in this area.

Put another way, to promote the information sharing that will enhance cybersecurity protections within critical infrastructure sectors, private industry must be assured that information they share will be closely protected and not used for any purpose other than enhancing cybersecurity responses and protections. And, they need to be able to recover any damages for improper sharing of such information.

In addition, for organizations to be able to share critical information in a timely manner with others in the industry, they must be assured that there will not be any antitrust issues on the back side of sharing this information. Much concern stems around such antitrust issues.

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

Organization for Economic Cooperation and Development (OECD) privacy principles may serve as a baseline. These need to be tied to U.S. privacy principles. It also is important to ensure that this Cybersecurity Framework being developed is consistent – and in no way interferes – with these OECD principles or with the other international standards and practices discussed throughout this document, and any other relevant international standards and practices, for that matter. In other words, the Cybersecurity Framework must not create or impose any standards or practices in the U.S. that could in any way prevent businesses from operating in global markets in which they currently have a presence or plan to have one.

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

As noted elsewhere in this document, legislation is needed to ensure the open sharing of information will not result in liabilities to organizations that share or receive such information.

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

The Code of Fair Information Practices should be taken into consideration during this Framework development process. In addition, the "right" to correction and review, as well as to expect notice or consent for the use and/or transfer of important information, and the "right" to expect accurate information should be considered.

In addition, to encourage adoption and effective implementation, consideration should be given to establishing methods for peer-to-peer collaboration and review in a non-mandatory environment. The nuclear industry established the Institute of Nuclear Power Operations (INPO) to help the entire industry "self-monitor," share best practices, conduct peer reviews, and thereby improve their performance. A similar model in this space might be desirable.